Executive Summary of Changes

Version 4.0 of the TxDOT Information Security and Privacy Controls Standards Catalog includes:

- Updates to the CSP v6.0 for CJIS, which completes the FBI's modernization project to align with NIST SP 800-53r5x.
- Updates to PCI DSS 4.0.1, including requirement changes effective March 31, 2025.
- Substantive changes to CP-02, RA-05, and SA-09(05); and the removal of IA-02(08) and PL-08 from the TxDOT Minimally Assessed Controls.
- Changes to publication: Appendices separate from Catalog.

CJIS Overlay

CJIS requirements have been updated to align with NIST 800-53r5. CSPv.5.9.1 had requirements numbered 5.1 through 5.13; 5.14 onward were added during the modernization process officially completed with CSPv6.0.

CSPv5.9.x ID	CSPv6.0 ID
5.1	5.1
5.2	AT
5.3	IR
5.4	AU
5.5	AC
5.6	IA
5.7	CM
5.8	MP
5.9	PE
5.10	SC
5.11	CA
5.12	PS
5.13	Renumbered to 5.20

CSPv5.9.x ID	**CSPv6.0 ID**
5.14	SA
5.15	SI
5.16	MA
5.17	PL
5.18	CP
5.19	RA

Requirements are now typically mapped to specific requirements, with the exception of administrative requirements (sections 1-4) and mobile (5.20). Updating to these new mappings required changes to the CJIS overlay as follows:

Description of Change	**TxDOT Controls Changed for CSPv6.0**
Added CJIS overlay to control	AC-01, AC-02(01), AC-02(02), AC-02(03), AC-02(04), AC-02(05), AC-02(13), AC-06(01), AC-06(02), AC-06(07), AC-06(09), AC-06(10), AC-11(01), AC-12, AC-17(02), AC-17(03), AC-17(04), AC-20(01), AC-20(02), AC-21, AC-22, AT-01, AT-02, AT-02(02), AT-02(03), AT-03(05), AU-03(03), AU-04, AU-06(01), AU-06(03), AU-07, AU-07(01), AU-09(04), CA-01, CA-02(01), CA-05, CA-06, CA-07, CA-07(01), CA-07(04), CA-09, CM-01, CM-02(02), CM-02(03), CM-03, CM-03(02), CM-03(04), CM-04, CM-04(02), CM-06, CM-07(02), CM-08(01), CM-08(03), CM-10, CM-11, CM-12, CM-12(01), CP-01, CP-02, CP-02(01), CP-02(03), CP-02(08), CP-03, CP-04, CP-04(01), CP-06, CP-06(01), CP-06(03), CP-07, CP-07(01), CP-07(02), CP-07(03), CP-08, CP-08(01), CP-08(02), CP-09, CP-09(01), CP-09(08), CP-10, CP-10(02), IA-02(08), IA-02(12), IA-03, IA-04(04), IA-05(06), IA-07, IA-08, IA-08(01), IA-08(02), IA-08(04), IA-11, IA-12, IA-12(02), IA-12(03), IA-12(05), IR-01, IR-03, IR-03(02), IR-06(03), IR-07, IR-07(01), MA-01, MA-02, MA-03, MA-03(01), MA-03(02), MA-03(03), MA-05, MA-06, PE-06(01), PE-08, PE-08(03), PE-09, PE-10, PE-11, PE-12, PE-13, PE-13(01), PE-14, PE-15, PE-17, PL-01, PL-04, PL-04(01), PL-08, PL-10, PL-11, PS-01, PS-02, PS-06, PS-07, PS-09, RA-01, RA-03, RA-05, RA-05(02), RA-05(05), RA-05(11), RA-07, RA-09, SA-01, SA-02, SA-03, SA-04, SA-04(01), SA-04(02), SA-04(09), SA-04(10), SA-05, SA-08, SA-08(33), SA-09(02), SA-10, SA-11, SA-15, SA-15(03), SA-22, SC-01, SC-04, SC-05, SC-07(03), SC-07(04), SC-07(05), SC-07(07), SC-07(08), SC-07(24), SC-08, SC-10, SC-12, SC-15, SC-18, SC-20, SC-21, SC-22, SC-23, SC-28, SC-39, SI-02(02), SI-04(05), SI-07, SI-07(01), SI-07(07), SI-08(02), SI-10, SI-11, SI-12, SI-12(01), SI-12(02), SI-12(03), SI-16, SR-01, SR-02, SR-02(01), SR-05, SR-08, SR-10
Removed CJIS Overlay from control	AC-10, CA-08, MP-03, PS-04(02), SC-07(18), SC-45(01), SI-04(01), SI-05(01)

Description of Change	TxDOT Controls Changed for CSPv6.0
Added to Catalog, added to CJIS Overlay	AC-03(14)
Removed from Catalog; no longer applicable to any baseline or overlay once CJIS was removed from control	AC-03(07), IR-06(02), SA-09(08), SC-07(13), SC-16, SC-43, SI-04(07)

Where the CJIS requirement is more stringent or different from the TxDOT control, additional CJIS Correspondence standards have been added.

PCI DSS Updates

PCI DSS updates from v4.0 to v4.0.1 were largely non-substantive. Language and formatting updates were applied to the Catalog as applicable. Also in this update to the Catalog, PCI DSS requirements effective March 31, 2025 have been incorporated:

PCI DSS 6.4.1 has been superseded by 6.4.2

PCI DSS 8.3.10 has been superseded by 8.3.10.1

PCI DSS 10.7.1 has been superseded by 10.7.2

PCI DSS 10.7.3 now applies to all entities.

Per-Control Changes

Substantive changes in this release were made to:

Control ID	Control Name	Description
IA-02(08)	Access to Accounts — Replay Resistant	Removed from Minimally Assessed Controls
PL-08	Security and Privacy Architectures	Removed from Minimally Assessed Controls

RA-05	Vulnerability Monitoring and Scanning	Stds.06&07 have been rescinded, specifics moved to ISS-01-218, TxDOT Vulnerability Scanning Standard.
SA-09(05)	Processing, Storage, and Service Location	Std.04 added to clarify pre-approval requirements. Added to Moderate and High baselines.

Changes to Appendices

With Catalog v4.0, appendices are now published separately from the Catalog.

ISS-01-801-1, Baselines, Overlays, and Minimal Assessed Controls (formerly Appendix D), has been updated.

ISS-01-801-2, PCI DSS to TxDOT Control IDs (formerly Appendix B), has been updated for PCI DSS 4.0.1.

ISS-01-801-3, CJIS to TxDOT Control IDs (formerly Appendix C). This appendix has been updated per the revised structure of CSP V6.0 and necessary changes to the mapping, and includes the correspondence between the latest release and the version previously included in the Catalog.

ISS-01-801-4, Texas Cybersecurity Framework to TxDOT Control IDs (formerly Appendix E), has been updated.

ISS-01-801

Standard Title: Information Security and Privacy Controls Standards Catalog

Effective Date: 05/15/2025

Date of Last Revision: 04/25/2024

Office of Primary Responsibility: TxDOT Information Security Office

---

Overview

Purpose and Applicability. The TxDOT Information Security and Privacy Controls Standards Catalog (Catalog) provides the complete set of the minimum security controls for information systems that process, store, transmit, or maintain TxDOT data.

Audience. This Catalog applies to all information systems and associated entities that process, store, or maintain TxDOT data. All TxDOT information owners and custodians should read and understand those portions of this Catalog that apply to the systems for which they are responsible.

Scope

The intent of the Catalog is to record all security and privacy control requirements with which TxDOT systems may be required to comply based on system categorization and data classification.

Using the Catalog

Introduction. TxDOT's Catalog establishes the minimum requirements for TxDOT's information security assets. Based on NIST SP 800-53r5, the Catalog includes requirements derived from state authority, including the Texas Department of Information Resources (DIR) and state legislation, as well as agency-specific requirements as determined by the Chief Information Security Officer (CISO) in light of the environment of

operations and the agency's security posture. The TxDOT Catalog can be considered the agency's equivalent to NIST SP 800-53r5. Where necessary, and in alignment with the tailoring guidelines provided in the SP 800-53r5, some controls have been tailored from the NIST-provided document by overwriting baselines; adding implementation standards; applying overlays, as applicable; and through tailoring of the language provided in SP 800-53r5.

DIR maintains a catalog based on SP 800-53. The TxDOT Catalog meets or exceeds requirements from DIR's document, and DIR state implementations are included in the Implementation Standards for applicable controls.

Additionally, ISS-01-801-4 (formerly Appendix E) provides a mapping from controls to the Texas Cybersecurity Framework (TCF), NIST SP 800-53r5, and DIR's Security Control Standards Catalog.

Overlays have been developed to address additional requirements to which some TxDOT systems are subject. Refer to the glossaries and instructional files maintained by those requiring bodies for more information. See TxDOT's Security and Privacy Glossary for agency definitions.

Catalog Conventions

The Catalog was developed from NIST's SP 800-53r5 (released Sept. 2020, updated to r5.1 December 2020 and r5.1.1 October 2023) and 800-53B (October 2020). Titles for controls and enhancements are identical to those documents though reformatted for readability.

All controls and enhancements to which TxDOT systems may be subject are present in this document. Requirements are tailored from 800-53r5. Baselines and overlays are tailored for TxDOT from those provided in SP 800-53B.

This document takes precedence over the NIST documents used as source material.

Publications

The TxDOT Information Security and Privacy Catalog (including all TxDOT information security and privacy control requirements, implementation standards, discussion, and references) is maintained by TxDOT Information Security. For a Word or Excel version of this Catalog or its appendices, e-mail InfoSecurity@txdot.gov.

ISS-01-801-1 (formerly Appendix D) Baselines, Overlays, and Minimal Assessed Controls

This table, formerly published as the TxDOT Information Security Control Baseline Standards, provides a view of the controls by number and name with applicable baselines and overlays.

ISS-01-801-2 (formerly Appendix B) PCI DSS to TxDOT Control IDs

This table provides a mapping of PCI DSS requirements to the TxDOT controls. All 250 numbered PCI DSS requirements correspond to one or more items in the Catalog, and correspondences are addressed within the body of individual controls.

ISS-01-801-3 (formerly Appendix C) CJIS to TxDOT Control IDs

This table provides a mapping of applicable CJIS requirements to the TxDOT controls. Correspondences are addressed within the body of individual controls.

ISS-01-801-4 (formerly Appendix E) Texas Cybersecurity Framework to TxDOT Control IDs

This table provides a mapping of TxDOT Control IDs to the Texas Cybersecurity Framework objectives. All controls and control enhancements included in the TxDOT Catalog appear in this table.

Contact

Questions about this content must be directed to InfoSecurity@TxDOT.gov. Only TxDOT's Chief Information Security Officer or delegate can address questions about this standard.

Version History

Version	Date	Updated By	Brief Description of Change
1.0	08/28/2020	Sylverre Polhemus-C	Initial Catalog release, published to GRC site and uploaded to DIR.
1.1	09/25/2020	Sylverre Polhemus-C	Minimal update of titles, numbering, baselines, and overlays to align with official release of NIST SP 800-53r5; published to GRC site.

Version	Date	Updated By	Brief Description of Change
2.0	1/15/2021	Sylverre Polhemus-C	Full update and packaging to align with official release of SP 800-53B and revisions to content per SP 800-53r5.1 (December 2020) update; published to GRC site, uploaded to DIR, and packaged in accessible format.
2.1	05/05/2021	Sylverre Polhemus-C	Full update and packaging to add PCI DSS correspondence and update minor changes (see errata) since 2.0; published to GRC site, uploaded to DIR, and packaged in accessible format.
2.2	03/15/2022	Sylverre Polhemus-C	Full update and packaging to add CJIS correspondence; incorporate updates to 1 TAC 202; and update minor changes (see errata) since 2.1; published to GRC site, uploaded to DIR, and packaged in accessible format.
2.2.1	08/01/2022	Sylverre Polhemus-C	Point release to address changes to RA-05 (for PCI DSS) and AC-11 (TxDOT Discussion to address Section 508 for ICT), plus a change to the overlays for CA-08.
2.3	03/31/2023	Sylverre Polhemus-C	Full update and packaging to add TX-RAMP correspondence and Prohibited Technologies requirements; minor changes (see errata) since 2.2.1; published to GRC site, uploaded to DIR, and packaged in accessible format.

Version	Date	Updated By	Brief Description of Change
2.4	08/01/2023	Sylverre Polhemus-C	Full update and packaging to align with updated DIR Control Standards Catalog. Published to GRC site, uploaded to DIR, and packaged in accessible format.
3.0	04/01/2024	Sylverre Polhemus-C	Full update and packaging to add FedRAMP overlays and Correspondence and to split the TX-RAMP overlay into Level 1/Level2; updates for PCI DSS 4.0; updates per TGC 2054, TAC 202; minor changes (see errata) since 2.2.1. Published to GRC site, uploaded to DIR, and packaged in accessible format.
3.0.1	04/25/2024	Sylverre Polhemus-C	Point release to update Minimally Assessed Controls and resolve a numbering conflict in the Correspondence Standards for RA-05. Published in all formats.
4.0	05/14/2025	Sylverre Polhemus-C	Full update and packaging to separate appendices from main body; update to PCI DSS 4.0.1; update to CSP v6.0; update baselines and Minimal Assessed Controls; and align with other TxDOT publications.

Contents

AC — Access Control 12
AT — Awareness and Training 118
AU — Audit and Accountability 138
CA — Assessment, Authorization, and Monitoring 190
CM — Configuration Management 235
CP — Contingency Planning 304
IA — Identification and Authentication 368
IR — Incident Response 449
MA — Maintenance 499
MP — Media Protection 522
PE — Physical and Environmental Protection 546
PL — Planning 595
PM — Program Management 617
PS — Personnel Security 687
PT — Personally Identifiable Information Processing and Transparency 710
RA — Risk Assessment 726
SA — System and Services Acquisition 765
SC — System and Communications Protection 834
SI — System and Information Integrity 910
SR — Supply Chain Risk Management 984

AC — Access Control

AC-01 Policy and Procedures

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level access control policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate a senior management official as defined in the access control policy to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 7.1.1 and 7.1.2.

Std.03 PCI — Rescinded in V3.0.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.04 CJIS — Review and update the current access control policy and procedures following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. [Source: CJIS AC-01]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Access control policy and procedures address the controls in the AC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs

collaborate on the development of access control policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to access control policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202.21; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-12, 800-30, 800-39, 800-100; NIST IR 7874; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

IA-01, PM-09, PS-08, SI-12

AC-02 Account Management

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;

b. Assign account managers;

c. Require prerequisites and criteria as defined in the System Security Plan (SSP) for group and role membership;

d. Specify:

1. Authorized users of the system;

2. Group and role membership; and

3. Access authorizations (i.e., privileges) and attributes as defined in the SSP (as required) for each account;

e. Require approvals by the Information Owner in accordance with access criteria for requests to create accounts;

f. Create, enable, modify, disable, and remove accounts in accordance with the TxDOT Information Security policy;

g. Monitor the use of accounts;

h. Notify account managers and personnel or roles as defined in the SSP within:

1. One calendar day when accounts are no longer required;

2. One calendar day when users are terminated or transferred; and

3. One calendar day when system usage or need-to-know changes for an individual;

i. Authorize access to the system based on:

1. A valid access authorization;

2. Intended system usage; and

3. Attributes as defined in the SSP (as required);

j. Review accounts for compliance with account management requirements annually;

k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and

l. Align account management processes with personnel termination and transfer processes.

Implementation Standards

Std.01 — AC-02 Std.01 moved to AC-06 Std.03c and SA-09 Std.15 in V2.4.

Std.02 — The Information Owner or their designated representative(s) are responsible for approving access to information resources and periodically reviewing access lists based on documented risk management decisions. [Source: 1 TAC 202.22(a)(1)(B)]

Std.03 — Establish and follow a process, preferably automated, for:

a. Granting system and application access upon new hire, rights grant, or role change of a user. [Source: CIS 6.1]

b. Revoking system, application, and network access by disabling accounts immediately upon termination or change in user responsibilities. [Source: CIS 6.2]

Std.04 — Individual, role, or group access to system components and data must be:

a. Denied unless specifically allowed;

b. Granted based on valid business requirements including need-to-know and need-to-share; and

c. Limited to only that required.

Std.05 — Systems that are not integrated with the enterprise-wide single sign-on solution must create, enable, modify, audit, disable, and remove accounts in accordance with access policy and account management processes.

Std.06 — Emergency accounts should be automatically disabled after the period defined in TxDOT's Business Continuity policy. Other temporary

accounts must be created with time limitations consistent with access policy and account management processes.

Std.07 — Third-party access to electronic resources is time-limited and must be terminated at the conclusion or termination of a contract or agreement.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 8.2.4.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.08 PCI —

a. An access control system(s) is in place that restricts access based on a user's need to know and covers all system components. [Source: PCI DSS 7.3.1]

b. The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function. [Source: PCI DSS 7.3.2]

c. The access control system(s) is set to "deny all" by default. [Source: PCI DSS 7.3.3]

Std.09 PCI — All user access to query repositories of stored cardholder data is restricted as follows:

a. Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges.

b. Only the responsible administrator(s) can directly access or query repositories of stored Cardholder Data (CHD).

[Source: PCI DSS 7.2.6]

Std.11 PCI — Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows:

a. Enabled only during the time period needed and disabled when not in use.

b. Use is monitored for unexpected activity.

[Source: PCI DSS 8.2.7]

For systems processing PCI DSS data, or that support PCI DSS processes, Std.07 is superseded by PCI DSS requirements 7.2.4 and 7.2.5.1:

Std.10 PCI — Rescinded in V3.0.

Std.12 PCI — All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows:

a. At least once every six months.

b. To ensure user accounts and access remain appropriate based on job function.

c. Any inappropriate access is addressed.

d. Management acknowledges that access remains appropriate.

[Source: PCI DSS 7.2.4]

Std.13 PCI — All access by application and system accounts and related access privileges are reviewed as follows:

a. Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1; at a minimum, at least once every six months).

b. The application/system access remains appropriate for the function being performed.

c. Any inappropriate access is addressed.

d. Management acknowledges that access remains appropriate.

[Source: PCI DSS 7.2.5.1; PCI DSS v4.x: Targeted Risk Analysis Guidance]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-02.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.11 FedRAMP — Notify account managers and personnel or roles as defined in the SSP within:

1. Twenty-four hours when accounts are no longer required;

2. Eight hours when users are terminated or transferred; and

3. Eight hours when system usage or need-to-know changes for an individual.

[Source: FedRAMP Security Controls Baseline AC-2]

Discussion

Examples of system account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service. Identification of authorized system users and the specification of access privileges reflect the requirements in other controls in the security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access, including system owner, mission or business owner, senior agency information security officer, or senior agency official for privacy. Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts.

Where access involves personally identifiable information, security programs collaborate with the senior agency official for privacy to establish the specific conditions for group and role membership; specify authorized users, group and role membership, and access authorizations for each account; and create, adjust, or remove system accounts in accordance with organizational policies. Policies can include such information as account expiration dates or other factors that trigger the disabling of accounts. Organizations may choose to define access privileges or other attributes by account, type of account, or a combination of the two. Examples of other attributes required for authorizing access include restrictions on time of day, day of week, and point of origin. In defining other system account attributes, organizations consider system-related requirements and mission/business requirements. Failure to consider these factors could affect system availability.

Temporary and emergency accounts are intended for short-term use. Organizations establish temporary accounts as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may

bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts, including local logon accounts used for special tasks or when network resources are unavailable (may also be known as accounts of last resort). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include when shared/group, emergency, or temporary accounts are no longer required and when individuals are transferred or terminated. Changing shared/group authenticators when members leave the group is intended to ensure that former group members do not retain access to the shared or group account. Some types of system accounts may require specialized training.

TxDOT Discussion

NOTE: Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. [Source: CIS 6.2]

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202.22; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-162, 800-178, 800-192; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-03, AC-05, AC-06, AC-17, AC-18, AC-20, AU-02, AU-12, CM-05, IA-02, IA-04, IA-05, IA-08, MA-03, MA-05, PE-02, PL-04, PS-02, PS-04, PS-05, PS-07, PT-02, PT-03, SC-07, SC-12, SC-13, SI-04

AC-02(01) Automated System Account Management

Baselines

Moderate, High

Overlays

CJIS; Sensitive; FedRAMP Moderate, FedRAMP High

Requirements

Support the management of system accounts using automated mechanisms as defined in System Security Plans (SSPs).

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.01 CJIS — Support the management of system accounts using automated mechanisms including email, phone, and text notifications. [Source: CJIS AC-02(01)]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Automated system account management includes using automated mechanisms to create, enable, modify, disable, and remove accounts; notify account managers when an account is created, enabled, modified, disabled, or removed, or when users are terminated or transferred; monitor system account usage; and report atypical system account usage. Automated mechanisms can include internal system functions and email, telephonic, and text messaging notifications.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-162, 800-178, 800-192; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

AC-02(02) Automated Temporary and Emergency Account Management

Baselines

Low, Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Automatically disable temporary and emergency accounts after the period specified in Std.01.

Implementation Standards

Std.01 — Configure temporary accounts to automatically disable after a fixed duration not to exceed 30 days for high baseline systems and 60 days for moderate or low baselines. Configure emergency accounts to automatically disable after a period not to exceed 72 hours.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, AC-02(02) is superseded by CJIS requirement AC-02(02):

Std.04 CJIS — Automatically remove temporary and emergency accounts within 72 hours. [Source: CJIS AC-02(02)]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate baseline, the following standard applies:

Std.02 FedRAMP — Automatically disable temporary and emergency accounts after no more than 96 hours from last use. [Source: FedRAMP Security Controls Baseline AC-2(2)]

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.03 FedRAMP — Automatically disable temporary and emergency accounts after no more than 24 hours from last use. [Source: FedRAMP Security Controls Baseline AC-2(2)]

Discussion

Management of temporary and emergency accounts includes the removal or disabling of such accounts automatically after a predefined time period rather than at the convenience of the system administrator. Automatic removal or disabling of accounts provides a more consistent implementation.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-162, 800-178, 800-192; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

AC-02(03) Disable Accounts

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Disable accounts within the time periods specified in the TxDOT Identification and Authentication Standard when the accounts:

a. Have expired;

b. Are no longer associated with a user or individual;

c. Are in violation of organizational policy; or

d. Have been inactive for the time periods specified in the TxDOT Identification and Authentication Standard.

Implementation Standards

None.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 8.2.6.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-02(03).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standards apply:

Std.01 FedRAMP — The service provider defines the time period for user accounts, not to exceed twenty-four hours. [Source: FedRAMP Security Controls Baseline AC-2(3)]

Std.02 FedRAMP — The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the Joint Authorization Board (JAB)/Authorizing Official (AO). Where user management is a function of the service, reports of activity of consumer users shall be made available. [Source: FedRAMP Security Controls Baseline AC-2(3)]

Std.03 FedRAMP — The service provider defines the time period of inactivity for device identifiers, not to exceed thirty-five days. [Source: FedRAMP Security Controls Baseline AC-2(3)]

Discussion

Disabling expired, inactive, or otherwise anomalous accounts supports the concepts of least privilege and least functionality which reduce the attack surface of the system.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

For DoD clouds, see DoD cloud website for specific DoD requirements that go above and beyond FedRAMP https://public.cyber.mil/dccs/.

[Source: FedRAMP Security Controls Baseline AC-2(3)]

TxDOT References

Identification and Authentication Standard; Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-162, 800-178, 800-192; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

AC-02(04) Automated Audit Actions

Baselines

Moderate, High

Overlays

CJIS; Sensitive; FedRAMP Moderate, FedRAMP High

Requirements

Automatically audit account creation, modification, enabling, disabling, and removal actions.

Implementation Standards

Std.01 — Account management information sources includes systems, appliances, devices, services, and applications (including databases). Automated account management audit action results must be delivered in a format compliant with TxDOT requirements. Results must be unaltered, searchable, and made available to TxDOT Information Security.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-02(04).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Account management audit records are defined in accordance with AU-02 and reviewed, analyzed, and reported in accordance with AU-06.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-162, 800-178, 800-192; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AU-02, AU-06

AC-02(05) Inactivity Logout

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Require that users log out when unattended except as defined in the access control policy.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-02(05).

TX-RAMP Correspondence

For systems subject to TX-RAMP Level 2, the following standard applies:

Std.01 TX-RAMP — Require that users log out when anticipated time away exceeds fifteen minutes. [Source: TX-RAMP Manual AC-2(5)]

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate baseline.

For systems subject to FedRAMP requirements at the High baseline, the following additional standard applies:

Std.01 FedRAMP — Require that users log out when anticipated time away exceeds fifteen minutes. [Source: FedRAMP Security Controls Baseline AC-2(5)]

Discussion

Inactivity logout is behavior- or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Automatic enforcement of inactivity logout is addressed by AC-11.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-162, 800-178, 800-192; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-11, AT-02, PL-04

AC-02(07) Privileged User Accounts

Baselines

N/A

Overlays

TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Establish and administer privileged user accounts in accordance with a role-based access scheme;

b. Monitor privileged role or attribute assignments;

c. Monitor changes to roles or attributes; and

d. Revoke access when privileged role or attribute assignments are no longer appropriate.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. Privileged roles include key management, account management, database administration, system and network administration, and web administration. A role-based access scheme organizes permitted system access and privileges into roles. In contrast, an attribute-based access scheme specifies allowed system access and privileges based on attributes.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202.22; TX-RAMP Program Manual

Federal References

NIST SP 800-162, 800-178, 800-192; FedRAMP Security Controls Baseline

Related Controls

None.

AC-02(09) Restrictions on Use of Shared and Group Accounts

Baselines

N/A

Overlays

TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Only permit the use of shared and group accounts that meet conditions defined in the System Security Plan (SSP) for establishing shared and group accounts.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Before permitting the use of shared or group accounts, organizations consider the increased risk due to the lack of accountability with such accounts.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

TX-RAMP Program Manual; DIR Security Control Standards Catalog

Federal References

NIST SP 800-162, 800-178, 800-192; FedRAMP Security Controls Baseline

Related Controls

None.

AC-02(11) Usage Conditions

Baselines

N/A

Overlays

FedRAMP High

Requirements

Enforce system usage as defined in the System Security Plan (SSP) for all system accounts.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Specifying and enforcing usage conditions helps to enforce the principle of least privilege, increase user accountability, and enable effective account monitoring. Account monitoring includes alerts generated if the account is used in violation of organizational parameters. Organizations can describe specific conditions or circumstances under which system accounts can be used, such as by restricting usage to certain days of the week, time of day, or specific durations of time.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

AC-02(12) Account Monitoring for Atypical Usage

Baselines

N/A

Overlays

TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Monitor system accounts for atypical usage as defined in the System Security Plan (SSP); and

b. Report atypical usage of system accounts to account managers and personnel or roles as defined in the SSP.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baseline, the following standard applies:

Std.01 FedRAMP — For privileged accounts, monitor and report atypical usage of system accounts to, at a minimum, the ISSO or similar role within the organization. [Source: FedRAMP Security Controls Baseline AC-2(12)]

Discussion

Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals. Monitoring for atypical usage may reveal rogue behavior by individuals or an attack in progress. Account monitoring may inadvertently

create privacy risks since data collected to identify atypical usage may reveal previously unknown information about the behavior of individuals. Organizations assess and document privacy risks from monitoring accounts for atypical usage in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-162, 800-178, 800-192; FedRAMP Security Controls Baseline

Related Controls

AU-06, AU-07, CA-07, IR-08, SI-04

AC-02(13) Disable Accounts for High-risk Individuals

Baselines

Moderate, High

Overlays

CJIS; FedRAMP High

Requirements

Disable accounts of individuals within 30 minutes of discovery of evidence of increased risk.

Implementation Standards

Std.01 — Disable accounts immediately upon report of any indication of compromise as defined in the System Security Plan (see SI-04).

Std.02 — Re-enable accounts with additional protections as appropriate only after incident handling process is complete.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Disable accounts of individuals within 30 minutes of discovery of direct threats to the confidentiality, integrity, or availability of CJI. [Source: CJIS AC-02(13)]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Users who pose a significant security and/or privacy risk include individuals for whom reliable evidence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm. Such harm includes adverse impacts to organizational operations, organizational assets, individuals, other organizations, or the Nation. Close coordination among system administrators, legal staff, human resource managers, and authorizing officials is essential when disabling system accounts for high-risk individuals.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-162, 800-178, 800-192; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AU-06, SI-04

AC-03 Access Enforcement

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Implementation Standards

Std.01 — Rescinded in V2.4.

Std.02 — Rescinded in V2.4.

Std.03 — Restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Std.04 — If encryption is used as an access control mechanism, it must meet TxDOT approved encryption standards (see SC-13).

Std.05 — Prevent access to organization-defined security-relevant information except during secure, non-operable system states.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.06 PCI — All non-console administrative access is encrypted using strong cryptography. [Source: PCI DSS 2.2.7]

Std.07 PCI — moved to IA-02 in V3.0.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-03.

Std.08 CJIS — Rescinded in V4.0.

Std.09 CJIS — Rescinded in V4.0.

Std.10 CJIS — Rescinded in V4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. In addition to enforcing authorized access at the system level and recognizing that systems can host many applications and services in support of mission and business functions, access enforcement mechanisms can also be employed at the application and service level to provide increased information security and privacy. In contrast to logical access controls that are implemented within the system, physical access controls are addressed by the controls in the Physical and Environmental Protection (PE) family.

TxDOT Discussion

Security-relevant information is any information within the system that can potentially impact the operation of security functions in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Secure, non-operable system states are states in which the system is not performing mission/business-related processing (for example, the system is offline for maintenance, troubleshooting, bootup, and shutdown).

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

Privacy Act; OMB A-130; NIST SP 800-57-1, 800-57-2, 800-57-3, 800-162, 800-178; NIST IR 7874; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-02, AC-04, AC-05, AC-06, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AT-02, AT-03, AU-09, CA-09, CM-05, CM-11, IA-02, IA-05, IA-06, IA-07, IA-11, MA-03, MA-04, MA-05, MP-04, PM-02, PS-03, PT-02, PT-03, SA-17, SC-02, SC-03, SC-04, SC-12, SC-13, SC-28, SI-04, SI-08

AC-03(14) Individual Access

Baselines

N/A

Overlays

CJIS

Requirements

Provide automated or manual processes to enable individuals to have access to the following elements of their personally identifiable information: organization-defined elements.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-03(14).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Individual access affords individuals the ability to review personally identifiable information about them held within organizational records, regardless of format. Access helps individuals to develop an understanding about how their personally identifiable information is being processed. It can also help individuals ensure that their data is accurate. Access mechanisms can include request forms and application interfaces. For federal agencies, PRIVACT processes can be located in systems of record notices and on agency websites. Access to certain types of records may not be appropriate (e.g., for federal agencies, law enforcement records within a system of records may be exempt from disclosure under the PRIVACT) or may require certain levels of authentication assurance. Organizational personnel consult with the senior agency official for privacy and legal counsel to determine appropriate mechanisms and access rights or limitations.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

CJIS Security Policy

Related Controls

IA-08, PM-20, PM-21, PM-22

AC-04 Information Flow Enforcement

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on information flow control policies as defined in System Security Plans (SSPs), Information Security Architecture, and Information Security Agreements (ISAs).

Implementation Standards

Std.01 — Ensure that only the required information, and not more, is communicated.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.02 CJIS — Enforce approved authorizations for controlling the flow of information within the system and between connected systems by preventing CJI from being transmitted unencrypted across the public network, blocking outside traffic that claims to be from within the agency, and not passing any web requests to the public network that are not from the agency-controlled or internal boundary protection devices (e.g., proxies, gateways, firewalls, or routers). [Source: CJIS AC-04]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Information flow control regulates where information can travel within a system and between systems (in contrast to who is allowed to access the information) and without regard to subsequent accesses to that information. Flow control restrictions include blocking external traffic that claims to be from within the organization, keeping export-controlled information from being transmitted in the clear to the Internet, restricting web requests that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between organizations may require an agreement

specifying how the information flow is enforced (see CA-03). Transferring information between systems in different security or privacy domains with different security or privacy policies introduces the risk that such transfers violate one or more domain security or privacy policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between connected systems. Organizations consider mandating specific architectural solutions to enforce specific security and privacy policies. Enforcement includes prohibiting information transfers between connected systems (i.e., allowing access only), verifying write permissions before accepting information from another security or privacy domain or connected system, employing hardware mechanisms to enforce one-way information flows, and implementing trustworthy regrading mechanisms to reassign security or privacy attributes and labels.

Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within systems and between connected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content. Organizations also consider the trustworthiness of filtering and/or inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 03 through 32 primarily address cross-domain solution needs that focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, such as high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf products. Information flow enforcement also applies to control plane traffic (e.g., routing and DNS).

TxDOT Discussion

Information control enforcement measures may include, but are not limited to, the following:

1. Access control lists (ACL);

2. Documented business justifications for the use of all services, protocols, and ports allowed;

3. Explicit security attributes on information, source, and destination objects;

4. Demilitarized zones (DMZ) implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports;

5. Anti-spoofing measures implemented if feasible to detect and block forged source IP addresses from entering the network;

6. Implementing stateful inspection (dynamic packet filtering);

7. Placing system components that store PII within in internal network zone, segregated from the DMZ and any untrusted networks; and

8. Prohibiting private IP addresses and routing information from being disclosed to unauthorized parties.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP-800-160-1, 800-162, 800-178; NIST IR 8112; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-03, AC-06, AC-17, AC-19, AC-21, AU-10, CA-03, CA-09, CM-07, PL-09, SA-17, SC-04, SC-07

AC-04(04) Flow Control of Encrypted Information

Baselines

N/A

Overlays

FedRAMP High

Requirements

Prevent encrypted information from bypassing procedures or methods as defined in the System Security Plan (SSP).

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.01 FedRAMP — The service provider must support Agency requirements to comply with M-21-31 (https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf) and M-22-09 (https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf). [Source: FedRAMP Security Controls Baseline AC-4(4)]

Discussion

Flow control mechanisms include content checking, security policy filters, and data type identifiers. The term encryption is extended to cover encoded data not recognized by filtering mechanisms.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

SI-04

AC-04(21) Physical or Logical Separation of Information Flows

Baselines

N/A

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

Separate information flows logically or physically using mechanisms and/or techniques as defined in the System Security Plan (SSP) to accomplish required separations by types of information as defined in the SSP.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Enforcing the separation of information flows associated with defined types of data can enhance protection by ensuring that information is not commingled while in transit and by enabling flow control by transmission paths that are not otherwise achievable. Types of separable information include inbound and outbound communications traffic, service requests and

responses, and information of differing security impact or classification levels.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

AC-05 Separation of Duties

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Identify and document duties of user types in the System Security Plan (SSP); and

b. Define system access authorizations to support separation of duties.

Implementation Standards

Std.01 — Rescinded in V2.2.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.02 PCI — Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed. [Source: PCI DSS 6.5.4]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Rescinded in V4.0.

Std.04 CJIS — Identify and document separation of duties based on specific duties, operations, or information systems, as necessary, to mitigate risk to CJI. [Source: CJIS AC-05]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of systems and system components when developing policy on separation of duties. Separation of duties is enforced through the account management activities in AC-02, access control mechanisms in AC-03, and identity management activities in IA-02, IA-04, and IA-12.

TxDOT Discussion

It is recommended to separate administration/operation, management/allocations, and audit/testing functions, and separate responsibilities for critical system functions among different individuals.

Examples of functions and sub-functions that should be considered for assignment to different individuals include:

1. Data Creation and Control Functions:

a. Data collection and preparation;

b. Data entry;

NOTE: Input of transactions that may result in a conflict of interest, fraud, abuse, or direct financial loss (for example, input of vendor invoices and purchasing and receiving information) shall be separated.

c. Data verification, reconciliation of output and approval; and

d. Database administration.

2. Software Development and Maintenance Functions:

a. Applications programming;

b. Design review;

c. Application testing and evaluation; and

d. Application maintenance.

3. Security Functions:

a. Security implementation; and

b. Review of security controls, security audits, and audit trail review.

Note for systems subject to FedRAMP Requirements:

Cloud Service Providers (CSPs) have the option to provide a separation of duties matrix as an attachment to the SSP. [Source: FedRAMP Security Controls Baseline AC-5]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-02, AC-03, AC-06, AU-09, CM-05, CM-11, CP-09, IA-02, IA-04, IA-05, IA-12, MA-03, MA-05, PM-02, PS-02, SA-08, SA-17

AC-06 Least Privilege

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Implementation Standards

Std.01 —

a. An access control model is defined and includes granting access as follows:

1. Appropriate access depending on the entity's business and access needs.

2. Access to system components and data resources that is based on users' job classification and functions.

3. The least privileges required (for example, user, administrator) to perform a job function.

[Source: PCI DSS 7.2.1]

b. Access is assigned to users, including privileged users, based on:

1. Job classification and function.

2. Least privileges necessary to perform job responsibilities.

[Source: PCI DSS 7.2.2]

c. Required privileges are approved by authorized personnel. [Source: PCI DSS 7.2.3]

Std.03 —

a. Sensitive, Confidential, or Regulated information shall be accessible only to authorized users.

b. An information file or record containing any confidential information shall be identified, documented, and protected in its entirety.

c. Information resources assigned from or shared between one state organization to another or from or between a state organization to a contractor or other third party, at a minimum, shall be protected in accordance with the conditions imposed by the providing state organization. [Source: DIR Control Standards Catalog AC-6]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 7.2.1, 7.2.2, and 7.2.3.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.04 PCI — All application and system accounts and related access privileges are assigned and managed as follows:

a. Based on the least privileges necessary for the operability of the system or application.

b. Access is limited to the systems, applications, or processes that specifically require their use.

[Source: PCI DSS 7.2.5]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-06.

Std.02 CJIS — Rescinded in V4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations consider the creation of additional processes, roles, and accounts as necessary to achieve least privilege. Organizations apply least privilege to the development, implementation, and operation of organizational systems.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-02, AC-03, AC-05, CM-05, CM-11, PL-02, PM-12, SA-08, SA-15, SA-17

AC-06(01) Authorize Access to Security Functions

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Authorize access for personnel or roles as defined in System Security Plans (SSPs) to:

a. Security functions (deployed in hardware, software, and firmware) as defined in SSPs; and

b. Security-relevant information as defined in Std.01.

Implementation Standards

Std.01 — At a minimum, explicitly authorize access (based on role) to the following list of security functions and security-relevant information:

a. Setting/modifying audit logs and auditing behavior;

b. Setting/modifying boundary protection system rules;

c. Configuring/modifying access authorizations (that is, permissions, privileges);

d. Setting/modifying authentication parameters; and

e. Setting/modifying system configurations and parameters.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.03 CJIS — Authorize access for personnel including security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information security personnel, maintainers, system programmers, etc.) to established system accounts, configured access authorizations (i.e., permissions, privileges), set events to be audited, set intrusion detection parameters, and other security functions. [Source: CJIS AC-06(01)]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate baseline.

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.02 FedRAMP — Authorize access for personnel or roles as defined in System Security Plans (SSPs) to:

a. All functions not publicly accessible; and

b. All security-relevant information not publicly available.

[Source: FedRAMP Security Controls Baseline AC-6(1)]

Discussion

Security functions include establishing system accounts, configuring access authorizations (i.e., permissions, privileges), configuring settings for events to be audited, and establishing intrusion detection parameters. Security-relevant information includes filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, and access control lists. Authorized personnel include security administrators, system administrators, system security officers, system programmers, and other privileged users.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-17, AC-18, AC-19, AU-09, PE-02

AC-06(02) Non-privileged Access for Nonsecurity Functions

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Require that users of system accounts (or roles) with access to any security functions or security-relevant information use non-privileged accounts or roles, when accessing nonsecurity functions.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-06(02).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Requiring the use of non-privileged accounts when accessing nonsecurity functions limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies, such as role-based access control, and where a change of role provides the same degree of assurance in the change of access authorizations for the user and the processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

Examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions. [Source: FedRAMP Security Controls Baseline AC-6(2)]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-17, AC-18, AC-19, PL-04

AC-06(03) Network Access to Privileged Commands

Baselines

N/A

Overlays

FedRAMP High

Requirements

Authorize network access to all privileged commands only for compelling operational needs and document the rationale for such access in the security plan for the system.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device).

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

AC-17, AC-18, AC-19

AC-06(05) Privileged Accounts

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Restrict privileged accounts on the system to personnel or roles requiring privileged access, as defined in the System Security Plan (SSP).

Implementation Standards

Std.01 — Restrict privileged accounts to the minimum number required. Limit super-user/root privileges to the maximum extent possible.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-06(05).

Std.02 CJIS — Rescinded in V4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from accessing privileged information or privileged functions. Organizations may differentiate in the application of restricting privileged accounts between allowed privileges for local accounts and for domain accounts provided that they retain the ability to control system configurations for key parameters and as otherwise necessary to sufficiently mitigate risk.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

IA-02, MA-03, MA-04

AC-06(07) Review of User Privileges

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Review at least annually the privileges assigned to roles or classes of users as defined in the System Security Plan (SSP) to validate the need for such privileges; and

b. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-06(07).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

The need for certain assigned user privileges may change over time to reflect changes in organizational mission and business functions, environments of operation, technologies, or threats. A periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CA-05, CA-07

AC-06(08) Privilege Levels for Code Execution

Baselines

N/A

Overlays

FedRAMP High

Requirements

Prevent the following software from executing at higher privilege levels than users executing the software: any software except software explicitly documented.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

In certain situations, software applications or programs need to execute with elevated privileges to perform required functions. However, depending on the software functionality and configuration, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications or programs, those users may indirectly be provided with greater privileges than assigned.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

AC-06(09) Log Use of Privileged Functions

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Log the execution of privileged functions.

Implementation Standards

Std.01 — Ensure that applications produce audit records containing sufficient information to identify the actor, time of action, type of action, and which component, feature, or function of the application was accessed.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-06(09).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging and analyzing the use of privileged functions is one way to detect such misuse and, in doing so, help mitigate the risk from insider threats and the advanced persistent threat.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AU-02, AU-03, AU-12

AC-06(10) Prohibit Non-privileged Users from Executing Privileged Functions

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Prevent non-privileged users from executing privileged functions.

Implementation Standards

Std.01 — Limit system access to the types of transactions and functions that authorized users are permitted to execute, either by specific account or by account type.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-06(10).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Privileged functions include disabling, circumventing, or altering implemented security or privacy controls, establishing system accounts, performing system integrity checks, and administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Privileged functions that require protection from non-privileged users include circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms. Preventing non-privileged users from executing privileged functions is enforced by AC-03.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

AC-07 Unsuccessful Logon Attempts

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Enforce a limit of, as identified in the TxDOT Identification and Authentication Standard (Lockout Threshold), a number of consecutive invalid logon attempts by a user during a period as defined in the Lockout Threshold; and

b. Automatically lock the account or node in accordance with the TxDOT Identification and Authentication Standard when the maximum number of unsuccessful attempts is exceeded.

Implementation Standards

Std.01 — Rescinded in V2.2.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, AC-07a. is superseded by PCI DSS requirement 8.3.4:

Std.02 PCI — Invalid authentication attempts are limited by:

a. Locking out the user ID after not more than 10 attempts.

b. Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.

[Source: PCI DSS 8.3.4]

CJIS Correspondence

For systems processing CJIS data, AC-07b is superseded by CJIS requirement AC-07:

Std.03 CJIS — Rescinded in V4.0.

Std.04 CJIS — Automatically lock the account or node until released by an administrator when the maximum number of unsuccessful attempts is exceeded. [Source: CJIS AC-07]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

The need to limit unsuccessful logon attempts and take subsequent action when the maximum number of attempts is exceeded applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are usually temporary and automatically release after a predetermined, organization-defined time period. If a delay algorithm is selected, organizations may employ different algorithms for different components of the system based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at the operating system and the application levels. Organization-defined actions that may be taken when the number of allowed consecutive invalid logon attempts is exceeded include prompting the user to answer a secret question in addition to the username and password, invoking a lockdown mode with limited user capabilities (instead of full lockout), allowing users to only logon from specified Internet Protocol (IP) addresses, requiring a CAPTCHA to prevent automated attacks, or applying user profiles such as location, time of day, IP address, device, or Media Access Control (MAC) address. If automatic system lockout or execution of a delay algorithm is not implemented in support of the availability objective, organizations consider a combination of other actions to help prevent brute force attacks. In addition to the above, organizations can prompt users to respond to a secret question before the number of allowed unsuccessful logon attempts is exceeded. Automatically unlocking an account after a specified period of time is generally not permitted. However, exceptions may be required based on operational mission or need.

TxDOT Discussion

Configure information systems in accordance with the Identification and Authentication Standard. This standard includes the possibility of an exponential growth method for lockouts. An example lockout plan is presented below:

1. For systems categorized as Low, configure the information system to lock out the user account automatically after ten (10) consecutive invalid login attempts during a 15-minute time period. Require the lockout to persist for a minimum of 15 minutes unless released by an administrator.

2. For systems categorized as Moderate, configure the information system to lock out the user account automatically after three (3) consecutive invalid login attempts during a 60-minute time period. Require the lockout to persist for a minimum of 30 minutes unless released by an administrator.

NOTE: Users may contact TxDOTNow to release the user account prior to the lockout's expiration if the lockout hinders productivity.

3. For systems categorized as High, configure the information system to lock out the user account automatically after three (3) consecutive invalid login attempts during a 120-minute time period. Require the lockout to persist until released by an administrator.

4. For any computing device that accesses or stores TxDOT Sensitive, Confidential, or Regulated Information, lock out the user after three (3) invalid login attempts during a fifteen-minute period and after 15 minutes of user inactivity.

5. For cloud service providers, providers configure the information system to:

a. Enforce a limit of not more than three (3) consecutive invalid login attempts by a user during a 15-minute time period; and

b. Automatically lock the account/node for 30 minutes when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.

State Implementation Details

1. As technology permits, state agencies must designate at least one threshold activated by invalid logon attempts (i.e., item a from the control description, an agency-defined number of invalid logon attempts by a user account within an agency-defined time-period).

2. As technology permits, state agencies must define, implement, and enforce at least one automatic action that occurs when an agency-defined threshold for invalid logon attempts has been reached (i.e., item b from the control description).

3. In designing and implementing access controls for information systems, state agencies should apply a risk-based approach that considers some or all of the following criteria:

a. Capabilities and features of the system;

b. The level of risk presented by the system;

c. Successful application and enforcement of other security controls, such as multifactor authentication, password entropy, and maturity of other authenticator management practices relevant to the information system;

d. The ability to detect and mitigate the risk of other types of attacks focused on authentication (e.g., "account spraying" attacks in which threat actors attempt to access multiple accounts from the same IP address or set of IP addresses without causing many failed logon attempts against each individual account targeted by the threat actors);

e. Whether the system is accessible from the Internet or other public or broadly accessible network(s);

f. Impacts to the agency's users, operations, and support resources if automatic account lockout controls are abused by threat actors to the determent of account or system availability; and

g. The application of more rigorous controls commensurate to the value and potential for abuse of a type of account (e.g., applying additional controls, enhancements, or overlays to privileged accounts).[Source: DIR Control Standards Catalog AC-7]

TxDOT References

Identification and Authentication Standard; Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-63-3, 800-124; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-02, AU-02, AU-06, IA-05

AC-07(02) Purge or Wipe Mobile Device

Baselines

N/A

Overlays

CJIS

Requirements

Purge or wipe information from organization-controlled mobile devices based on purging or wiping requirements and techniques as specified by the TxDOT-defined mobile device management solutions after the number, as defined in the TxDOT Identification and Authentication Standard, of consecutive, unsuccessful device logon attempts.

Implementation Standards

Std.01 — Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise. [Source: CIS 4.11]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirements 5.20.2 and 5.20.7.3.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

A mobile device is a computing device that has a small form factor such that it can be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Purging or wiping the device applies only to mobile devices for which the organization-defined number of unsuccessful logons occurs. The logon is to the mobile device, not to any one account on the device. Successful logons to accounts on mobile devices reset the unsuccessful logon count to zero. Purging or wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms.

TxDOT Discussion

None.

TxDOT References

Identification and Authentication Standard; Information Security and Privacy Policy

State References

None.

Federal References

NIST SP 800-63-3, 800-124; PCI DSS; CJIS Security Policy

Related Controls

AC-19, MP-05, MP-06

AC-08 System Use Notification

Baselines

Low, Moderate, High

Overlays

CJIS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Display the official TxDOT System Use Notification to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:

1. Users are accessing a TxDOT system;

2. System usage may be monitored, recorded, and subject to audit;

3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and

4. Use of the system indicates consent to monitoring and recording;

b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and

c. For publicly accessible systems:

1. Display system use information unless and until the user takes positive action (for example, clicking a button indicating "OK") to acknowledge agreement, before granting further access to the publicly accessible system;

2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

3. Include a description of the authorized uses of the system.

Implementation Standards

Std.01 — Rescinded in V2.4.

Std.02 — Agency information resources designated for use by the public shall be configured to enforce security policies and procedures without requiring user participation or intervention. Information resources must require the acceptance of a banner or notice prior to use. [Source: 1 TAC 202.22(a)(4)]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-08.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, and High baselines, the following standards apply:

Std.03 FedRAMP — The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the Joint Authorization Board (JAB)/Authorizing Official (AO). [Source: FedRAMP Security Controls Baseline AC-8]

Std.04 FedRAMP — The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the Joint Authorization Board (JAB)/Authorizing Official (AO). [Source: FedRAMP Security Controls Baseline AC-8]

Std.05 FedRAMP — If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the Joint Authorization Board (JAB)/Authorizing Official (AO). [Source: FedRAMP Security Controls Baseline AC-8]

Discussion

System use notifications can be implemented using messages or warning banners displayed before individuals log in to systems. System use notifications are used only for access via logon interfaces with human users. Notifications are not required when human interfaces do not exist. Based on an assessment of risk, organizations consider whether or not a secondary system use notification is needed to access applications or other system resources after the initial network logon. Organizations consider system use notification messages or banners displayed in multiple languages based on organizational needs and the demographics of system users. Organizations consult with the privacy office for input regarding privacy messaging and the Office of the General Counsel or organizational equivalent for legal review and approval of warning banner content.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided. [Source: FedRAMP Security Controls Baseline AC-8]

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202.22; DIR Security Control Standards Catalog

Federal References

CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-14, PL-04, SI-04

AC-10 Concurrent Session Control

Baselines

N/A

Overlays

FedRAMP High

Requirements

Limit the number of concurrent sessions for each user account to three (3) sessions for privileged access and two (2) sessions for non-privileged access.

Implementation Standards

Std.01 — Rescinded in V4.0.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.02 FedRAMP — Limit the number of concurrent sessions for each user account to three (3) sessions for privileged access and two (2) sessions for non-privileged access. [Source: FedRAMP Security Controls Baseline AC-10]

Discussion

Organizations may define the maximum number of concurrent sessions for system accounts globally, by account type, by account, or any combination thereof. For example, organizations may limit the number of concurrent sessions for system administrators or other individuals working in particularly sensitive domains or mission-critical applications. Concurrent session control addresses concurrent sessions for system accounts. It does

not, however, address concurrent sessions by single users via multiple system accounts.

TxDOT Discussion

None.

TxDOT References

None.

State References

DIR Security Control Standards Catalog

Federal References

FedRAMP Security Controls Baseline

Related Controls

SC-23

AC-11 Device Lock

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Prevent further access to the system by initiating a device lock after a maximum of 30 minutes of inactivity or upon receiving a request from a user; and

b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

Implementation Standards

Std.01 — On any system categorized as Moderate or High, the period of inactivity must be no more than 15 minutes before session lock occurs for remote and mobile devices.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.03 CJIS — Prevent further access to the system by initiating a device lock after a maximum of 30 minutes of inactivity and requiring the user to initiate a device lock before leaving the system unattended. [Source: CJIS AC-11]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.02 FedRAMP — Prevent further access to the system by initiating a device lock after fifteen minutes of inactivity, and requiring the user to initiate a device lock before leaving the system unattended. [Source: FedRAMP Security Controls Baseline AC-11]

Discussion

Device locks are temporary actions taken to prevent logical access to organizational systems when users stop work and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences. Device locks can be implemented at the operating system level or at the application level. A proximity lock may be used to initiate the device lock (e.g., via a Bluetooth-enabled device or dongle). User-initiated device locking is behavior or policy-based and, as such, requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging out of systems, such as when organizations require users to log out at the end of workdays.

TxDOT Discussion

TxDOT systems should be configured such that inputs and outputs are treated as activity regardless of format, such that, for example, screens do not automatically blank when speech-to-text is used in place of keyboard entry.

The same degree of privacy of input and output shall be provided to all individuals. When speech output required by 402.2 is enabled, the screen shall not blank automatically. [Source: Section 508 of the Rehabilitation Act, as amended; 405.1]

ICT with a display screen shall be speech-output enabled for full and independent use by individuals with vision impairments. [Source: Section 508 of the Rehabilitation Act, as amended; 402.2]

Notes for systems subject to CJIS requirements:

In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e., receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement. [Source: CJIS 5.5: AC-11]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

Section 508 of the Rehabilitation Act; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-02, AC-07, IA-11, PL-04

AC-11(01) Pattern-hiding Displays

Baselines

Moderate, High

Overlays

CJIS; Sensitive; FedRAMP Moderate, FedRAMP High

Requirements

Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

Implementation Standards

Std.01 — Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity. [Source: SP 800-171 3.1.10]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-11(01).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

The pattern-hiding display can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

AC-12 Session Termination

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Automatically terminate a user session after the user logs out of the system or removes the token (authenticator), or after a period of inactivity identified in Std.03.

Implementation Standards

Std.01 — For moderate and high-baseline systems, configure applications to terminate user sessions and require user re-authentication in accordance with the TxDOT Identification and Authentication Standard.

Std.02 — For Web and mobile applications, avoid non-expiring session cookies.

Std.03 — For Web and mobile applications, set idle session termination in accordance with the TxDOT Identification and Authentication Standard.

Std.04 — For Web and mobile applications, new sessions should be generated each time a user is authenticated.

Std.05 — For Web and mobile applications, sessions should be destroyed when a user logs out.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, Imp. Std.03 is superseded by PCI DSS requirement 8.2.8:

Std.06 PCI — If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session. [Source: PCI DSS 8.2.8]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-12.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Session termination addresses the termination of user-initiated logical sessions (in contrast to SC-10, which addresses the termination of network connections associated with communications sessions (i.e., network disconnect)). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated without terminating network sessions. Session termination ends all processes associated with a user's logical session except for those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events that require automatic termination of the session include organization-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on system use.

TxDOT Discussion

None.

TxDOT References

Identification and Authentication Standard; Information Security and Privacy Policy

State References

TX-RAMP Program Manual

Federal References

PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CM-02, MA-04, SC-10, SC-23

AC-14 Permitted Actions Without Identification or Authentication

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Identify specific user actions that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and

b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Define stipulations in the System Security Plan (SSP) for bypassing identification and authentication mechanisms to facilitate operations in emergency situations.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-14.

Std.03 CJIS — Rescinded in V4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Specific user actions may be permitted without identification or authentication if organizations determine that identification and authentication are not required for the specified user actions. Organizations may allow a limited number of user actions without identification or authentication, including when individuals access public websites or other publicly accessible federal systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations identify actions that normally require identification or authentication but may, under certain circumstances, allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. Permitting actions without identification or authentication does not apply to situations where identification and authentication have already occurred and are not repeated but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational systems without identification and authentication, and therefore, the value for the assignment operation can be "none."

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-08, IA-02, PL-02

AC-17 Remote Access

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorize each type of remote access to the system prior to allowing such connections.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — All remote access connections must be authorized prior to allowing such connections. [Source: DIR Control Standards Catalog AC-17]

Std.03 — Configurations Requirement:

a. All remote access to the network must use an organization-approved encrypted connection in compliance with SC-13.

b. Multi-factor authentication is required for all remote access. See the TxDOT Identification and Authentication Standard for further guidance.

Std.04 — Usage Restrictions:

a. Use only organization-authorized and -approved devices for remote access to organization non-public systems;

b. Take every reasonable effort to ensure the confidentiality, integrity, and availability of information and information systems used remotely (for example, not leaving laptops and other devices unattended or in public plain view); and

c. Users must understand their responsibilities for protecting Sensitive, Confidential, or Regulated data and the consequences for mishandling such data.

Std.05 — Implementation Guidance:

a. When employing multi-factor authentication for remote access to information systems, ensure that it complies with the TxDOT Identification and Authentication Standard;

b. Approved devices remotely connecting to the organization network must have a VPN client installed, with an organization issued VPN certificate;

c. Implement adequate security measures (e.g., virus, malware, and spam protection, firewall, intrusion detection) on client computers prior to allowing VPN remote access;

d. Virtual desk applications shall be securely configured to minimize the ability of users to copy data;

e. The information system shall use automated functions to monitor and control remote access methods;

f. Systems shall log all remote access occurrences, including both end user and administrator activity user credential, date/time, and duration of connection at a minimum); and

g. Route all remote accesses through managed network access control points. Limiting the number of access control points for remote accesses reduces the attack surface for organizations.

Std.06 — The ISO shall authorize the execution of privileged commands and access to security-relevant information, e.g. logging into a firewall device for administrative functions. Remote access under these conditions shall be authorized only for compelling operational needs and the agency shall document the rationale for such access. Such actions shall be logged and audited.

PCI DSS Correspondence

Std.07 PCI — Rescinded in V3.0.

For systems processing PCI DSS data, or that support PCI DSS processes, Std.05d. is superseded by PCI DSS requirement 3.4.2:

Std.08 PCI — When using remote-access technologies, technical controls prevent copy and/or relocation of primary account number (PAN) for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need. [Source: PCI DSS 3.4.2]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-17.

Std.09 CJIS — Rescinded in V4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Remote access is access to organizational systems (or processes acting on behalf of users) that communicate through external networks such as the Internet. Types of remote access include dial-up, broadband, and wireless. Organizations use encrypted virtual private networks (VPNs) to enhance confidentiality and integrity for remote connections. The use of encrypted VPNs provides sufficient assurance to the organization that it can effectively treat such connections as internal networks if the cryptographic mechanisms used are implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. VPNs with encrypted tunnels can also affect the ability to adequately monitor network communications traffic for malicious code. Remote access controls apply to systems other than public web servers or systems designed for public access. Authorization of each remote access type addresses authorization prior to allowing remote access without specifying the specific formats for such authorization. While organizations may use information exchange and system connection security agreements to manage remote access connections to other systems, such agreements are addressed as part of CA-03. Enforcing access restrictions for remote access is addressed via AC-03.

TxDOT Discussion

None.

TxDOT References

Identification and Authentication Standard; Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-46, 800-77, 800-113, 800-114, 800-121; NIST IR 7966; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-02, AC-03, AC-04, AC-18, AC-19, AC-20, CA-03, CM-10, IA-02, IA-03, IA-08, MA-04, PE-17, PL-02, PL-04, SC-10, SC-12, SC-13, SI-04

AC-17(01) Monitoring and Control

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Employ automated mechanisms to monitor and control remote access methods.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirements AC-17(01) and 5.20.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Monitoring and control of remote access methods allows organizations to detect attacks and help ensure compliance with remote access policies by auditing the connection activities of remote users on a variety of system components, including servers, notebook computers, workstations, smart phones, and tablets. Audit logging for remote access is enforced by AU-02. Audit events are defined in AU-02a.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-46, 800-77, 800-113, 800-114, 800-121; NIST IR 7966; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AU-02, AU-06, AU-12

AC-17(02) Protection of Confidentiality and Integrity Using Encryption

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Implementation Standards

Std.01 — Encryption for all remote access sessions over networks outside TxDOT's authorization boundaries must comply with SC-13.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-17(02).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Virtual private networks can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol that provides end-to-end communications security over networks and is used for Internet communications and online transactions.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-46, 800-77, 800-113, 800-114, 800-121; NIST IR 7966; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

SC-08, SC-12, SC-13

AC-17(03) Managed Access Control Points

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Route remote accesses through authorized and managed network access control points.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-17(03).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organizations consider the Trusted Internet Connections (TIC) initiative DHS TIC requirements for external network connections since limiting the number of access control points for remote access reduces attack surfaces.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-46, 800-77, 800-113, 800-114, 800-121; NIST IR 7966; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

SC-07

AC-17(04) Privileged Commands and Access

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: compelling operational needs; and

b. Document the rationale for remote access in the security plan for the system.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-17(04).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Remote access to systems represents a significant potential vulnerability that can be exploited by adversaries. As such, restricting the execution of privileged commands and access to security-relevant information via remote access reduces the exposure of the organization and the susceptibility to threats by adversaries to the remote access capability.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-46, 800-77, 800-113, 800-114, 800-121; NIST IR 7966; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-06, CA-05, SC-12, SC-13

AC-17(09) Disconnect or Disable Access

Baselines

Moderate, High

Overlays

Sensitive; TX-RAMP Level 2

Requirements

Provide the capability to disconnect or disable remote access to the system within the periods defined in Stds.02 & 03.

Implementation Standards

Std.01 — Terminate or suspend network connections (that is, system-to-system interconnections) upon issuance of an order by the TxDOT CIO, CISO, or Senior Official for Privacy (SOP).

Std.02 — High baseline systems must have the capability to be disconnected within 10 minutes.

Std.03 — Moderate baseline systems must have the capability to be disconnected within 20 minutes.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 requirements.

For systems subject to TX-RAMP Level 2, the following standard applies:

Std.04 TX-RAMP — Systems must have the capability to be disconnected within 15 minutes. [Source: TX-RAMP Manual AC-17(9)]

FedRAMP Correspondence

None.

Discussion

The speed of system disconnect or disablement varies based on the criticality of missions or business functions and the need to eliminate immediate or future remote access to systems.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-46, 800-77, 800-113, 800-114, 800-121; NIST IR 7966

Related Controls

CP-02

AC-18 Wireless Access

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and

b. Authorize each type of wireless access to the system prior to allowing such connections.

Implementation Standards

Std.01 — TxDOT, as a state agency, shall establish the requirements and security restrictions for installing or providing access to the state agency's information resources systems. The wireless policy shall address the following topic areas:

a. Wireless Local Area Networks. Ensure that Service Set Identifiers (SSID) values are changed from the manufacturer default setting.

b. Transmitting and Encrypting Information. Types of information that may be transmitted via wireless networks and devices with or without encryption including mission critical information or sensitive personal information. TxDOT shall not transmit confidential information via a wireless connection to or from a portable computing device unless secure encryption protocols that meet appropriate protection or certification standards as detailed within this Security Control Standards Catalog, are used to protect the information.

c. Installation or Use of Wireless Personal Area Networks. Prohibit and periodically monitor any unauthorized installation or use of Wireless Personal

Area Networks on state agency IT systems by individuals without the approval of the state agency information resources manager. [Source: DIR Control Standards Catalog AC-18]

Std.02 — Vendor default accounts are managed as follows:

a. If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6.

b. If the vendor default account(s) will not be used, the account is removed or disabled.

[Source: PCI DSS 2.2.2]

Std.03 — Authorized and unauthorized wireless access points are managed as follows:

a. The presence of wireless (Wi-Fi) access points is tested for,

b. All authorized and unauthorized wireless access points are detected and identified,

c. Testing, detection, and identification occurs at least once every three months.

d. If automated monitoring is used, personnel are notified via generated alerts.

[Source: PCI DSS 11.2.1]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 2.2.2 and 11.2.1.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.04 PCI —

a. For wireless environments connected to the Cardholder Data Environment (CDE) or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to:

1. Default wireless encryption keys.

2. Passwords on wireless access points.

3. SNMP defaults.

4. Any other security-related wireless vendor defaults.

[Source: PCI DSS 2.3.1]

b. For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows:

1. Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary.

2. Whenever a key is suspected of or known to be compromised.

[Source: PCI DSS 2.3.2]

c. Wireless networks transmitting a primary account number (PAN) or connected to the Cardholder Data Environment (CDE) use industry best practices to implement strong cryptography for authentication and transmission. [Source: PCI DSS 4.2.1.2]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirements AC-18 and 5.20.

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.05 CJIS — For all agency-managed wireless access points (APs) with access to an agency's network that processes unencrypted CJI:

a. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other available privacy features.

b. Disable the broadcast SSID feature so that the client SSID must match that of the AP.

c. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.

d. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired

infrastructure. Limit access between wireless networks and the wired network to only operational needs. [Source: CJIS 5.20.1.1]

Std.06 CJIS — Organizational security policy shall be used to dictate the use of Bluetooth and its associated devices based on the agency's operational and business processes. [Source: CJIS 5.20.1.3]

Std.07 CJIS — Organizations shall, at a minimum, ensure that wireless devices:

a. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in System and Information Integrity (SI).

b. Are configured for local device authentication (see Section 5.20.7.1).

c. Use advanced authentication or CSO-approved compensating controls as per Section 5.20.7.2.1.

d. Encrypt all CJI resident on the device.

e. Erase cached information, to include authenticators (see Identification and Authentication (IA)) in applications, when session is terminated.

f. Employ personal firewalls on full-featured operating system devices or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.

g. Employ malicious code protection on full-featured operating system devices or run a MDM system that facilitates the ability to provide anti-malware services from the agency level. [Source: CJIS 5.20.3]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Wireless technologies include microwave, packet radio (ultra-high frequency or very high frequency), 802.11x, and Bluetooth. Wireless networks use

authentication protocols that provide authenticator protection and mutual authentication.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-94, 800-97; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-02, AC-03, AC-17, AC-19, CA-09, CM-07, IA-02, IA-03, IA-08, PL-04, SI-04

AC-18(01) Authentication and Encryption

Baselines

Moderate, High

Overlays

CJIS; Sensitive; FedRAMP Moderate, FedRAMP High

Requirements

Protect wireless access to the system using authentication of both users and devices as appropriate (for example, devices to wireless networks and users to enterprise services) and encryption.

Implementation Standards

Std.01 — Implement Extensible Authentication Protocol (EAP) with Wi-Fi Access Protection or IEEE 802.11i on WLANs or access points to provide encryption and strong identification and authentication for moderate- and high-impact systems.

Std.02 — Verify that wireless communications are mutually authenticated. [Source: OWASP: Application Security Verification Standard C.9]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-18(01).

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — For all agency-managed wireless access points (APs) with access to an agency's network that processes unencrypted CJI:

a. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Identification and Authentication (IA).

b. Ensure that encryption key sizes are at least 128-bits.

c. Ensure that the default shared keys are replaced by unique keys.

d. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface. [Source: CJIS 5.20.1.1]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Wireless networking capabilities represent a significant potential vulnerability that can be exploited by adversaries. To protect systems with wireless access points, strong authentication of users and devices along with strong encryption can reduce susceptibility to threats by adversaries involving wireless technologies.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-94, 800-97; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

SC-08, SC-12, SC-13

AC-18(03) Disable Wireless Networking

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-18(03).

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.01 CJIS — For all agency-managed wireless access points (APs) with access to an agency's network that processes unencrypted CJI, ensure that the ad hoc mode has been disabled. [Source: CJIS 5.20.1.1]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Wireless networking capabilities that are embedded within system components represent a significant potential vulnerability that can be exploited by adversaries. Disabling wireless capabilities when not needed for essential organizational missions or functions can reduce susceptibility to threats by adversaries involving wireless technologies.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-94, 800-97; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

CP-02

AC-18(04) Restrict Configurations by Users

Baselines

N/A

Overlays

FedRAMP High

Requirements

Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Organizational authorizations to allow selected users to configure wireless networking capabilities are enforced, in part, by the access enforcement mechanisms employed within organizational systems.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

SC-07, SC-15

AC-18(05) Antennas and Transmission Power Levels

Baselines

N/A

Overlays

CJIS; FedRAMP High

Requirements

Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.01 CJIS — For all agency-managed wireless access points (APs) with access to an agency's network that processes unencrypted CJI, test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes. [Source: CJIS 5.20.1.1]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Actions that may be taken to limit unauthorized use of wireless communications outside of organization-controlled boundaries include reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be captured outside of the physical perimeters of the organization, employing measures such as emissions security to control wireless emanations, and using directional or beamforming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such mitigating actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational systems as well as other systems that may be operating in the area.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-94, 800-97; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

None.

AC-19 Access Control for Mobile Devices

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and

b. Authorize the connection of mobile devices to organizational systems.

Implementation Standards

Std.01 — TxDOT shall establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, whether owned by TxDOT or the employee. [Source: DIR Control Standards Catalog AC-19]

Std.02 — Encryption is required for all mobile devices that contains TxDOT Sensitive, Confidential, or Regulated Information.

Std.03 — Require multi-factor authentication for remote network access, where supported. [Source: CIS 6.4]

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.04 PCI — Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the Cardholder Data Environment (CDE) as follows:

a. Specific configuration settings are defined to prevent threats being introduced into the entity's network.

b. Security controls are actively running.

c. Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.

[Source: PCI DSS 1.5.1]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirements AC-19 and 5.20.1.2.2.

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.05 CJIS — When directly accessing CJI from devices running a limited-feature operating system:

a. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.

b. MDM with centralized administration configured and implemented to perform at least the following controls:

1. Remote locking of device;

2. Remote wiping of device;

3. Setting and locking device configuration;

4. Detection of "rooted" and "jailbroken" devices;

5. Enforcement of folder or disk level encryption;

6. Application of mandatory policy settings on the device;

7. Detection of unauthorized configurations;

8. Detection of unauthorized software or applications;

9. Ability to determine the location of agency controlled devices; and

10. Prevention of unpatched devices from accessing CJI or CJI systems. [Source: CJIS 5.20.2]

Std.06 CJIS — A personal firewall shall be employed on all mobile devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems). At a minimum, the personal firewall shall perform the following activities:

a. Manage program access to the Internet.

b. Block unsolicited requests to connect to the user device.

c. Filter incoming traffic by IP address or protocol.

d. Filter incoming traffic by destination ports.

e. Maintain an IP traffic log. [Source: CJIS 5.20.4.3]

Std.07 CJIS — Access control shall be accomplished by the application that accesses CJI. [Source: CJIS 5.20.6]

Std.08 CJIS —

a. When mobile devices are authorized for use in accessing CJI, local device authentication shall be used to unlock the device for use.

b. The authenticator used shall meet the requirements in Identification and Authentication (IA). [Source: CJIS 5.20.7.1]

Std.09 CJIS — When certificates or cryptographic keys used to authenticate a mobile device are used in lieu of compensating controls for advanced authentication, they shall be:

a. Protected against being extracted from the device; and

b. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use. [Source: CJIS 5.20.7.3]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Mobile device functionality may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones and tablets. Mobile devices are typically associated with a single individual. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of notebook/desktop systems, depending on the nature and intended purpose of the device. Protection and control of mobile devices is behavior or policy-based and requires users to take physical action to protect and control such devices when outside of controlled areas. Controlled areas are spaces for which

organizations provide physical or procedural controls to meet the requirements established for protecting information and systems.

Due to the large variety of mobile devices with different characteristics and capabilities, organizational restrictions may vary for the different classes or types of such devices. Usage restrictions and specific implementation guidance for mobile devices include configuration management, device identification and authentication, implementation of mandatory protective software, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware.

Usage restrictions and authorization to connect may vary among organizational systems. For example, the organization may authorize the connection of mobile devices to its network and impose a set of usage restrictions, while a system owner may withhold authorization for mobile device connection to specific applications or impose additional usage restrictions before allowing mobile device connections to a system. Adequate security for mobile devices goes beyond the requirements specified in AC-19. Many safeguards for mobile devices are reflected in other controls. AC-20 addresses mobile devices that are not organization-controlled.

TxDOT Discussion

Notes for systems subject to CJIS requirements:

Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements. [Source: CJIS 5.20.1.2.2]

Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery, if so desired by the agency.

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of full-featured operating systems may not function properly on devices with limited-feature operating systems. MDM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented.

Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time. [Source: CJIS 5.20.2]

A device certificate alone placed on the device shall not be considered valid proof that the device is being operated by an authorized user. [Source: CJIS 5.20.7.3]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-114, 800-124; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-03, AC-04, AC-07, AC-11, AC-17, AC-18, AC-20, CA-09, CM-02, CM-06, IA-02, IA-03, MP-02, MP-04, MP-05, MP-07, PL-04, SC-07, SI-03, SI-04

AC-19(05) Full Device or Container-Based Encryption

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Employ full-device encryption where possible, and container-based encryption otherwise to protect the confidentiality and integrity of information on all mobile devices authorized to connect to TxDOT information systems.

Implementation Standards

Std.01 — For moderate- and high-baseline systems, enterprise solutions for full-disk or full-device encryption must be deployed.

Std.02 — All mobile devices (including, but not limited to, smartphones, tablets, diagnostics and calibration devices) must employ TxDOT-defined mobile device management and encryption solutions.

Std.03 — All removable storage devices must be encrypted in accordance with SC-13.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.04 CJIS — Employ full-device encryption to protect the confidentiality and integrity of information on full- and limited-feature operating system mobile devices authorized to process, store, or transmit CJI. [Source: CJIS AC-19(05)]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Container-based encryption provides a more fine-grained approach to data and information encryption on mobile devices, including encrypting selected data structures such as files, records, or fields.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-114, 800-124; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

SC-12, SC-13, SC-28

AC-20 Use of External Systems

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Establish terms and conditions as defined in Std.04, consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

1. Access the system from external systems; and

2. Process, store, or transmit organization-controlled information using external systems; or

b. Prohibit the use of all types of external systems except as authorized per Stds.03 & 04.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 —

a. TxDOT, as a state agency entering into or renewing a contract with a vendor authorized to access, transmit, use, or store data for the agency, shall include a provision in the contract requiring the vendor to meet the security controls the agency determines are proportionate with the agency's risk under the contract based on the sensitivity of the agency's data.

b. TxDOT shall require the vendor to periodically provide evidence to the agency that the vendor meets the security controls required under the contract. [Source: DIR Control Standards Catalog AC-20]

Std.03 — Limit connections to and use of external systems to only those required for business operations.

Std.04 — Establish and document terms and conditions via Interconnection Security Agreements (ISAs).

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.05 CJIS — Each Local Agency Security Officer (LASO) shall:

a. Identify who is using the CSA-approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.

b. Identify and document how the equipment is connected to the state system.

c. Ensure that personnel security screening procedures are being followed as stated in this Policy.

d. Ensure the approved and appropriate security measures are in place and working as expected.

e. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents. [Source: CJIS 3.2.9]

Std.06 CJIS — Prohibit the use of personally-owned information systems including mobile devices (i.e., bring your own device [BYOD]) and publicly accessible systems for accessing, processing, storing, or transmitting CJI. [Source: CJIS AC-20]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

External systems are systems that are used by but not part of organizational systems, and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness. External systems include personally owned systems, components, or devices; privately owned computing and communications devices in commercial or public facilities; systems owned or controlled by nonfederal organizations; systems managed by contractors; and federal information systems that are not owned by, operated by, or under the direct supervision or authority of the organization. External systems also include systems owned or operated by other components within the same organization and systems within the organization with different authorization boundaries. Organizations have the option to prohibit the use of any type of external system or prohibit the use of specified types of external systems, (e.g., prohibit the use of any external system that is not organizationally owned or prohibit the use of personally-owned systems).

For some external systems (i.e., systems operated by other organizations), the trust relationships that have been established between those organizations and the originating organization may be such that no explicit terms and conditions are required. Systems within these organizations may not be considered external. These situations occur when, for example, there are pre-existing information exchange agreements (either implicit or explicit) established between organizations or components or when such agreements are specified by applicable laws, executive orders, directives, regulations, policies, or standards. Authorized individuals include organizational personnel, contractors, or other individuals with authorized access to organizational systems and over which organizations have the authority to impose specific rules of behavior regarding system access. Restrictions that organizations impose on authorized individuals need not be uniform, as the restrictions may vary depending on trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments.

External systems used to access public interfaces to organizational systems are outside the scope of AC-20. Organizations establish specific terms and conditions for the use of external systems in accordance with organizational security policies and procedures. At a minimum, terms and conditions address the specific types of applications that can be accessed on organizational systems from external systems and the highest security category of information that can be processed, stored, or transmitted on external systems. If the terms and conditions with the owners of the

external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

The interrelated controls of AC-20, CA-3, and SA-9 should be differentiated as follows:

AC-20 describes system access to and from external systems.

CA-3 describes documentation of an agreement between the respective system owners when data is exchanged between the Cloud Service Offering (CSO) and an external system.

SA-9 describes the responsibilities of external system owners. These responsibilities would typically be captured in the agreement required by CA-3.

[Source: FedRAMP Security Controls Baseline AC-20]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 199; NIST SP 800-171, 800-172; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-02, AC-03, AC-17, AC-19, CA-03, PL-02, PL-04, SA-09, SC-07

AC-20(01) Limits on Authorized Use

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:

a. Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or

b. Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-20(01).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Limiting authorized use recognizes circumstances where individuals using external systems may need to access organizational systems. Organizations need assurance that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been implemented can be achieved by external, independent assessments, attestations, or other means, depending on the confidence level required by organizations.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 199; NIST SP 800-171, 800-172; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CA-02

AC-20(02) Portable Storage Devices — Restricted Use

Baselines

Moderate, High

Overlays

CJIS; Sensitive; FedRAMP Moderate, FedRAMP High

Requirements

Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using the restrictions defined in Stds.01 & 02.

Implementation Standards

Std.01 — All portable storage devices connecting to TxDOT systems must comply with the Media Protection policy and procedures. TxDOT-owned portable storage devices may be used on external systems but data cannot be transferred from those devices to the external systems.

Std.02 — Rewritable devices must be scanned for malware prior to accessing TxDOT systems after any use on non-TxDOT systems.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-20(02).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Limits on the use of organization-controlled portable storage devices in external systems include restrictions on how the devices may be used and under what conditions the devices may be used.

TxDOT Discussion

An example of Std.01 being implemented is a presentation that may be stored on a portable device and accessed by a projection system not controlled by TxDOT. When the portable device is connected to the TxDOT system, it must be scanned for malware prior to being accessed.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FIPS 199; NIST SP 800-171, 800-172; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

MP-07

AC-21 Information Sharing

Baselines

Moderate, High

Overlays

CJIS; Sensitive; FedRAMP Moderate, FedRAMP High

Requirements

a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for information sharing circumstances as described in the Information Sharing Agreement (ISA), where user discretion is required; and

b. Employ automated or manual review processes as described in Std.01 to assist users in making information sharing and collaboration decisions.

Implementation Standards

Std.01 — Access authorizations must be documented in the System Security Plan (SSP) and reviewed at least as often as the SSP for currency, business need, and to ensure that no intentional or unintentional information sharing with unauthorized parties occurs.

Std.02 — Provide training to authorized users on the mechanisms or processes available for making appropriate sharing decisions, specifically including access restrictions for data classifications.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-21.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Information sharing applies to information that may be restricted in some manner based on some formal or administrative determination. Examples of such information include, contract-sensitive information, classified information related to special access programs or compartments, privileged information, proprietary information, and personally identifiable information.

Security and privacy risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to these determinations. Depending on the circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program or compartment. Access restrictions may include non-disclosure agreements (NDA). Information flow techniques and security attributes may be used to provide automated assistance to users making sharing and collaboration decisions.

TxDOT Discussion

Information Sharing and Analysis Organization:

1. The Texas Department of Information Resources (DIR) shall establish an information sharing and analysis organization to provide a forum for state agencies, local governments, public and private institutions of higher education, and the private sector to share information regarding cybersecurity threats, best practices, and remediation strategies.

2. DIR shall provide administrative support to the information sharing and analysis organization.

3. A participant in the information sharing and analysis organization shall assert any exception available under state or federal law, including Section 552.139, in response to a request for public disclosure of information shared through the organization. Section 552.007 does not apply to information described by this subsection. [Source: TGC 2054.0594]

Sharing information can help to manage risks. This information may include vulnerabilities, threats, security incidents and mitigation measures, criticality of systems and components, or delivery information for supply chain risk management. This information sharing should be carefully managed to ensure that the information is accessible only to authorized individuals with a legitimate business need.

TxDOT References

Information Security and Privacy Policy

State References

TGC 2054; DIR Security Control Standards Catalog

Federal References

OMB A-130; NIST SP 800-150; NIST IR 8062; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-03, AC-04, PT-02, PT-07, RA-03, SC-15

AC-22 Publicly Accessible Content

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Designate individuals authorized to make information publicly accessible;

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible system for nonpublic information quarterly or as new information is posted and remove such information, if discovered.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — If Sensitive, Confidential, or Regulated information is discovered on a public site, the information must be handled according to the organization's incident management policies and procedures.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AC-22.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

In accordance with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines, the public is not authorized to have access to nonpublic information, including information protected under the PRIVACT and proprietary information. Publicly accessible content addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Posting information on non-organizational systems (e.g., non-organizational public websites, forums, and social media) is covered by organizational policy. While organizations may have individuals who are responsible for developing and implementing policies about the information that can be made publicly accessible, publicly accessible content addresses the management of the individuals who make such information publicly accessible.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

Privacy Act; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-03, AT-02, AT-03

AT – Awareness and Training

AT-01 Policy and Procedures

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level awareness and training policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;

b. Designate a senior management official as defined in the awareness and training policy to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and

c. Review and update the current awareness and training:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The TxDOT Executive Director or their designated representative(s) shall ensure that the state agency has trained personnel to assist the agency in complying with the requirements of 1 TAC 202 and related policies. [Source: 1 TAC 202.20(b)(4)]

Std.03 — The Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.04 CJIS — Review and update the current awareness and training policy and procedures following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. [Source: CJIS AT-01]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Awareness and training policy and procedures address the controls in the AT family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of awareness and training policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to awareness and training policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-12, 800-30, 800-39, 800-50, 800-100; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

PM-09, PS-08, SI-12

AT-02 Literacy Training and Awareness

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):

1. As part of initial training for new users and annually thereafter; and

2. When required by system changes or following major changes to legislation or security requirements;

b. Employ the following techniques to increase the security and privacy awareness of system users: awareness techniques in accordance with the awareness and training policy, procedures, and standards;

c. Update literacy training and awareness content annually and following major changes to legislation or security requirements; and

d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — An agency-wide information security program must be approved by the TxDOT Executive Director and include administering an ongoing information security awareness education program in compliance with the requirements of Texas Government Code Sec. 2054.5191 - .5192 for all users; and introducing information security awareness and informing new employees of information security policies and procedures during the onboarding process. [Source: 1 TAC 202.24(b)(2, 3)]

Std.03 — To the extent possible, TxDOT shall provide employees described by TGC 2054.135(c) (that is, employees of the agency who handle sensitive

information, including financial, medical, personnel, or student data) with cybersecurity awareness training to coincide with the distribution of:

a. The data use agreement required under TGC 2054.135; and

b. Each biennial update to that agreement. [Source: TGC 2054.135(d)]

Std.04 — TxDOT may select the most appropriate cybersecurity training program certified under TGC 2054.519 for employees of the state agency. [Source: TGC 2054.5191(c)]

Std.05 — At least once each year, TxDOT shall:

a. Identify its employees and elected officials who have access to TxDOT computer systems and who use a computer to complete at least 25 percent of the employee's or official's required duties; and [Source: TGC 2054.5191(a)]

b. Require those employees and officials to complete a cybersecurity training program certified under TGC 2054.519. [Source: TGC 2054.5191(a-1)(2)]

Std.06 — The TxDOT Executive Director shall verify completion of a cybersecurity training program by employees and officials of the state agency in a manner specified by DIR. Additionally, the TxDOT Executive Director shall periodically require an internal review of the agency to ensure compliance with TGC 2054.5191. [Source: TGC 2054.5191(c, d)]

Std.07 — TxDOT shall require any contractor who has access to a state computer system or database to complete a cybersecurity training program certified under TGC 2054.519 as selected by the agency. The cybersecurity training program must be completed by a contractor during the term of the contract and during any renewal period. A contractor required to complete a cybersecurity training program under this section shall verify completion of the program to the contracting state agency. [Source: TGC 2054.5192(b, c, e)]

Std.08 — Required completion of a cybersecurity training program must be included in the terms of a contract awarded by a state agency to a contractor. [Source: TGC 2054.5192(d)]

Std.09 — The person who oversees contract management for TxDOT shall report the contractor's completion to the department; and periodically review agency contracts to ensure compliance with this section. [Source: TGC 2054.5192(e)]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 12.6.1, 12.6.2, and 12.6.3.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.10 PCI — Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the Cardholder Data Environment (CDE), including but not limited to:

a. Phishing and related attacks.

b. Social engineering.

[Source: PCI DSS 12.6.3.1]

c. Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1. [Source: PCI DSS 12.6.3.2]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.11 CJIS —

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors): When required by system changes or within 30 days of any security event for individuals involved in the event; and

b. Update literacy training and awareness content annually and following changes in the information system operating environment, when security incidents occur, or when changes are made in the CJIS Security Policy. [Source: CJIS AT-02]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Organizations provide basic and advanced levels of literacy training to system users, including measures to test the knowledge level of users. Organizations determine the content of literacy training and awareness based on specific organizational requirements, the systems to which personnel have authorized access, and work environments (e.g., telework). The content includes an understanding of the need for security and privacy as well as actions by users to maintain security and personal privacy and to respond to suspected incidents. The content addresses the need for operations security and the handling of personally identifiable information.

Awareness techniques include displaying posters, offering supplies inscribed with security and privacy reminders, displaying logon screen messages, generating email advisories or notices from organizational officials, and conducting awareness events. Literacy training after the initial training described in AT-02a.1 is conducted at a minimum frequency consistent with applicable laws, directives, regulations, and policies. Subsequent literacy training may be satisfied by one or more short ad hoc sessions and include topical information on recent attack schemes, changes to organizational security and privacy policies, revised security and privacy expectations, or a subset of topics from the initial training. Updating literacy training and awareness content on a regular basis helps to ensure that the content remains relevant. Events that may precipitate an update to literacy training and awareness content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

TxDOT Discussion

TxDOT may deny access to its computer system or database to an individual described by Subsection (a-1)(1) who the governing body or the governing body's designee determines is noncompliant with the requirements of Subsection (a-1)(2). [Source: TGC 2054. 5191(a-2)]

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; TGC 2054; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-50, 800-160-2, 800-181; ODNI CTF; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-03, AC-17, AC-22, AT-03, AT-04, CP-03, IA-04, IR-02, IR-07, PL-04, PM-13, PM-21, PS-07, PT-02, SA-08, SA-16

AT-02(02) Insider Threat

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Provide literacy training on recognizing and reporting potential indicators of insider threat.

Implementation Standards

Std.01 — Include content on insider threat in training for employees and contractors in accordance with PM-12.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AT-02(02).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction; attempts to gain access to information not required for job performance; unexplained access to financial resources; bullying or harassment of fellow employees; workplace violence; and other serious violations of policies, procedures, directives, regulations, rules, or practices. Literacy training includes how to communicate the concerns of employees and management regarding potential indicators of insider threat through channels established by the organization and in accordance with established policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role. For example, training for managers may be focused on changes in the behavior of team members, while training for employees may be focused on more general observations.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-50, 800-160-2, 800-181; ODNI CTF; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

PM-12

AT-02(03) Social Engineering and Mining

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP High

Requirements

Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

Implementation Standards

Std.01 — Information Security Training for employees and contractors must include content on social engineering and social mining including instructions on reporting.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AT-02(03).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Social engineering is an attempt to trick an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system. Social engineering includes phishing, pretexting, impersonation, baiting, quid pro quo, thread-jacking, social media exploitation, and tailgating. Social mining is an attempt to gather information about the organization that may be used to support future attacks. Literacy training includes information on how to communicate the concerns of employees and management regarding potential and actual instances of social engineering and data mining through organizational channels based on established policies and procedures.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-50, 800-160-2, 800-181; ODNI CTF; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

AT-03 Role-Based Training

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: as outlined in Information Security Role Based Training guidance:

1. Before authorizing access to the system, information, or performing assigned duties, and when an employee enters a new position that requires additional role-specific training, and annually thereafter; and

2. When required by system changes;

b. Update role-based training content annually and following major changes to legislation or security requirements; and

c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The TxDOT Executive Director or their designated representative(s) shall ensure that the state agency has trained personnel to

assist the agency in complying with the requirements of 1 TAC 202 and related policies. [Source: 1 TAC 202.20(b)(4)]

Std.03 — The Information Security Officer shall be responsible for providing for training and direction for personnel with significant responsibilities for information security with respect to such responsibilities. [Source: 1 TAC 202.21(b)(4)]

Std.04 — TxDOT may spend public funds as appropriate to reimburse a state agency employee or administrator who serves in an information technology, cybersecurity, or other cyber-related position for fees associated with industry-recognized certification examinations. [Source: TGC 656.047(a)(1)]

Std.05 — TxDOT shall comply with the mandatory guidelines provided by DIR regarding the initial and continuing education requirements needed for cybersecurity training that must be completed by all information resources employees of the agencies. [Source: TGC 2054.076(b-1)]

Std.06 — TxDOT shall, with available funds, identify information security issues and develop a plan to prioritize the remediation of those issues. The agency shall include in the plan:

a. Analysis of the percentage of state agency personnel in information technology, cybersecurity, or other cyber-related positions who currently hold the appropriate industry-recognized certifications as identified by the National Initiative for Cybersecurity Education;

b. The level of preparedness of TxDOT cyber personnel and potential personnel who do not hold the appropriate industry-recognized certifications to successfully complete the industry-recognized certification examinations; and

c. A strategy for mitigating any workforce-related discrepancy in information technology, cybersecurity, or other cyber-related positions with the appropriate training and industry-recognized certifications. [Source: TGC 2054.575(a)(3, 4, 5)]

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.10 CJIS —

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities:

• All individuals with unescorted access to a physically secure location;

• General User: A user, but not a process, who is authorized to use an information system;

• Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform;

• Organizational Personnel with Security Responsibilities: Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL.

1. Before authorizing access to the system, information, or performing assigned duties, and annually thereafter; and

2. When required by system changes.

b. Update role-based training content annually and following audits of the CSA and local agencies; changes in the information system operating environment; security incidents; or when changes are made to the CJIS Security Policy;

c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training;

d. Incorporate the minimum following topics into the appropriate role-based training content:

1. All individuals with unescorted access to a physically secure location:

a. Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information Penalties;

b. Reporting Security Events;

c. Incident Response Training;

d. System Use Notification;

e. Physical Access Authorizations;

f. Physical Access Control;

g. Monitoring Physical Access;

h. Visitor Control;

i. Personnel Sanctions.

2. General User: A user, but not a process, who is authorized to use an information system. In addition to AT-3(d)(1) above, include the following topics:

a. Criminal Justice Information;

b. Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information;

c. Personally Identifiable Information;

d. Information Handling;

e. Media Storage;

f. Media Access;

g. Audit Monitoring, Analysis, and Reporting;

h. Access Enforcement;

i. Least Privilege;

j. System Access Control;

k. Access Control Criteria;

l. System Use Notification;

m. Session Lock;

n. Personally Owned Information Systems;

o. Password;

p. Access Control for Display Medium;

q. Encryption;

r. Malicious Code Protection;

s. Spam and Spyware Protection;

t. Cellular Devices;

u. Mobile Device Management;

v. Wireless Device Risk Mitigations;

w. Wireless Device Malicious Code Protection;

x. Literacy Training and Awareness/Social Engineering and Mining;

y. Identification and Authentication (Organizational Users);

z. Media Protection.

3. Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform. In addition to AT-3(d) (1) and (2) above, include the following topics:

a. Access Control;

b. System and Communications Protection and Information Integrity;

c. Patch Management;

d. Data backup and storage—centralized or decentralized approach;

e. Most recent changes to the CJIS Security Policy.

4. Organizational Personnel with Security Responsibilities: Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL. In addition to AT-3 (d) (1), (2), and (3) above, include the following topics:

a. Local Agency Security Officer Role;

b. Authorized Recipient Security Officer Role;

c. Additional state/local/tribal/territorial or federal agency roles and responsibilities;

d. Summary of audit findings from previous state audits of local agencies;

e. Findings from the last FBI CJIS Division audit.

[Source: CJIS AT-03]

Std.07 CJIS — Rescinded in V4.0.

Std.08 CJIS — Rescinded in V4.0.

Std.09 CJIS — Rescinded in V4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Organizations determine the content of training based on the assigned roles and responsibilities of individuals as well as the security and privacy requirements of organizations and the systems to which personnel have authorized access, including technical training specifically tailored for assigned duties. Roles that may require role-based training include senior leaders or management officials (e.g., head of agency/chief executive officer, chief information officer, senior accountable official for risk management, senior agency information security officer, senior agency official for privacy), system owners; authorizing officials; system security officers; privacy officers; acquisition and procurement officials; enterprise architects; systems engineers; software developers; systems security engineers; privacy engineers; system, network, and database administrators; auditors; personnel conducting configuration management activities; personnel performing verification and validation activities; personnel with access to system-level software; control assessors; personnel with contingency planning and incident response duties; personnel with privacy management responsibilities; and personnel with access to personally identifiable information.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Role-based training also includes policies, procedures, tools, methods, and artifacts for the security and privacy roles defined. Organizations provide the training necessary for individuals to fulfill their responsibilities related to operations and supply chain risk management within the context of organizational security and privacy programs. Role-based training also applies to contractors who provide services to federal

agencies. Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Updating role-based training on a regular basis helps to ensure that the content remains relevant and effective. Events that may precipitate an update to role-based training content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

TxDOT Discussion

State Implementation Details

Security awareness training shall be delivered in accordance with Texas Government Code 2054.519. [Source: DIR Control Standards Catalog AT-3]

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; TGC 656; TGC 2054; DIR Information Resources Employees Continuing Education Guidelines for Cybersecurity; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-50, 800-181; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-03, AC-17, AC-22, AT-02, AT-04, CP-03, IR-02, IR-04, IR-07, PL-04, PM-13, PS-07, PS-09, SA-03, SA-08, SA-11, SA-16, SR-05, SR-06, SR-11, SR-11(01)

AT-03(05) Processing Personally Identifiable Information

Baselines

N/A

Overlays

CJIS; Privacy

Requirements

Provide personnel or roles that have access to personally identifiable information (PII) with initial and annual training in the employment and operation of personally identifiable information processing and transparency controls.

Implementation Standards

Std.01 — Ensure that role-based training includes proper handling of sensitive personal information (SPI).

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.02 CJIS — Provide all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI with initial and annual training in the employment and operation of personally identifiable information processing and transparency controls. [Source: CJIS AT-03(05)]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Personally identifiable information processing and transparency controls include the organization's authority to process personally identifiable information and personally identifiable information processing purposes. Role-based training for federal agencies addresses the types of information that may constitute personally identifiable information and the risks, considerations, and obligations associated with its processing. Such training also considers the authority to process personally identifiable information documented in privacy policies and notices, system of records notices, computer matching agreements and notices, privacy impact assessments, PRIVACT statements, contracts, information sharing agreements, memoranda of understanding, and/or other documentation.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; NIST SP 800-50, 800-181; CJIS Security Policy

Related Controls

PT-02, PT-03, PT-05

AT-04 Training Records

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and

b. Retain individual training records for termination of employment + five years.

Implementation Standards

Std.01 — Rescinded in V2.2.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AT-04.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Documentation for specialized training may be maintained by individual supervisors at the discretion of the organization. The National Archives and Records Administration provides guidance on records retention for federal agencies.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AT-02, AT-03, CP-03, IR-02, PM-14, SI-12

AU – Audit and Accountability

AU-01 Policy and Procedures

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level audit and accountability policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;

b. Designate a senior management official as defined in the audit and accountability policy to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and

c. Review and update the current audit and accountability:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 10.1.1 and 10.1.2.

Std.03 PCI — Rescinded in V3.0.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.04 CJIS — Review and update the current audit and accountability policy and procedures following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. [Source: CJIS AU-01]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Audit and accountability policy and procedures address the controls in the AU family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy

assurance. Therefore, it is important that security and privacy programs collaborate on the development of audit and accountability policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to audit and accountability policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-12, 800-30, 800-39, 800-100; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

PM-09, PS-08, SI-12

AU-02 Event Logging

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Identify the types of events that the system is capable of logging in support of the audit function: event types as defined in Std.04;

b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;

c. Specify the following event types for logging within the system: as specified in the System Security Plan (SSP), the subset of the auditable events defined in AU-02a. for specific components of the system, along with the frequency of (or situation requiring) auditing for each identified event type in accordance with AU-06;

d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and

e. Review and update the event types selected for logging annually.

Implementation Standards

Std.01 — Information resources systems shall provide the means whereby authorized personnel have the ability to audit and establish individual accountability for any action that can potentially cause access to, generation or modification of, or affect the release of confidential information. [Source: DIR Control Standards Catalog AU-2]

Std.02 — Appropriate audit trails shall be maintained to provide accountability for updates to mission critical information, hardware and software and for all changes to automated security or access rules. [Source: DIR Control Standards Catalog AU-2]

Std.03 — Based on TxDOT's assessment of the risk, TxDOT shall maintain a sufficiently complete history of transactions to permit an audit of the information resources system by logging and tracing the activities of individuals through the system. [Source: DIR Control Standards Catalog AU-2]

Std.04 — If capable, systems must log the following event types:

a. Authentication events;

b. File and Objects events;

c. Writes/downloads to devices/media (for example, floppy disks, CD/DVD drives, USB devices/printers) (Success/Failure);

d. Uploads from devices/media (for example, USB, CD/DVD drives (Success/Failure);

e. User and Group Management events;

f. Use of Privileged/Special Rights events;

g. Admin or root-level access (Success/Failure);

h. Privilege/Role escalation (Success/Failure);

i. Audit and log data accesses (Success/Failure);

j. System reboot, restart, and shutdown (Success/Failure);

k. Print to a device (Success/Failure);

l. Print to a file (for example, pdf format) (Success/Failure);

m. Application (for example, Firefox, Internet Explorer, MS Office Suite, etc.) initialization (Success/Failure);

n. Export of information (Success/Failure) include (for example, to CDRW, thumb drives, or remote systems);

o. Import of information (Success/Failure) include (for example, from CDRW, thumb drives, or remote systems).

Std.05 — Event logs must be retained in a format that allows compilation of auditing records from multiple components into a system-wide, time-correlated audit trail.

Std.06 — At a minimum, the list of auditable events for a system must be adequate to support after-the-fact investigations of security events. Event logging plans for a system must be updated following any investigation where a deficiency of auditing is uncovered for a similar system.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirements AU-02 and 5.20.1.1.

TX-RAMP Correspondence

For systems subject to TX-RAMP Level 1 or Level 2 requirements, the following standard applies:

Std.07 TX-RAMP — If capable, systems must log the following event types: Policy change, process tracking, and, for Web applications, authorization checks. [Source: TX-RAMP Manual AU-2]

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.08 FedRAMP —

a. Identify the types of events that the system is capable of logging in support of the audit function: successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes;

b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;

c. Specify the following event types for logging within the system: organization-defined subset of the auditable events defined in AU-2a to be audited continually for each identified event;

d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and

e. Review and update the event types selected for logging annually and whenever a change in the threat environment is discovered or when changes to the threat environment are communicated to the service provider by the Joint Authorization Board (JAB)/Authorizing Official (AO).

[Source: FedRAMP Security Controls Baseline AU-2]

Discussion

An event is an observable occurrence in a system. The types of events that require logging are those events that are significant and relevant to the security of systems and the privacy of individuals. Event logging also supports specific monitoring and auditing needs. Event types include password changes, failed logons or failed accesses related to systems, security or privacy attribute changes, administrative privilege usage, PIV credential usage, data action changes, query parameters, or external credential usage. In determining the set of event types that require logging, organizations consider the monitoring and auditing appropriate for each of the controls to be implemented. For completeness, event logging includes all protocols that are operational and supported by the system.

To balance monitoring and auditing requirements with other system needs, event logging requires identifying the subset of event types that are logged at a given point in time. For example, organizations may determine that systems need the capability to log every file access successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. The types of events that organizations desire to be logged may change. Reviewing and updating the set of logged events is necessary to help ensure that the events remain relevant and continue to support the needs of the organization. Organizations consider how the types of logging events can reveal information about individuals that may give rise to privacy risk and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the logging event is based on patterns or time of usage.

Event logging requirements, including the need to log specific event types, may be referenced in other controls and control enhancements. These include AC-02(04), AC-03(10), AC-06(09), AC-17(01), CM-03f, CM-05(01), IA-03(03)(b), MA-04(01), MP-04(02), PE-03, PM-21, PT-07, RA-08, SC-07(09), SC-07(15), SI-03(08), SI-04(22), SI-07(08), and SI-10(01). Organizations include event types that are required by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Audit records can be generated at various levels, including at the packet level as information traverses the network. Selecting the appropriate level of event logging is an important part of a monitoring and auditing capability and can identify the root causes of problems. When defining event types, organizations consider the logging necessary to cover related event types, such as the steps in distributed, transaction-based processes and the actions that occur in service-oriented architectures.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-92; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-02, AC-03, AC-06, AC-07, AC-08, AC-17, AU-03, AU-04, AU-05, AU-06, AU-07, AU-11, AU-12, CM-03, CM-05, CM-06, IA-03, MA-04, MP-04, PE-03, PM-21, PT-02, PT-07, RA-08, SA-08, SC-07, SC-18, SI-03, SI-04, SI-07, SI-10, SI-11

AU-03 Content of Audit Records

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Ensure that audit records contain information that establishes the following:

a. What type of event occurred;

b. When the event occurred;

c. Where the event occurred;

d. Source of the event;

e. Outcome of the event; and

f. Identity of any individuals, subjects, or objects/entities associated with the event.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — For moderate- and high-security baseline systems, the audit function must have the capability of providing more detailed information for audit events identified by type, location, or subject as required by TxDOT.

Std.03 — Raw audit records must be available in an unaltered format.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 10.2.2.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AU-03.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Audit record content that may be necessary to support the auditing function includes event descriptions (item a), time stamps (item b), source and destination addresses (item c), user or process identifiers (items d and f), success or fail indications (item e), and filenames involved (items a, c, e, and f). Event outcomes include indicators of event success or failure and event-specific results, such as the system security and privacy posture after the event occurred. Organizations consider how audit records can reveal information about individuals that may give rise to privacy risks and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the trail records inputs or is based on patterns or time of usage.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST IR 8062; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AU-02, AU-08, AU-12, MA-04, PL-09, SA-08, SI-07, SI-11

AU-03(01) Additional Audit Information

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Generate audit records containing the following additional information: as defined in Std.02 below, sufficient information to support after-the-fact investigation.

Implementation Standards

Std.01 — Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. [Source: SP 800-171 3.3.1]

Std.02 — Additional information must be limited to that explicitly needed for specific audit requirements. Systems must be configured to generate audit records containing the following additional elements as feasible:

a. Filename accessed;

b. Program or command used to initiate the event;

c. Manufacturer-specific event name/type of event;

d. Source and destination network addresses;

e. Source and destination port or protocol identifiers;

f. Other security-relevant actions associated with processing; and

g. Any additional significant system events or risks.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Rescinded in V4.0.

Std.06 CJIS — Generate audit records containing the following additional information:

a. Session, connection, transaction, and activity duration;

b. Source and destination addresses;

c. Object or filename involved; and

d. Number of bytes received and bytes sent (for client-server transactions) in the audit records for audit events identified by type, location, or subject.

e. The III portion of the log shall clearly identify:

1. The operator;

2. The authorized receiving agency;

3. The requestor; and

4. The secondary recipient. [Source: CJIS AU-03(01)]

TX-RAMP Correspondence

For systems subject to TX-RAMP Level 2, the following standard applies:

Std.04 TX-RAMP — Systems must be configured to generate audit records containing the following additional elements as feasible:

a. Session, connection, transaction, or activity duration;

b. For client-server transactions, the number of bytes received and bytes sent;

c. Additional informational messages to diagnose or identify the event; and

d. Characteristics that describe or identify the object or resource being acted upon. [Source: TX-RAMP Manual AU-3(1)]

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.05 FedRAMP — Generate audit records containing the following additional information: session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon; individual identities of group account users; full-text of privileged commands. [Source: FedRAMP Security Controls Baseline AU-3(1)]

Discussion

The ability to add information generated in audit records is dependent on system functionality to configure the audit record content. Organizations may consider additional information in audit records including, but not limited to, access control or flow control rules invoked and individual identities of group account users. Organizations may also consider limiting additional audit record information to only information that is explicitly needed for audit requirements. This facilitates the use of audit trails and audit logs by not including information in audit records that could potentially be misleading, make it more difficult to locate information of interest, or increase the risk to individuals' privacy.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements: For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry. [Source: FedRAMP Security Controls Baseline AU-3(1)]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST IR 8062; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

None.

AU-03(03) Limit Personally Identifiable Information Elements

Baselines

N/A

Overlays

CJIS; Privacy

Requirements

Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: only those elements authorized for inclusion per AU-03.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AU-03(03).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Limiting personally identifiable information in audit records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; NIST IR 8062; CJIS Security Policy

Related Controls

AU-03, RA-03

AU-04 Audit Log Storage Capacity

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Allocate audit log storage capacity to accommodate audit log retention requirements as defined in the Records Retention Schedule.

Implementation Standards

Std.01 — Rescinded in V2.2.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AU-04.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Organizations consider the types of audit logging to be performed and the audit log processing requirements when allocating audit log storage capacity. Allocating sufficient audit log storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of audit logging capability.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AU-02, AU-05, AU-06, AU-07, AU-09, AU-11, AU-12, SI-04

AU-05 Response to Audit Logging Process Failures

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Alert personnel or roles as identified in the System Security Plan (SSP) within 15 minutes in the event of an audit logging process failure; and

b. Take the following additional actions: actions as outlined in the SSP.

Implementation Standards

Std.01 — Rescinded in V2.2.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Take the following additional actions: restart all audit logging processes and verify system(s) are logging properly. [Source: CJIS AU-05]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following additional standard applies:

Std.02 FedRAMP — In the event of an audit logging process failure, take the following additional actions: overwrite oldest record. [Source: FedRAMP Security Controls Baseline AU-5]

Discussion

Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity. Organization-defined actions include overwriting oldest audit records, shutting down the system, and stopping the generation of audit records. Organizations may choose to define additional actions for audit logging process failures based on the type of failure, the location of the

failure, the severity of the failure, or a combination of such factors. When the audit logging process failure is related to storage, the response is carried out for the audit log storage repository (i.e., the distinct system component where the audit logs are stored), the system on which the audit logs reside, the total audit log storage capacity of the organization (i.e., all audit log storage repositories combined), or all three. Organizations may decide to take no additional actions after alerting designated roles or personnel.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AU-02, AU-04, AU-07, AU-09, AU-11, AU-12, SI-04, SI-12

AU-05(01) Storage Capacity Warning

Baselines

N/A

Overlays

FedRAMP High

Requirements

Provide a warning to personnel or roles as identified in the System Security Plan (SSP) within one month before expected negative impact when allocated audit log storage volume reaches 75% of repository maximum audit log storage capacity.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Organizations may have multiple audit log storage repositories distributed across multiple system components with each repository having different storage volume capacities.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

AU-05(02) Real-Time Alerts

Baselines

N/A

Overlays

FedRAMP High

Requirements

Provide an alert within real-time to service provider personnel with authority to address failed audit events when the following audit failure events occur: audit failure events requiring real-time alerts, as defined by organization audit requirement documents.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

AU-06 Audit Record Review, Analysis, and Reporting

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Review and analyze system audit records as specified in the Continuous Monitoring Program for indications of inappropriate or unusual activity as defined in the System Security Plan (SSP) in accordance with AU-02 and the potential impact of the inappropriate or unusual activity;

b. Report findings to personnel as identified in the SSP; and

c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 —

a. Comply with all relevant legal requirements applicable to monitoring activities. Items that are monitored include:

1. Authorized access; and

2. Unauthorized access attempts.

b. Specify how often audit logs are reviewed, how the reviews are documented, and the specific roles and responsibilities of the personnel conducting the reviews, including the professional certifications or other qualifications required.

c. Periodically test monitoring and detection processes, remediate deficiencies, and improve processes. [Source: Hitrust 09.ab Monitoring System Use]

Std.03 — Ensure that proper logging is enabled in order to audit administrator activities. Review system administrator and operator logs on a regular basis. [Source: Hitrust 09.ad Administrator and Operator Logs]

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.04 PCI — The following audit logs are reviewed at least once daily:

a. All security events.

b. Logs of all system components that store, process, or transmit Cardholder Data (CHD) and/or Sensitive Authentication Data (SAD).

c. Logs of all critical system components.

d. Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers).

[Source: PCI DSS 10.4.1]

e. Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically. [Source: PCI DSS 10.4.2]

f. The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1; at a minimum, at least once every seven days (weekly). [Source: PCI DSS 10.4.2.1; PCI DSS v4.x: Targeted Risk Analysis Guidance]

g. Exceptions and anomalies identified during the review process are addressed. [Source: PCI DSS 10.4.3]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.05 CJIS — Rescinded in V4.0.

Std.06 CJIS — For all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI, review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly. [Source: CJIS 5.20.1.1]

Std.09 CJIS — Review and analyze system audit records weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity. [Source: CJIS AU-06]

TX-RAMP Correspondence

For systems subject to TX-RAMP Level 1 or Level 2 requirements, the following standard applies:

Std.07 TX-RAMP — Review and analyze system audit records at least monthly for indications of inappropriate or unusual activity as defined in the System Security Plan (SSP) in accordance with AU-02 and the potential impact of the inappropriate or unusual activity. [Source: TX-RAMP Manual AU-6]

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standards apply:

Std.08 FedRAMP — Review and analyze system audit records at least weekly for indications of inappropriate or unusual activity as defined in the System Security Plan (SSP) in accordance with AU-02 and the potential impact of the inappropriate or unusual activity. [Source: FedRAMP Security Controls Baseline AU-6]

Std.09 FedRAMP — Coordination between service provider and consumer shall be documented and accepted by the Joint Authorization Board (JAB)/Authorizing Official (AO). In multi-tenant environments, capability and means for providing review, analysis, and reporting to consumer for data pertaining to consumer shall be documented. [Source: FedRAMP Security Controls Baseline AU-6]

Discussion

Audit record review, analysis, and reporting covers information security- and privacy-related logging performed by organizations, including logging that results from the monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and non-local maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at system interfaces, and use of mobile code or Voice over Internet Protocol (VoIP). Findings can be reported to organizational entities that include the incident response team, help desk, and security or privacy offices. If organizations are prohibited from reviewing and analyzing audit records or unable to conduct such activities, the review or analysis may be carried out by other organizations granted such authority. The frequency, scope, and/or depth of the audit record review, analysis, and reporting may be adjusted to meet organizational needs based on new information received.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-86, 800-101; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-02, AC-03, AC-05, AC-06, AC-07, AC-17, AU-07, CA-02, CA-07, CM-02, CM-05, CM-06, CM-10, CM-11, IA-02, IA-03, IA-05, IA-08, IR-05, MA-04, MP-04, PE-03, PE-06, RA-05, SA-08, SC-07, SI-03, SI-04, SI-07

AU-06(01) Automated Process Integration

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; Sensitive; FedRAMP Moderate, FedRAMP High

Requirements

Integrate audit record review, analysis, and reporting processes using automated mechanisms as identified in System Security Plans (SSPs).

Implementation Standards

Std.01 — Ensure that appropriate records are aggregated to a centralized audit repository for analysis and review by TxDOT Information Security:

a. Information is provided to TxDOT Information Security in a searchable format compliant with TxDOT, state, and federal requirements;

b. Audit record sources include systems, appliances, devices, services, and applications (including databases); and

c. TxDOT Information Security-directed audit information collection rules/requests (for example, sources, queries, data calls) are implemented/provided within the timeframe specified in the request.

Std.02 — Raw audit records and raw security information/results from relevant automated tools must be available in an unaltered format to TxDOT Information Security.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 10.4.1.1.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.03 PCI — Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify. [Source: PCI DSS 10.3.3]

Std.04 PCI — Rescinded in V3.0.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AU-06(01).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organizational processes that benefit from integrated audit record review, analysis, and reporting include incident response, continuous monitoring, contingency planning, investigation and response to suspicious activities, and Inspector General audits.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-86, 800-101; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

PM-07

AU-06(03) Correlate Audit Record Repositories

Baselines

Moderate, High

Overlays

CJIS; Sensitive; FedRAMP Moderate, FedRAMP High

Requirements

Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

Implementation Standards

Std.01 — Correlated results from automated tools must be searchable by TxDOT Information Security:

a. Information is provided to TxDOT Information Security in a format compliant with TxDOT, state, and Federal (for example, Continuous Diagnostics and Mitigation) requirements;

b. Repository sources include systems, appliances, devices, services, and applications (including databases); and

c. TxDOT Information Security directed repository information collection rules/requests (for example, sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AU-06(03).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organization-wide situational awareness includes awareness across all three levels of risk management (i.e., organizational level, mission/business process level, and information system level) and supports cross-organization awareness.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-86, 800-101; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AU-12, IR-04

AU-06(04) Central Review and Analysis

Baselines

N/A

Overlays

FedRAMP High

Requirements

Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Automated mechanisms for centralized reviews and analyses include Security Information and Event Management products.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

AU-02, AU-12

AU-06(05) Integrated Analysis of Audit Records

Baselines

N/A

Overlays

FedRAMP High

Requirements

Integrate analysis of audit records with analysis of system monitoring information to further enhance the ability to identify inappropriate or unusual activity.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Integrated analysis of audit records does not require vulnerability scanning, the generation of performance data, or system monitoring. Rather, integrated analysis requires that the analysis of information generated by scanning, monitoring, or other data collection activities is integrated with the analysis of audit record information. Security Information and Event Management tools can facilitate audit record aggregation or consolidation from multiple system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans of the system and in correlating attack detection events with scanning results. Correlation with performance data can uncover denial-of-service attacks or other types of attacks that result in the unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

AU-12, IR-04

AU-06(06) Correlation with Physical Monitoring

Baselines

N/A

Overlays

FedRAMP High

Requirements

Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.01 FedRAMP — Coordination between service provider and consumer shall be documented and accepted by the Joint Authorization Board (JAB)/Authorizing Official (AO). [Source: FedRAMP Security Controls Baseline AU-6(6)]

Discussion

The correlation of physical audit record information and the audit records from systems may assist organizations in identifying suspicious behavior or supporting evidence of such behavior. For example, the correlation of an individual's identity for logical access to certain systems with the additional physical security information that the individual was present at the facility when the logical access occurred may be useful in investigations.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

AU-06(07) Permitted Actions

Baselines

N/A

Overlays

FedRAMP High

Requirements

Specify the permitted actions for each system process, role, or user associated with the review, analysis, and reporting of audit record information.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Organizations specify permitted actions for system processes, roles, and users associated with the review, analysis, and reporting of audit records through system account management activities. Specifying permitted actions on audit record information is a way to enforce the principle of least privilege. Permitted actions are enforced by the system and include read, write, execute, append, and delete.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

AU-07 Audit Record Reduction and Report Generation

Baselines

Moderate, High

Overlays

CJIS; Sensitive; FedRAMP Moderate, FedRAMP High

Requirements

Provide and implement an audit record reduction and report generation capability that:

a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and

b. Does not alter the original content or time ordering of audit records.

Implementation Standards

Std.01 — Configure SIEM tools and systems to provide audit reduction and report generation capabilities that support near real-time audit review and after-the-fact investigations based on selectable event criteria in accordance with AU-06.

Std.02 — Ensure that audit record processing does not degrade the operational performance of the control system. [Source: Catalog of Control Systems Security: Recommendations for Standards Developers]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AU-07.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Audit record reduction is a process that manipulates collected audit log information and organizes it into a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always emanate from the same system or from the same organizational entities that conduct audit logging activities. The audit record reduction capability includes modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can generate customizable reports. Time ordering of audit records can be an issue if the granularity of the timestamp in the record is insufficient.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-02, AU-02, AU-03, AU-04, AU-05, AU-06, AU-12, CM-05, IA-05, IR-04, PM-12, SI-04

AU-07(01) Automatic Processing

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; FedRAMP Moderate, FedRAMP High

Requirements

Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: all fields within audit records specified in AU-03.

Implementation Standards

None.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.01 PCI —

a. Audit logs capture all individual user access to cardholder data. [Source: PCI DSS 10.2.1.1]

b. Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts. [Source: PCI DSS 10.2.1.2]

c. Audit logs capture all access to audit logs. [Source: PCI DSS 10.2.1.3]

d. Audit logs capture all invalid logical access attempts. [Source: PCI DSS 10.2.1.4]

e. Audit logs capture all changes to identification and authentication credentials including, but not limited to:

1. Creation of new accounts.

2. Elevation of privileges.

3. All changes, additions, or deletions to accounts with administrative access.

[Source: PCI DSS 10.2.1.5]

f. Audit logs capture the following:

1. All initialization of new audit logs; and

2. All starting, stopping, or pausing of the existing audit logs.

[Source: PCI DSS 10.2.1.6]

g. Audit logs capture all creation and deletion of system-level objects. [Source: PCI DSS 10.2.1.7]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AU-07(01).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Events of interest can be identified by the content of audit records, including system resources involved, information objects accessed, identities of individuals, event types, event locations, event dates and times, Internet Protocol addresses involved, or event success or failure. Organizations may define event criteria to any degree of granularity required, such as locations selectable by a general networking location or by specific system component.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

AU-08 Time Stamps

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Use internal system clocks to generate time stamps for audit records; and

b. Record time stamps for audit records that meet the degree of synchronization between systems and reference clocks as defined in the System Security Plan (SSP) based on the sensitivity of the system, at minimum within 30 seconds of accuracy and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

Implementation Standards

Std.01 — Rescinded in V2.2.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 10.6.1.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Record time stamps for audit records that meet hundredths of a second (i.e., hh:mm:ss:00) interval and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp. [Source: CJIS AU-08]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.02 FedRAMP — Record time stamps for audit records that meet one second granularity of time measurement and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp. [Source: FedRAMP Security Controls Baseline AU-8]

Discussion

Time stamps generated by the system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks (e.g., clocks synchronizing within hundreds of milliseconds or tens of milliseconds). Organizations may define different time granularities for different system components. Time service can be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AU-03, AU-12, SC-45

AU-09 Protection of Audit Information

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and

b. Alert personnel or roles as specified in System Security Plans (SSPs) upon detection of unauthorized access, modification, or deletion of audit information.

Implementation Standards

Std.01 — Rescinded in V2.2.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 10.3.2.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AU-09.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Audit information includes all information needed to successfully audit system activity, such as audit records, audit log settings, audit reports, and personally identifiable information. Audit logging tools are those programs and devices used to conduct system audit and logging activities. Protection of audit information focuses on technical protection and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by both media protection controls and physical and environmental protection controls.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 180, 202; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-03, AC-06, AU-06, AU-11, MP-02, MP-04, PE-02, PE-03, PE-06, SA-08, SC-08, SI-04

AU-09(02) Store on Separate Physical Systems or Components

Baselines

N/A

Overlays

FedRAMP High

Requirements

Store audit records at least weekly in a repository that is part of a physically different system or system component than the system or component being audited.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Storing audit records in a repository separate from the audited system or system component helps to ensure that a compromise of the system being audited does not also result in a compromise of the audit records. Storing audit records on separate physical systems or components also preserves the confidentiality and integrity of audit records and facilitates the management of audit records as an organization-wide activity. Storing audit records on separate systems or components applies to initial generation as well as backup or long-term storage of audit records.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

AU-04, AU-05

AU-09(03) Cryptographic Protection

Baselines

N/A

Overlays

FedRAMP High

Requirements

Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Cryptographic mechanisms used for protecting the integrity of audit information include signed hash functions using asymmetric cryptography. This enables the distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements: Note that this enhancement requires the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13.)

[Source: FedRAMP Security Controls Baseline AU-9(3)]

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

AU-10, SC-12, SC-13

AU-09(04) Access by Subset of Privileged Users

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; Sensitive; FedRAMP Moderate, FedRAMP High

Requirements

Authorize access to management of audit logging functionality to only the subset of privileged users or roles identified in the System Security Plan (SSP).

Implementation Standards

Std.01 — Restrict access to audit logging functionality to system owners, authorized system administrators, designated security officials, and others with a valid business need and who are not subject to auditing by the system. System and network administrators must not have the ability to modify or delete audit log entries.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 10.3.1.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AU-09(04).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Individuals or roles with privileged access to a system and who are also the subject of an audit by that system may affect the reliability of the audit information by inhibiting audit activities or modifying audit records. Requiring privileged access to be further defined between audit-related privileges and other privileges limits the number of users or roles with audit-related privileges.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FIPS 140, 180, 202; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-05, CP-02, CP-04

AU-10 Non-Repudiation

Baselines

High

Overlays

PCI DSS; FedRAMP High

Requirements

Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed any processing or transmitting of TxDOT information not classified as Public.

Implementation Standards

Std.01 — Enable auditing sufficient to uniquely identify actors, actions, times of actions, and devices associated with actions (see AU-03).

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.02 PCI — Audit logs are enabled and active for all system components and cardholder data. [Source: PCI DSS 10.2.1]

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.03 FedRAMP — Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed minimum actions including the addition, modification, deletion, approval, sending, or receiving of data. [Source: FedRAMP Security Controls Baseline AU-10]

Discussion

Types of individual actions covered by non-repudiation include creating information, sending and receiving messages, and approving information. Non-repudiation protects against claims by authors of not having authored certain documents, senders of not having transmitted messages, receivers of not having received messages, and signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from an individual or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request, or receiving specific information). Organizations obtain non-repudiation services by employing various techniques or mechanisms, including digital signatures and digital message receipts.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FIPS 140, 180, 186, 202; NIST SP 800-177; PCI DSS; FedRAMP Security Controls Baseline

Related Controls

AU-09, PM-12, SA-08, SC-08, SC-12, SC-13, SC-17, SC-23

AU-11 Audit Record Retention

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Retain audit records for a time period consistent with TxDOT Records Retention schedule, not less than one year, to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Audit records include system, application, and database-level audit logs and logs for network devices. Where possible, audit records should be retained for 90 days online, after which they may be stored offline or transferred from remote access devices to a central log server for a period not less than one year.

Std.03 — When subject to a legal investigation, audit records must be maintained until released by the investigating authority. After release, maintain audit records in accordance with the records retention schedule.

Std.04 — Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. [Source: SP 800-171 3.3.1]

Std.05 — Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. [Source: SP 800-171 3.3.2]

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, Std.02 is superseded by PCI DSS requirement 10.5.1:

Std.09 PCI — Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis. [Source: PCI DSS 10.5.1]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AU-11.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standards apply:

Std.06 FedRAMP — Retain audit records for a time period in compliance with M-21-31 to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements. [Source: FedRAMP Security Controls Baseline AU-11]

Std.07 FedRAMP — The service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements. [Source: FedRAMP Security Controls Baseline AU-11]

Std.08 FedRAMP — The service provider must support Agency requirements to comply with M-21-31 (https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf) [Source: FedRAMP Security Controls Baseline AU-11]

Discussion

Organizations retain audit records until it is determined that the records are no longer needed for administrative, legal, audit, or other operational purposes. This includes the retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration

(NARA) General Records Schedules provide federal policy on records retention.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

The service provider is encouraged to align with M-21-31 where possible. [Source: FedRAMP Security Controls Baseline AU-11]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AU-02, AU-04, AU-05, AU-06, AU-09, CM-08, MP-06, RA-05, SI-12

AU-12 Audit Record Generation

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-02a on all information systems and system components where audit capability exists;

b. Allow designated personnel or roles as identified in the System Security Plan (SSP) to select the event types that are to be logged by specific components of the system; and

c. Generate audit records for the event types defined in AU-02c that include the audit record content defined in AU-03.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Where feasible, systems must provide the capability to compile audit records from multiple components into a system-wide (logical or physical) audit trail that is time-correlated to within acceptable tolerances between time stamps of individual records in the audit trail.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement AU-12.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Audit records can be generated from many different system components. The event types specified in AU-02d are the event types for which audit logs are to be generated and are a subset of all event types for which the system can generate audit records.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-06, AC-17, AU-02, AU-03, AU-04, AU-05, AU-06, AU-07, CM-05, MA-04, MP-04, PM-12, SA-08, SC-18, SI-03, SI-04, SI-07, SI-10

AU-12(01) System-Wide and Time-Correlated Audit Trail

Baselines

N/A

Overlays

FedRAMP High

Requirements

Compile audit records from all network, data storage, and computing devices into a system-wide (logical or physical) audit trail that is time-correlated to within acceptable tolerances between time stamps of individual records in the audit trail.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

AU-08, SC-45

AU-12(03) Changes by Authorized Individuals

Baselines

N/A

Overlays

FedRAMP High

Requirements

Provide and implement the capability for service provider-defined individuals or roles with audit configuration responsibilities to change the logging to be performed on all network, data storage, and computing devices based on event types the system is capable of auditing as defined in AU-02a within time thresholds defined in contracts and SLAs.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Permitting authorized individuals to make changes to system logging enables organizations to extend or limit logging as necessary to meet organizational requirements. Logging that is limited to conserve system resources may be extended (either temporarily or permanently) to address certain threat situations. In addition, logging may be limited to a specific set of event types to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which logging actions are changed (e.g., near real-time, within minutes, or within hours).

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

AC-03

CA — Assessment, Authorization, and Monitoring

CA-01 Policy and Procedures

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level assessment, authorization, and monitoring policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;

b. Designate a senior management official as defined in the assessment, authorization, and monitoring policy to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and

c. Review and update the current assessment, authorization, and monitoring:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 11.1.1 and 11.1.2.

Std.03 PCI — Rescinded in V3.0.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.04 CJIS — Review and update the current assessment, authorization, and monitoring policy and procedures following changes to the assessment criteria. [Source: CJIS CA-01]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Assessment, authorization, and monitoring policy and procedures address the controls in the CA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of assessment, authorization, and monitoring policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to assessment, authorization, and monitoring policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-12, 800-30, 800-37, 800-39, 800-53A, 800-100, 800-137, 800-137A; NIST IR 8062; PCI DSS; FedRAMP Security Controls Baseline

Related Controls

PM-09, PS-08, SI-12

CA-02 Control Assessments

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;

b. Develop a control assessment plan that describes the scope of the assessment including:

1. Controls and control enhancements under assessment;

2. Assessment procedures to be used to determine control effectiveness; and

3. Assessment environment, assessment team, and assessment roles and responsibilities;

c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;

d. Assess the controls in the system and its environment of operation at the frequency specified in Std.02 to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;

e. Produce a control assessment report that document the results of the assessment; and

f. Provide the results of the control assessment to personnel as identified in the assessment, authorization, and monitoring policy.

Implementation Standards

Std.01 — Control assessments shall be conducted at least biennially. [Source: DIR Control Standards Catalog CA-2]

Std.02 —

a. At least once every two years, TxDOT shall conduct an information security assessment of the agency's:

1. Information resources systems, network systems, digital data storage systems, digital data security measures, and information resources vulnerabilities; and

2. Data governance program with participation from the agency's data management officer, if applicable, and in accordance with requirements established by department rule.

b. Not later than November 15 of each even-numbered year, or the 60th day after the date the agency completes the assessment, whichever occurs first, TxDOT shall report the results of the assessment to:

1. The Department of Information Resources (DIR); and

2. On request, the governor, the lieutenant governor, and the speaker of the house of representatives.

c. DIR by rule shall establish the requirements for the information security assessment and report required by this section.

d. The report and all documentation related to the information security assessment and report are confidential and not subject to disclosure under Chapter 552. The state agency or department may redact or withhold the information as confidential under Chapter 552 without requesting a decision from the attorney general under Subchapter G, Chapter 552. [Source: TGC 2054.515]

Std.03 — The Information Security Officer shall be responsible for ensuring that security assessments are conducted biennially for systems containing confidential data and periodically for systems containing agency sensitive or public data. [Source: 1 TAC 202.21(b)(6)(B)]

Std.04 — Risk assessments conducted by Information Owners (or delegates) may take the place of control assessments if the system does not meet any of the following criteria:

a. High baseline;

b. Regulated Data; or

c. Confidential Internet-facing system.

Std.05 — Systems may, at the direction of the TxDOT CISO, be required to undergo a targeted or full security assessment.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.08 CJIS —

a. Assess the controls in the system and its environment of operation and any controls that have been impacted by evolving threats at least once every three years; and

b. Provide the results of the control assessment report to the individual who executed the CJIS User Agreement or is in contract with the FBI.[Source: CJIS CA-02]

TX-RAMP Correspondence

For systems subject to TX-RAMP Level 1 or Level 2 requirements, the following standard applies:

Std.05 TX-RAMP — Assess the controls in the system and its environment of operation at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements. [Source: TX-RAMP Manual CA-2]

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.06 FedRAMP —

1. Assess the controls in the system and its environment of operation at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;

2. Produce a control assessment report that document the results of the assessment; and

3. Provide the results of the control assessment to individuals or roles to include FedRAMP PMO.

[Source: FedRAMP Security Controls Baseline CA-2]

Discussion

Organizations ensure that control assessors possess the required skills and technical expertise to develop effective assessment plans and to conduct assessments of system-specific, hybrid, common, and program management controls, as appropriate. The required skills include general knowledge of risk management concepts and approaches as well as comprehensive knowledge of and experience with the hardware, software, and firmware system components implemented.

Organizations assess controls in systems and the environments in which those systems operate as part of initial and ongoing authorizations, continuous monitoring, FISMA annual assessments, system design and development, systems security engineering, privacy engineering, and the system development life cycle. Assessments help to ensure that organizations meet information security and privacy requirements, identify weaknesses and deficiencies in the system design and development process, provide essential information needed to make risk-based decisions as part of authorization processes, and comply with vulnerability mitigation procedures. Organizations conduct assessments on the implemented controls as documented in security and privacy plans. Assessments can also be conducted throughout the system development life cycle as part of systems engineering and systems security engineering processes. The design for controls can be assessed as RFPs are developed, responses assessed, and design reviews conducted. If a design to implement controls and subsequent implementation in accordance with the design are assessed during development, the final control testing can be a simple confirmation utilizing previously completed control assessment and aggregating the outcomes.

Organizations may develop a single, consolidated security and privacy assessment plan for the system or maintain separate plans. A consolidated assessment plan clearly delineates the roles and responsibilities for control assessment. If multiple organizations participate in assessing a system, a coordinated approach can reduce redundancies and associated costs.

Organizations can use other types of assessment activities, such as vulnerability scanning and system monitoring, to maintain the security and privacy posture of systems during the system life cycle. Assessment reports document assessment results in sufficient detail, as deemed necessary by

organizations, to determine the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting requirements. Assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of authorization decisions are provided to authorizing officials, senior agency officials for privacy, senior agency information security officers, and authorizing official designated representatives.

To satisfy annual assessment requirements, organizations can use assessment results from the following sources: initial or ongoing system authorizations, continuous monitoring, systems engineering processes, or system development life cycle activities. Organizations ensure that assessment results are current, relevant to the determination of control effectiveness, and obtained with the appropriate level of assessor independence. Existing control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. After the initial authorizations, organizations assess controls during continuous monitoring. Organizations also establish the frequency for ongoing assessments in accordance with organizational continuous monitoring strategies. External audits, including audits by external entities such as regulatory agencies, are outside of the scope of CA-02.

TxDOT Discussion

A Control Assessment Plan that describes the scope of the assessment should be developed to include:

1. The controls and control enhancements under assessment;

2. The assessment procedures to be used to determine control effectiveness;

3. Required documentation and supporting materials, including but not limited to:

a. System Security Plan (SSP);

b. Interconnection Security Assessments (ISAs);

c. System Categorization;

d. Plan of Action and Milestones (POAM);

e. Contingency Plan;

f. Relevant and valid test results, assessments, continuous monitoring results, audits, reviews; and

g. Service Layer Agreements (SLAs) if applicable.

4. The assessment environment, assessment, team, and assessment roles and responsibilities; and

5. Any additional information required for the Control Assessment Report (CAR).

Note for systems subject to FedRAMP Requirements:

Reference FedRAMP Annual Assessment Guidance. [Source: FedRAMP Security Controls Baseline CA-2]

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; TGC 2054; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; FIPS 199; NIST SP 800-18, 800-37, 800-39, 800-53A, 800-115, 800-137; NIST IR 8011-1, 8062; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-20, CA-05, CA-06, CA-07, IR-08, PM-09, RA-05, SA-11, SI-03, SI-12, SR-02, SR-03

CA-02(01) Independent Assessors

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Employ independent assessors or assessment teams to conduct control assessments.

Implementation Standards

Std.01 — Only high-rated systems, moderate-rated systems with Regulated data, and moderate-rated systems with Confidential data that are also Internet facing, must have a control assessment conducted by an independent assessor or assessment team, unless otherwise directed by the TxDOT CISO.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CA-02(01).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low baseline.

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.02 FedRAMP — For JAB Authorization, must use an accredited 3PAO. [Source: FedRAMP Security Controls Baseline CA-2(1)]

Discussion

Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of systems. Impartiality means that assessors are free from any perceived or actual conflicts of interest regarding the development, operation, sustainment, or management of the systems under assessment or the determination of control effectiveness. To achieve impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in positions of advocacy for the organizations acquiring their services.

Independent assessments can be obtained from elements within organizations or be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of systems and/or the risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. Assessor independence determination includes whether contracted assessment services have sufficient independence, such as when system owners are not directly involved in contracting processes or cannot influence the impartiality of the assessors conducting the assessments. During the system design and development phase, having independent assessors is analogous to having independent SMEs involved in design reviews.

When organizations that own the systems are small or the structures of the organizations require that assessments be conducted by individuals that are in the developmental, operational, or management chain of the system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Assessments performed for purposes other than to support authorization decisions are more likely to be useable for such decisions when performed by assessors with sufficient independence, thereby reducing the need to repeat assessments.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; FIPS 199; NIST SP 800-18, 800-37, 800-39, 800-53A, 800-115, 800-137; NIST IR 8011-1, 8062; FedRAMP Security Controls Baseline

Related Controls

None.

CA-02(02) Specialized Assessments

Baselines

N/A

Overlays

FedRAMP High

Requirements

Include as part of control assessments, at least annually, announced vulnerability scanning.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Organizations can conduct specialized assessments, including verification and validation, system monitoring, insider threat assessments, malicious user testing, and other forms of testing. These assessments can improve readiness by exercising organizational capabilities and indicating current levels of performance as a means of focusing actions to improve security and privacy. Organizations conduct specialized assessments in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can include vulnerabilities uncovered during assessments into vulnerability remediation processes. Specialized assessments can also be

conducted early in the system development life cycle (e.g., during initial design, development, and unit testing).

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

PE-03, SI-02

CA-02(03) Leveraging Results from External Organizations

Baselines

N/A

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

Leverage the results of control assessments performed by any FedRAMP Accredited Third Party Assessment Organization (3PAO) on systems that do not require TX-RAMP certification when the assessment meets the conditions of the Joint Authorization Board (JAB)/Authorizing Official (AO) in the FedRAMP Repository.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Organizations may rely on control assessments of organizational systems by other (external) organizations. Using such assessments and reusing existing assessment evidence can decrease the time and resources required for assessments by limiting the independent assessment activities that organizations need to perform. The factors that organizations consider in determining whether to accept assessment results from external organizations can vary. Such factors include the organization's past experience with the organization that conducted the assessment, the reputation of the assessment organization, the level of detail of supporting assessment evidence provided, and mandates imposed by applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Accredited testing laboratories that support the Common Criteria Program ISO 15408-1, the NIST Cryptographic Module Validation Program (CMVP), or the NIST Cryptographic Algorithm Validation Program (CAVP) can provide independent assessment results that organizations can leverage.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

SA-04

CA-03 Information Exchange

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Approve and manage the exchange of information between the system and other systems using interconnection security agreements (ISAs);

b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and

c. Review and update the agreements annually.

Implementation Standards

Std.01 — Authorize all connections from internal/organization information system to other information systems outside of TxDOT through the use of ISAs and monitor/control the system connections on an ongoing basis.

Std.02 — All ISAs must be approved by the Authorizing Official and the Information Security Officer.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirements 5.1 and 5.1.1.

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Rescinded in V4.0.

Std.04 CJIS — Rescinded in V4.0.

Std.06 CJIS —

a. Approve and manage the exchange of information between the agency system and external systems using the following agreements when applicable;

1. Executed CJIS User Agreements

a. Each CSA, SIB, or IA shall execute a signed written agreement (see Appendix D.1) with the FBI CJIS Division stating their willingness to demonstrate conformity with the CJISSECPOL before accessing and consuming CJIS systems and services as set forth in the agreement.

b. The agreement shall include the standards, audit, and sanctions governing utilization of CJIS systems and services.

c. The FBI CJIS Division is authorized to periodically test the ability to penetrate the FBI's network through the external connection or system upon proper notification of all signatories in the user agreement.

2. Criminal Justice Agency User Agreements

a. Any CJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access.

b. The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere. These agreements shall include:

i. Audit;

ii. Dissemination;

iii. Hit confirmation;

iv. Logging;

v. Quality Assurance (QA);

vi. Screening (Criminal Justice Employment);

vii. Security;

viii. Timeliness;

ix. Training;

x. Use of the system; and

xi. Validation.

3. Agreements for Noncriminal Justice Use of CHRI

A CJA, NCJA (public), or NCJA (private) designated to request civil fingerprint-based background checks, with full consent of the individual to whom the background check is taking place, for noncriminal justice functions, shall be eligible for access to CHRI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. The CJA, NCJA (public), or NCJA (private) receiving access to CHRI shall enter into signed written agreements with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. The written agreement shall specify the policies to which the agency must adhere, which includes all pertinent areas of the CJISSECPOL. Each NCJA that directly access FBI systems shall allow the FBI to periodically test the ability to penetrate the FBI's network through the external connection or system. A CJA, NCJA (public), or NCJA (private) authorized to access CHRI for noncriminal justice functions pursuant to federal law or state statute approved by the U.S. Attorney General (defined by the Compact Council as an Authorized Recipient), cannot make CHRI available to another governmental agency, nongovernmental agency, or private contractor to perform noncriminal justice administrative functions without implementation of one of the following:

a. Security and Management Control Outsourcing Standard for Non-Channelers. Implementation is applicable to noncriminal justice administrative functions that do not require a direct connection to the FBI for submission of fingerprints and receipt of CHRI. Examples include making fitness determinations, processing, storing, or destroying documents, and maintaining IT platforms that do not connect to CJIS systems. Prior to implementation, Authorized Recipients must request and receive written permission from the State Compact Officer, Chief Administrator of the state's criminal history record repository, or the FBI Compact Officer, as applicable.

b. Security and Management Control Outsourcing Standard for Channeling. Implementation is applicable only to Channeling functions performed by an FBI-approved Channeler that require a direct connection to the FBI for submission of fingerprints and receipt of CHRI. Prior to implementation, Authorized Recipients must request and receive written permission from the State Compact Officer, Chief Administrator of the state's criminal history record repository, or the FBI Compact Officer, as applicable.

c. Management Control Agreement or Security Addendum (see Appendix H) pursuant to Title 28, C.F.R., Section 20.33 (a) (6) or (7). Although by regulation implementation of a Management Control Agreement or the Security Addendum is applicable to the administration of criminal justice pursuant to that agreement performed on behalf of CJAs, under very limited circumstances, implementation may also be applicable to CJAs that obtain and use CHRI for noncriminal justice purposes. Implementation for noncriminal justice purposes is only applicable when another governmental agency or private contractor performs both criminal justice and noncriminal justice administrative functions involving access to CHRI on behalf of the CJA. It is important to note that if the servicing governmental agency or private contractor solely performs noncriminal justice administrative functions, then the CJA would be required to implement the Security and Management Control Outsourcing Standard for Non-Channelers.

b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and

c. Review and update the agreements at least triennially or when responsibilities or signatories change.

d. Secondary Dissemination

1. Log the dissemination of CHRI when released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s). If CJI does not contain CHRI and is not part of an information exchange agreement, then it does not need to be logged.

2. Validate the requestor of CJI in conformance with the local policy as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission; or a member of the public receiving CJI via authorized dissemination. [Source: CJIS CA-03]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.05 FedRAMP — Review and update the agreements at least annually and on input from Joint Authorization Board (JAB)/Authorizing Official (AO). [Source: FedRAMP Security Controls Baseline CA-3]

Discussion

System information exchange requirements apply to information exchanges between two or more systems. System information exchanges include connections via leased lines or virtual private networks, connections to internet service providers, database sharing or exchanges of database transaction information, connections and exchanges with cloud services, exchanges via web-based services, or exchanges of files via file transfer protocols, network protocols (e.g., IPv4, IPv6), email, or other organization-to-organization communications. Organizations consider the risk related to new or increased threats that may be introduced when systems exchange information with other systems that may have different security and privacy requirements and controls. This includes systems within the same organization and systems that are external to the organization. A joint authorization of the systems exchanging information, as described in CA-06(01) or CA-06(02), may help to communicate and reduce risk.

Authorizing officials determine the risk associated with system information exchange and the controls needed for appropriate risk mitigation. The types of agreements selected are based on factors such as the impact level of the information being exchanged, the relationship between the organizations exchanging information (e.g., government to government, government to business, business to business, government or business to service provider, government or business to individual), or the level of access to the organizational system by users of the other system. If systems that exchange information have the same authorizing official, organizations need not develop agreements. Instead, the interface characteristics between the systems (e.g., how the information is being exchanged. how the information is protected) are described in the respective security and privacy plans. If the systems that exchange information have different authorizing officials within the same organization, the organizations can develop agreements or provide the same information that would be provided in the appropriate agreement type from CA-03a in the respective security and privacy plans for the systems. Organizations may incorporate agreement information into formal contracts, especially for information exchanges established between federal agencies and nonfederal organizations (including service providers, contractors, system developers, and system integrators). Risk considerations include systems that share the same networks.

TxDOT Discussion

State Implementation Details

Information resources assigned from or shared between one state agency to another or from or between a state agency to a third-party shall be protected in accordance with the conditions imposed by the providing state agency at a minimum. [Source: DIR Control Standards Catalog CA-3]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; FIPS 199; NIST SP 800-47; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-04, AC-20, CA-06, IA-03, IR-04, PL-02, PT-07, RA-03, SA-09, SC-07, SI-12

CA-03(06) Transfer Authorizations

Baselines

N/A

Overlays

FedRAMP High

Requirements

Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

To prevent unauthorized individuals and systems from making information transfers to protected systems, the protected system verifies—via independent means—whether the individual or system attempting to transfer information is authorized to do so. Verification of the authorization to transfer information also applies to control plane traffic (e.g., routing and DNS) and services (e.g., authenticated SMTP relays).

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

AC-02, AC-03, AC-04

CA-05 Plan of Action and Milestones

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and

b. Update existing plan of action and milestones as corrective actions occur, and review at least quarterly until all findings are resolved, based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — An agency-wide information security program must be approved by the agency head and include a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency. [Source: 1 TAC 202.24(a)(5)]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CA-05.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standards apply:

Std.03 FedRAMP — Update existing plan of action and milestones at least monthly based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities. [Source: FedRAMP Security Controls Baseline CA-5]

Std.04 FedRAMP — POA&Ms must be provided at least monthly. [Source: FedRAMP Security Controls Baseline CA-5]

Discussion

Plans of action and milestones are useful for any type of organization to track planned remedial actions. Plans of action and milestones are required in authorization packages and subject to federal reporting requirements established by OMB.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

Reference FedRAMP-POAM-Template. [Source: FedRAMP Security Controls Baseline CA-5]

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-37; FedRAMP Security Controls Baseline

Related Controls

CA-02, CA-07, PM-04, PM-09, RA-07, SI-02, SI-12

CA-06 Authorization

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Assign a senior official as the authorizing official for the system;

b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;

c. Ensure that the authorizing official for the system, before commencing operations:

1. Accepts the use of common controls inherited by the system; and

2. Authorizes the system to operate;

d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;

e. Update the authorizations per Stds.05 & 06.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Rescinded in V2.2.

Std.03 — The TxDOT Executive Director or their designated representative(s) shall approve high level residual risk management decisions as required by 1 TAC 202. [Source: 1 TAC 202.20(b)(6)]

Std.04 — Approval of the security risk acceptance, transference, or mitigation decision shall be the responsibility of the Information Security Officer or their designee(s), in coordination with the information owner, for systems identified with a Low or Moderate residual risk; and the TxDOT Executive Director for all systems identified with a High residual risk. [Source: 1 TAC 202.25(4)]

Std.05 — The security authorization for a system is updated:

a. When significant changes are made to the system;

b. When changes in requirements result in a different security baseline;

c. When changes occur to authorizing legislation, regulatory standards, or federal requirements that impact the system;

d. After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; or

e. Based on classification,

1. High: One year after the last authorization;

2. Moderate: Two years after the last authorization;

3. Low: Four years after the last authorization.

Std.06 — The security authorization for common controls is updated:

a. When changes occur to authorizing legislation, organization policy, regulatory standards, or federal requirements that affect the controls;

b. After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; or

c. Based on classification,

1. High: One year after the last authorization;

2. Moderate: Two years after the last authorization;

3. Low: Four years after the last authorization.

Std.07 — Assessments, authorizations, and decisions may be included in the accreditation package in accordance with the TxDOT Authority to Operate process.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, CA-06 b. and e. are superseded by the following requirements from CJIS CA-06:

Std.04 CJIS —

a. Assign the CSO, SIB Chief, or IA Official as the authorizing official for common controls available for inheritance by organizational systems;

b. Update the authorizations at least every three (3) years. [Source: CJIS CA-06]

TX-RAMP Correspondence

For systems subject to TX-RAMP Level 1 or Level 2 requirements, the following standard applies:

Std.09 — Update the authorizations at least every three years or when a significant change occurs. [Source: TX-RAMP Manual CA-6]

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.08 FedRAMP — Update the authorizations in accordance with OMB A-130 requirements or when a significant change occurs. [Source: FedRAMP Security Controls Baseline CA-6]

Discussion

Authorizations are official management decisions by senior officials to authorize operation of systems, authorize the use of common controls for inheritance by organizational systems, and explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon controls. Authorizing officials provide budgetary oversight for organizational systems and common controls or assume responsibility for the mission and business functions supported by those systems or common controls. The authorization process is a federal responsibility, and therefore, authorizing officials must be federal employees. Authorizing officials are both responsible and accountable for security and privacy risks associated with the operation and use of organizational systems. Nonfederal organizations may have similar processes to authorize systems and senior officials that assume the authorization role and associated responsibilities.

Authorizing officials issue ongoing authorizations of systems based on evidence produced from implemented continuous monitoring programs. Robust continuous monitoring programs reduce the need for separate reauthorization processes. Through the employment of comprehensive continuous monitoring processes, the information contained in authorization

packages (i.e., security and privacy plans, assessment reports, and plans of action and milestones) is updated on an ongoing basis. This provides authorizing officials, common control providers, and system owners with an up-to-date status of the security and privacy posture of their systems, controls, and operating environments. To reduce the cost of reauthorization, authorizing officials can leverage the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F and according to FedRAMP Significant Change Policies and Procedures. The service provider describes the types of changes to the information system or the environment of operations that would impact the risk posture. The types of changes are approved and accepted by the JAB/AO. [Source: FedRAMP Security Controls Baseline CA-6]

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-37, 800-137; FedRAMP Security Controls Baseline

Related Controls

CA-02, CA-03, CA-07, PM-09, PM-10, RA-03, SA-10, SI-12

CA-07 Continuous Monitoring

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

a. Establishing the following system-level metrics to be monitored: metrics defined in the Continuous Monitoring Program;

b. Establishing frequencies as specified in the Continuous Monitoring Program for monitoring and frequencies as specified in the program's requirement documents for assessment of control effectiveness;

c. Ongoing control assessments in accordance with the continuous monitoring strategy;

d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;

e. Correlation and analysis of information generated by control assessments and monitoring;

f. Response actions to address results of the analysis of control assessment and monitoring information; and

g. Reporting the security and privacy status of the system to the personnel and at the frequencies specified in Stds.02 & 03.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The Information Security Officer shall be responsible for reporting, at least annually, directly to the TxDOT Executive Director the status and effectiveness of the security program and its controls. [Source: 1 TAC 202.21(b)(11)]

Std.03 — The Information Security Officer shall directly report to the TxDOT Executive Director, at least annually, on the adequacy and effectiveness of information security policies, procedures, practices, and compliance with the requirements of 1 TAC 202 and the effectiveness of current information security program and status of key initiatives. [Source: 1 TAC 202.23(a),(a)(1)]

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.04 PCI — Ensure that the following is included in contracts or SLAs for service providers: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks:

a. Daily log reviews.

b. Configuration reviews for network security controls.

c. Applying configuration standards to new systems.

d. Responding to security alerts.

e. Change-management processes.

[Source: PCI DSS 12.4.2]

Std.05 PCI — Ensure that the following is included in contracts or SLAs for service providers: Reviews conducted in accordance with Requirement 12.4.2 are documented to include:

a. Results of the reviews.

b. Documented remediation actions taken for any tasks that were found to not be performed at Requirement 12.4.2.

c. Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program.

[Source: PCI DSS 12.4.2.1]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.09 CJIS — Report the security and privacy status of the system to organizational personnel with information security, privacy responsibilities, and system/network administrators annually, when security events/incidents occur, and when requested. [Source: CJIS CA-07]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.06 FedRAMP — Include, in the system-level continuous monitoring strategy, reporting the security and privacy status of the system to the Joint Authorization Board (JAB)/Authorizing Official (AO). [Source: FedRAMP Security Controls Baseline CA-7]

Std.07 FedRAMP — Operating System, Database, Web Application, Container, and Service Configuration Scans: at least monthly. All scans performed by Independent Assessor: at least annually. [Source: FedRAMP Security Controls Baseline CA-7]

Std.08 FedRAMP — Cloud Service Offerings (CSOs) with more than one agency ATO must implement a collaborative Continuous Monitoring (ConMon) approach described in the FedRAMP Guide for Multi-Agency Continuous Monitoring. This requirement applies to CSOs authorized via the Agency path as each agency customer is responsible for performing ConMon oversight. It does not apply to CSOs authorized via the Joint Authorization Board (JAB) path because the JAB performs ConMon oversight. [Source: FedRAMP Security Controls Baseline CA-7]

Discussion

Continuous monitoring at the system level facilitates ongoing awareness of the system security and privacy posture to support organizational risk management decisions. The terms "continuous" and "ongoing" imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. The results of continuous monitoring generate risk response actions by organizations. When monitoring the effectiveness of multiple controls that have been grouped into capabilities, a root-cause analysis may be needed to determine the specific control that has failed. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security and privacy information on a continuing basis through reports and dashboards gives organizational officials the ability to make effective

and timely risk management decisions, including ongoing authorization decisions.

Automation supports more frequent updates to hardware, software, and firmware inventories, authorization packages, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of systems. Monitoring requirements, including the need for specific monitoring, may be referenced in other controls and control enhancements, such as AC-02g, AC-17(01), AT-04a, CM-03f, CM-06d, CM-11c, IR-05, MA-02b, MA-03a, MA-04a, PE-03d, PE-06, PE-14b, PE-16, PM-06, PM-31, PS-07e, SA-09c, SC-07a, SC-07(24)(b), SC-18b, SC-43b, SI-04, and SR-04.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

FedRAMP does not provide a template for the Continuous Monitoring Plan. CSPs should reference the FedRAMP Continuous Monitoring Strategy Guide when developing the Continuous Monitoring Plan. [Source: FedRAMP Security Controls Baseline CA-7]

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-37, 800-39, 800-53A, 800-115, 800-137; NIST IR 8011-1, 8062; PCI DSS; FedRAMP Security Controls Baseline

Related Controls

AC-02, AC-06, AC-17, AT-04, AU-06, CA-02, CA-05, CA-06, CM-03, CM-04, CM-06, CM-11, IA-05, IR-05, MA-02, MA-03, MA-04, PE-03, PE-06, PE-14, PE-16, PL-02, PM-04, PM-06, PM-09, PM-10, PM-12, PM-14, PM-28, PM-31, PS-07, PT-07, RA-03, RA-05, RA-07, SA-08, SA-09, SA-11, SC-05, SC-07, SC-18, SI-03, SI-04, SI-12, SR-06

CA-07(01) Independent Assessment

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

Implementation Standards

Std.01 — Employ assessors at the TxDOT CISO-defined level of independence in accordance with CA-02 and CA-02(01).

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CA-07(01).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organizations maximize the value of control assessments by requiring that assessments be conducted by assessors with appropriate levels of independence. The level of required independence is based on organizational continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in advocacy positions for the organizations acquiring their services.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; NIST SP 800-37, 800-39, 800-53A, 800-115, 800-137; NIST IR 8011-1, 8062; FedRAMP Security Controls Baseline

Related Controls

None.

CA-07(04) Risk Monitoring

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

a. Effectiveness monitoring;

b. Compliance monitoring; and

c. Change monitoring.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CA-07(04).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Risk monitoring is informed by the established organizational risk tolerance. Effectiveness monitoring determines the ongoing effectiveness of the implemented risk response measures. Compliance monitoring verifies that required risk response measures are implemented. It also verifies that security and privacy requirements are satisfied. Change monitoring identifies changes to organizational systems and environments of operation that may affect security and privacy risk.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-37, 800-39, 800-53A, 800-115, 800-137; NIST IR 8011-1, 8062; FedRAMP Security Controls Baseline

Related Controls

None.

CA-08 Penetration Testing

Baselines

Moderate, High

Overlays

PCI DSS; Privacy; TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Conduct penetration testing at the frequency identified in Std.02 on assets as identified in Std.03 that create, access, process, transmit, or store any TxDOT information classified as Confidential or Regulated.

Implementation Standards

Std.01 — Data Security Plan for Online and Mobile Applications

a. Each state agency implementing an Internet website or mobile application that processes any sensitive personal or personally identifiable information or confidential information must:

1. Submit a biennial data security plan to the Department of Information Resources not later than June 1 of each even-numbered year to establish planned beta testing for the website or application; and

2. Subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test.

[Source: TGC 2054.516(a)]

Std.02 — Penetration Test Frequency

a. Internet websites and mobile application penetration tests:

1. Prior to an authority to operate being granted for the system to go into production.

2. Whenever there is a major system change.

b. Organization performs external facing penetration test at least annually.

Std.03 — Penetration Test Types

a. Internet websites and mobile application penetration tests: Conduct a penetration test that includes both credentialed and non-credentialed dynamic application security testing

b. Organization performs external-facing penetration test: Conduct a penetration test that includes:

1. Coverage for the entire environment, perimeter, and critical systems; and

2. Reviewing and considering threats and vulnerabilities experienced in the last 12 months.

Std.04 — All identified vulnerabilities must be documented in the organization's risk register.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.05 PCI — A penetration testing methodology is defined, documented, and implemented by the entity, and includes:

a. Industry-accepted penetration testing approaches.

b. Coverage for the entire Cardholder Data Environment (CDE) perimeter and critical systems.

c. Testing from both inside and outside the network.

d. Testing to validate any segmentation and scope- reduction controls.

e. Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4.

f. Network-layer penetration tests that encompass all components that support network functions as well as operating systems.

g. Review and consideration of threats and vulnerabilities experienced in the last 12 months.

h. Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing.

i. Retention of penetration testing results and remediation activities results for at least 12 months.

[Source: PCI DSS 11.4.1]

Std.06 PCI — External penetration testing is performed:

a. Per the entity's defined methodology;

b. At least once every 12 months;

c. After any significant infrastructure or application upgrade or change;

d. By a qualified internal resource or qualified external third party; and

e. Organizational independence of the tester exists (not required to be a Qualified Security Assessor (QSA) or Approved Scanning Vendor (ASV)).

[Source: PCI DSS 11.4.3]

Std.07 PCI — Internal penetration testing is performed:

a. Per the entity's defined methodology;

b. At least once every 12 months;

c. After any significant infrastructure or application upgrade or change;

d. By a qualified internal resource or qualified external third-party; and

e. Organizational independence of the tester exists (not required to be a QSA or ASV).

[Source: PCI DSS 11.4.2]

Std.08 PCI — Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows:

a. In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1.

b. Penetration testing is repeated to verify the corrections.

[Source: PCI DSS 11.4.4]

Std.09 PCI — If segmentation is used to isolate the Cardholder Data Environment (CDE) from other networks, penetration tests are performed on segmentation controls as follows:

a. At least once every 12 months and after any changes to segmentation controls/methods.

b. Covering all segmentation controls/methods in use.

c. According to the entity's defined penetration testing methodology.

d. Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems.

e. Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3).

f. Performed by a qualified internal resource or qualified external third party.

g. Organizational independence of the tester exists (not required to be a Qualified Security Assessor (QSA) or Approved Scanning Vendor (ASV)).

[Source: PCI DSS 11.4.5]

Std.10 PCI — Ensure that the following is included in contracts or SLAs for service providers: If segmentation is used to isolate the Cardholder Data Environment (CDE) from other networks, penetration tests are performed on segmentation controls as follows:

a. At least once every six months and after any changes to segmentation controls/methods.

b. Covering all segmentation controls/methods in use.

c. According to the entity's defined penetration testing methodology.

d. Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems.

e. Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3).

f. Performed by a qualified internal resource or qualified external third party.

g. Organizational independence of the tester exists (not required to be a Qualified Security Assessor (QSA) or Approved Scanning Vendor (ASV)).

[Source: PCI DSS 11.4.6]

Std.12 PCI — Ensure that the following is included in contracts or SLAs for service providers: Multi-tenant service providers support their customers for

external penetration testing per Requirement 11.4.3 and 11.4.4. [Source: PCI DSS 11.4.7]

CJIS Correspondence

Std.11 CJIS — Rescinded in v4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is conducted by agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application level security. Penetration testing can be used to validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include time, resources, and skills. Penetration testing attempts to duplicate the actions of adversaries and provides a more in-depth analysis of security- and privacy-related weaknesses or deficiencies. Penetration testing is especially important when organizations are transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols).

Organizations can use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted internally or externally on the hardware, software, or firmware components of a system and can exercise both physical and technical controls. A standard method for penetration testing includes a pretest analysis based on full knowledge of the system, pretest identification of potential vulnerabilities based on the pretest analysis, and testing designed to determine the exploitability of vulnerabilities. All parties agree to the rules of engagement before commencing penetration testing scenarios. Organizations correlate the rules of engagement for the penetration tests with the tools, techniques, and procedures that are anticipated to be employed by adversaries. Penetration testing may result in the exposure of information that is protected by laws or regulations, to individuals conducting the testing. Rules of engagement, contracts, or other appropriate mechanisms can be used to

communicate expectations for how to protect this information. Risk assessments guide the decisions on the level of independence required for the personnel conducting penetration testing.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

Reference the FedRAMP Penetration Test Guidance. [Source: FedRAMP Security Controls Baseline CA-8]

TxDOT References

Information Security and Privacy Policy

State References

TGC 2054; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

RA-05, SA-09, SA-11, SR-05, SR-06

CA-08(01) Independent Penetration Testing Agent or Team

Baselines

N/A

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Independent penetration testing agents or teams are individuals or groups who conduct impartial penetration testing of organizational systems. Impartiality implies that penetration testing agents or teams are free from perceived or actual conflicts of interest with respect to the development, operation, or management of the systems that are the targets of the penetration testing. CA-02(01) provides additional information on independent assessments that can be applied to penetration testing.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

CA-02

CA-08(02) Red Team Exercises

Baselines

N/A

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement: red team exercises as defined in the Incident Response Plan (IRP).

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Red team exercises extend the objectives of penetration testing by examining the security and privacy posture of organizations and the capability to implement effective cyber defenses. Red team exercises simulate attempts by adversaries to compromise mission and business functions and provide a comprehensive assessment of the security and privacy posture of systems and organizations. Such attempts may include technology-based attacks and social engineering-based attacks. Technology-based attacks include interactions with hardware, software, or firmware components and/or mission and business processes. Social engineering-

based attacks include interactions via email, telephone, shoulder surfing, or personal conversations. Red team exercises are most effective when conducted by penetration testing agents and teams with knowledge of and experience with current adversarial tactics, techniques, procedures, and tools. While penetration testing may be primarily laboratory-based testing, organizations can use red team exercises to provide more comprehensive assessments that reflect real-world conditions. The results from red team exercises can be used by organizations to improve security and privacy awareness and training and to assess control effectiveness.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

See the FedRAMP Documents page > Penetration Test Guidance

https://www.FedRAMP.gov/documents/ [Source: FedRAMP Security Controls Baseline CA-8(2)]

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

CA-09 Internal System Connections

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Authorize internal connections of all system components or classes of components defined in the applicable System Security Plan (SSP) to the system;

b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;

c. Terminate internal system connections after session limits specified in the TxDOT Identification and Authentication Standard; and

d. Review at the frequency specified in the Continuous Monitoring Program, or at least annually if not otherwise specified, the continued need for each internal connection.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — For any system categorized as moderate or high, the System Security Plan (SSP) will identify the types of personally owned equipment that may be internally connected with organizational information systems and networks, compliant with TxDOT mobile device security policies.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CA-09.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Internal system connections are connections between organizational systems and separate constituent system components (i.e., connections between components that are part of the same system) including components used

for system development. Intra-system connections include connections with mobile devices, notebook and desktop computers, tablets, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each internal system connection individually, organizations can authorize internal connections for a class of system components with common characteristics and/or configurations, including printers, scanners, and copiers with a specified processing, transmission, and storage capability or smart phones and tablets with a specific baseline configuration. The continued need for an internal system connection is reviewed from the perspective of whether it provides support for organizational missions or business functions.

TxDOT Discussion

None.

TxDOT References

Identification and Authentication Standard; Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-124; NIST IR 8023; FedRAMP Security Controls Baseline

Related Controls

AC-03, AC-04, AC-18, AC-19, CM-02, IA-03, SC-07, SI-12

CM — Configuration Management

CM-01 Policy and Procedures

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level configuration management policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;

b. Designate a senior management official as defined in the configuration management policy to manage the development, documentation, and dissemination of the configuration management policy and procedures; and

c. Review and update the current configuration management:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 2.1.1 and 2.1.2.

Std.03 PCI — Rescinded in V3.0.

Std.04 PCI — Rescinded in V3.0.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.05 CJIS — Review and update the current configuration management policy and procedures following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. [Source: CJIS CM-01]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Configuration management policy and procedures address the controls in the CM family that are implemented within systems and organizations. The risk

management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of configuration management policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to configuration management policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-12, 800-30, 800-39, 800-100; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

PM-09, PS-08, SA-08, SI-12

CM-02 Baseline Configuration

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and

b. Review and update the baseline configuration of the system:

1. Annually;

2. When required due to a major system change; and

3. When system components are installed or upgraded.

Implementation Standards

Std.01 — TxDOT must keep confidential its network security information as detailed in its Information Security Monitoring Baseline Configuration Specifications. [Source: TGC 2059.055(b)(1, 2, 3)]

Std.02 — Information Resource Technology (IRT) assets must comply with the TxDOT Information Security Minimum Configuration Baseline Standard.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, CM-02b.1 is superseded by PCI DSS requirement 1.2.7:

Std.03 PCI — Configurations of Network Security Controls (NSCs) are reviewed at least once every six months to confirm they are relevant and effective. [Source: PCI DSS 1.2.7]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.04 CJIS — When an agency allows mobile devices that are approved to access or store CJI to function as Wi-Fi hotspots connecting to the Internet, they shall be configured, at a minimum, as follows:

a. Enable encryption on the hotspot;

b. Change the hotspot's default SSID;

1. Ensure the hotspot SSID does not identify the device make/model or agency ownership;

c. Create a wireless network password (Pre-shared key);

d. Enable the hotspot's port filtering/blocking features if present; and

e. Only allow connections from agency controlled devices. [Source: CJIS 5.20.1.4]

Std.06 CJIS —

a. Develop, document, and maintain a current and complete topological drawing depicting the interconnectivity of the agency network to criminal justice information systems and services; and

b. Review and update the baseline configuration and topological drawing of the system:

1. At least annually;

2. When required due to security-relevant changes to the system and/or security incidents occur; and

3. When system components are installed or upgraded. [Source: CJIS CM-02]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low baseline.

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.05 FedRAMP — Review and update the baseline configuration of the system when directed by the Joint Authorization Board (JAB). [Source: FedRAMP Security Controls Baseline CM-2]

Discussion

Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines as organizational systems change over time. Baseline configurations of systems reflect the current enterprise architecture.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

TGC 2059; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-124, 800-128; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-19, AU-06, CA-09, CM-01, CM-03, CM-05, CM-06, CM-08, CM-09, CP-09, CP-10, MA-02, PL-08, PM-05, SA-08, SA-10, SA-15, SC-18

CM-02(02) Automation Support for Accuracy and Currency

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; FedRAMP Moderate, FedRAMP High

Requirements

Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using automated mechanisms as defined in applicable System Security Plans (SSPs).

Implementation Standards

None.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.01 PCI — Configuration files for Network Security Controls (NSCs) are:

a. Secured from unauthorized access.

b. Kept consistent with active network configurations.

[Source: PCI DSS 1.2.8]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CM-02(02).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Automated mechanisms that help organizations maintain consistent baseline configurations for systems include configuration management tools, hardware, software, firmware inventory tools, and network management tools. Automated tools can be used at the organization level, mission and business process level, or system level on workstations, servers, notebook computers, network components, or mobile devices. Tools can be used to track version numbers on operating systems, applications, types of software installed, and current patch levels. Automation support for accuracy and

currency can be satisfied by the implementation of CM-08(02) for organizations that combine system component inventory and baseline configuration activities.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-124, 800-128; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CM-07, IA-03, RA-05

CM-02(03) Retention of Previous Configurations

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Retain at least the latest approved and a minimum of two previous versions of baseline configurations of the system to support rollback.

Implementation Standards

Std.01 — Storage must comply with CM-02.

Std.02 — Changes to all system components in the production environment are made according to established procedures that include procedures to address failures and return to a secure state. [Source: PCI DSS 6.5.1]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 6.5.1.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CM-02(03).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Retaining previous versions of baseline configurations to support rollback includes hardware, software, firmware, configuration files, configuration records, and associated documentation.

TxDOT Discussion

None.

TxDOT References

Data Classification Policy; Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-124, 800-128; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

CM-02(07) Configure Systems and Components for High-Risk Areas

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

a. Issue travel-configured information technology assets when Std.01 applies with whole-disk encryption and mandatory remote access connection authorized per AC-17 to individuals traveling to locations that the organization deems to be of significant risk; and

b. Apply the following controls to the systems or components when the individuals return from travel: malware scanning and reimaging.

Implementation Standards

Std.01 — Applies to any information technology assets being transported to countries listed on the US Department of State's travel advisory website that has a level of advice "Level 2 – Exercise increased caution" or higher.

Std.02 — Examine returned computers for signs of tampering.

a. If evidence exists, follow the implementation standards established in IR-06;

b. If evidence of tampering does not exist, follow standard operating procedures to have the equipment scanned for malware and re-imaged for the next travelling user.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement 5.20.1.2.1.

For systems processing CJIS data, CM-02(07)a is superseded by CJIS requirement CM-02(07)a:

Std.03 CJIS — Issue devices (e.g., mobile devices) with CJISSECPOL compliant configurations to individuals traveling to locations that the organization deems to be of significant risk. [Source: CJIS CM-02(07)]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

When it is known that systems or system components will be in high-risk areas external to the organization, additional controls may be implemented to counter the increased threat in such areas. For example, organizations can take actions for notebook computers used by individuals departing on and returning from travel. Actions include determining the locations that are of concern, defining the required configurations for the components, ensuring that components are configured as intended before travel is initiated, and applying controls to the components after travel is completed. Specially configured notebook computers include computers with sanitized hard drives, limited applications, and more stringent configuration settings. Controls applied to mobile devices upon return from travel include examining the mobile device for signs of physical tampering and purging and reimaging disk drives. Protecting information that resides on mobile devices is addressed in the MP (Media Protection) family.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-124, 800-128; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

MP-04, MP-05

CM-03 Configuration Change Control

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Determine and document the types of changes to the system that are configuration-controlled;

b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;

c. Document configuration change decisions associated with the system;

d. Implement approved configuration-controlled changes to the system;

e. Retain records of configuration-controlled changes to the system for at least two change cycles of baseline configurations as defined in CM-02(03), and as feasible for the life of the system;

f. Monitor and review activities associated with configuration-controlled changes to the system; and

g. Coordinate and provide oversight for configuration change control activities through the Change Advisory Board (CAB) that convenes per agency change control procedures and when there is a significant change to systems or environments.

Implementation Standards

Std.01 — All changes must be auditable and audited.

Std.02 — All security-related information resources changes shall be approved by the information owner through a change control process. [Source: DIR Control Standards Catalog CM-3]

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.04 PCI — Changes to all system components in the production environment are made according to established procedures that include:

a. Reason for, and description of, the change.

b. For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production.

[Source: PCI DSS 6.5.1]

Std.05 PCI — All changes to network connections and to configurations of Network Security Controls (NSCs) are approved and managed in accordance with the change control process defined at Requirement 6.5.1. [Source: PCI DSS 1.2.2]

CJIS Correspondence

For systems processing CJIS data, CM-03e is superseded by CJIS requirement CM-03e:

Std.06 CJIS — Retain records of configuration-controlled changes to the system for two (2) years. [Source: CJIS CM-03]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.03 FedRAMP — The service provider establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page) in accordance with record retention policies and procedures. The means of communication are approved and accepted by the Joint Authorization Board (JAB)/Authorizing Official (AO). [Source: FedRAMP Security Controls Baseline CM-3]

Discussion

Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of system changes, including system upgrades and modifications. Configuration change control includes changes to baseline configurations, configuration items of systems, operational procedures, configuration settings for system components, remediate vulnerabilities, and unscheduled or unauthorized changes. Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes. For changes that impact privacy

risk, the senior agency official for privacy updates privacy impact assessments and system of records notices. For new systems or major upgrades, organizations consider including representatives from the development organizations on the Configuration Control Boards or Change Advisory Boards. Auditing of changes includes activities before and after changes are made to systems and the auditing activities required to implement such changes. See also SA-10.

TxDOT Discussion

The configuration change control process for the information system, system components, or changes to the configuration settings for information technology products (including, but not limited to, operating systems, applications, firewalls, and routers) should include a systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications.

Normal and emergency changes, including changes resulting from the remediation of flaws, should be included in the configuration change control process. All changes should be tested, validated, and documented before implementation on operational systems.

Testing should not interfere with normal operations. An operational system may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If an information system must be taken off-line for testing, the tests should be scheduled to occur during planned system outages whenever possible. In situations where the operational system cannot be tested without disrupting mission-critical functions, employ compensating controls (for example, providing a replicated system to conduct testing) in accordance with the general tailoring guidance.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-124, 800-128; NIST IR 8062; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CA-07, CM-02, CM-04, CM-05, CM-06, CM-09, CM-11, IA-03, MA-02, PE-16, RA-08, SA-08, SA-10, SC-28, SI-02, SI-03, SI-04, SI-07, SI-10, SR-11

CM-03(01) Automated Documentation, Notification, and Prohibition of Changes

Baselines

N/A

Overlays

FedRAMP High

Requirements

Use automated mechanisms as defined in the Information Security Plan to:

a. Document proposed changes to the system;

b. Notify the Change Approval Board (CAB) of proposed changes to the system and request change approval;

c. Highlight proposed changes to the system that have not been approved or disapproved within organization agreed-upon time period;

d. Prohibit changes to the system until designated approvals are received;

e. Document all changes to the system; and

f. Notify organization-defined configuration management approval authorities when approved changes to the system are completed.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

None.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

CM-03(02) Testing, Validation, and Documentation of Changes

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Test, validate, and document changes to the system before finalizing the implementation of the changes.

Implementation Standards

Std.01 — Changes to all system components in the production environment are made according to established procedures that include testing to verify

that the change does not adversely impact system security. [Source: PCI DSS 6.5.1]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 6.5.1.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CM-03(02).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Changes to systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-06. Organizations ensure that testing does not interfere with system operations that support organizational mission and business functions. Individuals or groups conducting tests understand security and privacy policies and procedures, system security and privacy policies and procedures, and the health, safety, and environmental risks associated with specific facilities or processes. Operational systems may need to be taken offline, or replicated to the extent feasible, before testing can be conducted. If systems must be taken offline for testing, the tests are scheduled to occur during planned system outages whenever possible. If the testing cannot be conducted on operational systems, organizations employ compensating controls.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-124, 800-128; NIST IR 8062; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

CM-03(04) Security and Privacy Representatives

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Require information security and privacy representatives as designated by the CISO to be members of the configuration change control element defined in CM-03g.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CM-03(04).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Information security and privacy representatives include system security officers, senior agency information security officers, senior agency officials

for privacy, or system privacy officers. Representation by personnel with information security and privacy expertise is important because changes to system configurations can have unintended side effects, some of which may be security- or privacy-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security and privacy posture of systems. The configuration change control element referred to in the second organization-defined parameter reflects the change control elements defined by organizations in CM-03g.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-124, 800-128; NIST IR 8062; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

CM-03(06) Cryptography Management

Baselines

N/A

Overlays

FedRAMP High

Requirements

Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: all security safeguards that rely on cryptography.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

The controls referenced in the control enhancement refer to security and privacy controls from the control catalog. Regardless of the cryptographic mechanisms employed, processes and procedures are in place to manage those mechanisms. For example, if system components use certificates for identification and authentication, a process is implemented to address the expiration of those certificates.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

SC-12

CM-04 Impact Analyses

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

Implementation Standards

Std.01 — CM-04 Std.01 moved to CM-03 Std.02 in V2.4.

Std.02 — Rescinded in V2.4.

Std.03 — Ensure that impact analyses address control system safety and security interdependencies. [Source: Catalog of Control Systems Security: Recommendations for Standards Developers]

Std.04 — If a proposed change has a significant effect on the security of the system, initiate re-authorization activities. Follow guidance in SP 800-37.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CM-04.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Organizational personnel with security or privacy responsibilities conduct impact analyses. Individuals conducting impact analyses possess the necessary skills and technical expertise to analyze the changes to systems as well as the security or privacy ramifications. Impact analyses include reviewing security and privacy plans, policies, and procedures to understand control requirements; reviewing system design documentation and operational procedures to understand control implementation and how specific system changes might affect the controls; reviewing the impact of changes on organizational supply chain partners with stakeholders; and determining how potential changes to a system create new risks to the privacy of individuals and the ability of implemented controls to mitigate those risks. Impact analyses also include risk assessments to understand the impact of the changes and determine if additional controls are required.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-128; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CA-07, CM-03, CM-08, CM-09, MA-02, RA-03, RA-05, RA-08, SA-05, SA-08, SA-10, SI-02

CM-04(01) Separate Test Environments

Baselines

Moderate, High

Overlays

PCI DSS; FedRAMP High

Requirements

Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.

Implementation Standards

Std.01 — For any system categorized as moderate or high, test environments must be kept either physically or logically separate from production environments. Copies of production data must not be used for testing unless the data has been authorized for public release.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.01 PCI — Pre-production environments are separated from production environments and the separation is enforced with access controls. [Source: PCI DSS 6.5.3]

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

A separate test environment requires an environment that is physically or logically separate and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment and that information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not implemented, organizations determine the strength of mechanism required when implementing logical separation.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-128; PCI DSS; FedRAMP Security Controls Baseline

Related Controls

SA-11, SC-07

CM-04(02) Verification of Controls

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

Implementation Standards

None.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.01 PCI — Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable. [Source: PCI DSS 6.5.2]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CM-04(02).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Implementation in this context refers to installing changed code in the operational system that may have an impact on security or privacy controls.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-128; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

SA-11, SC-03, SI-06

CM-05 Access Restrictions for Change

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

Implementation Standards

Std.01 — Limit personnel authorized to make changes to the infrastructure based on their job responsibilities, and approve individuals prior to granting access.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CM-05.

Std.02 CJIS — Rescinded in V4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Changes to the hardware, software, or firmware components of systems or the operational procedures related to the system can potentially have significant effects on the security of the systems or individuals' privacy. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes. Access restrictions include physical and logical access controls (see AC-03 and PE-03), software libraries, workflow automation, media libraries, abstract layers (i.e., changes implemented into external interfaces rather than directly into systems), and change windows (i.e., changes occur only during specified times).

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 186; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-03, AC-05, AC-06, CM-09, PE-03, SC-28, SI-02, SI-10

CM-05(01) Automated Access Enforcement and Audit Records

Baselines

High

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

a. Enforce access restrictions using automated mechanisms as identified in applicable System Security Plans (SSPs); and

b. Automatically generate audit records of the enforcement actions.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organizations log system accesses associated with applying configuration changes to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FIPS 140, 186; FedRAMP Security Controls Baseline

Related Controls

AU-02, AU-06, AU-07, AU-12, CM-06, CM-11, SI-12

CM-05(05) Privilege Limitation for Production and Operation

Baselines

N/A

Overlays

TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Limit privileges to change system components and system-related information within a production or operational environment; and

b. Review and reevaluate privileges at least quarterly.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

In many organizations, systems support multiple mission and business functions. Limiting privileges to change system components with respect to operational systems is necessary because changes to a system component may have far-reaching effects on mission and business processes supported by the system. The relationships between systems and mission/business processes are, in some cases, unknown to developers. System-related information includes operational procedures.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

TX-RAMP Program Manual

Federal References

FIPS 140, 186; FedRAMP Security Controls Baseline

Related Controls

AC-02

CM-06 Configuration Settings

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using approved common secure configurations derived from sources defined in Stds.02 & 03;

b. Implement the configuration settings;

c. Identify, document, and approve any deviations from established configuration settings for all configurable system components based on explicit operational requirements; and

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — All configuration baselines implemented in a production environment must be coordinated with and approved by TxDOT Information Security.

Std.03 — To resolve configuration conflicts among multiple security guidelines, follow the latest (current) guidance from the highest applicable source in the TxDOT hierarchy as follows:

a. TxDOT Information Security Configuration Baselines

b. The Center for Internet Security (CIS);

c. NIST National Checklist Program (NCP) Repository;

d. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG);

e. National Security Agency (NSA) STIGs; or

f. Vendor Configuration Baselines.

Std.04 — All configuration baselines used must be documented in the System Security Plan (SSP).

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.05 PCI — Configuration standards for Network Security Control (NSC) rulesets are:

a. Defined.

b. Implemented.

c. Maintained.

[Source: PCI DSS 1.2.1]

Std.06 PCI — Configuration standards are developed, implemented, and maintained to:

a. Cover all system components.

b. Address all known security vulnerabilities.

c. Be consistent with industry-accepted system hardening standards or vendor hardening recommendations.

d. Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1.

e. Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.

[Source: PCI DSS 2.2.1]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CM-06.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low baseline, the following standards apply:

Std.07 FedRAMP — The service provider shall use the DoD STIGs or Center for Internet Security guidelines to establish configuration settings. [Source: FedRAMP Security Controls Baseline CM-6]

Std.08 FedRAMP — The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available). [Source: FedRAMP Security Controls Baseline CM-6]

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standards apply:

Std.09 FedRAMP — The service provider shall use the DoD STIGs to establish configuration settings; Center for Internet Security up to Level 2 (CIS Level 2) guidelines shall be used if STIGs are not available; Custom baselines shall be used if CIS is not available. [Source: FedRAMP Security Controls Baseline CM-6]

Std.10 FedRAMP — The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available). [Source: FedRAMP Security Controls Baseline CM-6]

Discussion

Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system. Information technology products for which configuration settings can be defined include mainframe computers, servers, workstations, operating systems, mobile devices, input/output devices, protocols, and applications. Parameters that impact the security posture of systems include registry settings; account, file, or directory permission settings; and settings for functions, protocols, ports, services, and remote connections. Privacy parameters are parameters impacting the privacy posture of systems, including the parameters required to satisfy other privacy controls. Privacy parameters include settings for access controls, data processing preferences, and processing and retention

permissions. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the configuration baseline for the system.

Common secure configurations (also known as security configuration checklists, lockdown and hardening guides, and security reference guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for information technology products and platforms as well as instructions for configuring those products or platforms to meet operational requirements. Common secure configurations can be developed by a variety of organizations, including information technology product developers, manufacturers, vendors, federal agencies, consortia, academia, industry, and other organizations in the public and private sectors.

Implementation of a common secure configuration may be mandated at the organization level, mission and business process level, system level, or at a higher level, including by a regulatory agency. Common secure configurations include the United States Government Configuration Baseline and security technical implementation guides (STIGs), which affect the implementation of CM-06 and other controls such as AC-19 and CM-07. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol provide an effective method to uniquely identify, track, and control configuration settings.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

Compliance checks are used to evaluate configuration settings and provide general insight into the overall effectiveness of configuration management activities. Cloud Service Providers (CSPs) and Third Party Assessment Organizations (3PAOs) typically combine compliance check findings into a single CM-6 finding, which is acceptable. However, for initial assessments, annual assessments, and significant change requests, FedRAMP requires a clear understanding, on a per-control basis, where risks exist. Therefore, 3PAOs must also analyze compliance check findings as part of the controls assessment. Where a direct mapping exists, the 3PAO must document additional findings per control in the corresponding SAR Risk Exposure Table (RET), which are then documented in the CSP's Plan of Action and Milestones (POA&M). This will likely result in the details of individual control findings overlapping with those in the combined CM-6 finding, which is acceptable.

During monthly continuous monitoring, new findings from CSP compliance checks may be combined into a single CM-6 POA&M item. CSPs are not required to map the findings to specific controls because controls are only assessed during initial assessments, annual assessments, and significant change requests.

[Source: FedRAMP Security Controls Baseline CM-6]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-70, 800-126, 800-128; USGCB; NCPR; DOD STIG; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-03, AC-19, AU-02, AU-06, CA-03, CA-09, CM-02, CM-03, CM-05, CM-07, CM-11, CP-07, CP-09, CP-10, IA-03, IA-05, PL-08, PL-09, RA-05, SA-04, SA-05, SA-08, SA-09, SC-18, SC-28, SI-02, SI-04, SI-06

CM-06(01) Automated Management, Application, and Verification

Baselines

High

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

Manage, apply, and verify configuration settings for all configurable system components using automated mechanisms as identified in applicable System Security Plans (SSPs).

Implementation Standards

Std.01 — Information system automated central management systems must be verified to meet system mission and user requirements.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Automated tools (e.g., hardening tools, baseline configuration tools) can improve the accuracy, consistency, and availability of configuration settings information. Automation can also provide data aggregation and data correlation capabilities, alerting mechanisms, and dashboards to support risk-based decision-making within the organization.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-70, 800-126, 800-128; USGCB; NCPR; DOD STIG; FedRAMP Security Controls Baseline

Related Controls

CA-07

CM-06(02) Respond to Unauthorized Changes

Baselines

High

Overlays

PCI DSS; FedRAMP High

Requirements

Take the following actions in response to unauthorized changes to configuration settings for all data, systems, and components: actions defined in Std.01.

Implementation Standards

Std.01 — Where feasible, employ automated mechanisms to respond to unauthorized changes. Where automation is not feasible, employ manual monitoring and incorporate response into the incident response capability to ensure that events are tracked, monitored, corrected, and auditable. Whether automated or manual, responses must include:

a. Alerting responsible actors (personnel or roles, partners, other organizations);

b. Restoring to approved configuration if possible or halting system processing as warranted; and

c. Investigation or escalation as required.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.02 PCI — The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to:

a. Intrusion-detection and intrusion-prevention systems.

b. Change-detection mechanisms for critical files.

c. Detection of unauthorized wireless access points.

[Source: PCI DSS 12.10.5]

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Responses to unauthorized changes to configuration settings include alerting designated organizational personnel, restoring established configuration settings, or—in extreme cases—halting affected system processing.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-70, 800-126, 800-128; USGCB; NCPR; DOD STIG; PCI DSS; FedRAMP Security Controls Baseline

Related Controls

IR-04, IR-06, SI-07

CM-07 Least Functionality

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Configure the system to provide only mission-essential capabilities as identified in contingency plans and the System Security Plan (SSP); and

b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: all functions, ports, protocols, and/or services except those authorized and listed in the SSP.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Actively monitor permitted ports, protocols, and services in accordance with the Continuous Monitoring Program (see CA-07).

Std.03 — Provide timely responses, as defined by the CISO, to informational requests for organizational configuration status and posture information.

Std.08 — All services, protocols, and ports allowed are identified, approved, and have a defined business need. [Source: PCI DSS 1.2.5]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 1.2.5 and 2.2.2.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.04 PCI — Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated. [Source: PCI DSS 1.2.6]

Std.05 PCI — System security parameters are configured to prevent misuse. [Source: PCI DSS 2.2.6]

Std.06 PCI — Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled. [Source: PCI DSS 2.2.4]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CM-07.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.07 FedRAMP — The service provider shall use Security guidelines (See CM-6) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if STIGs or CIS is not available. [Source: FedRAMP Security Controls Baseline CM-7]

Discussion

Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default may not be necessary to support essential organizational missions, functions, or operations. Additionally, it is sometimes convenient to provide multiple services from a single system component, but doing so increases risk over limiting the services provided by that single component. Where feasible, organizations limit component functionality to a single function per component. Organizations consider removing unused or unnecessary software and disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunneling. Organizations employ network scanning tools, intrusion detection and prevention systems, and end-point protection technologies, such as firewalls and host-based intrusion detection systems, to identify and prevent the use of prohibited functions, protocols, ports, and services. Least functionality can also be achieved as part of the fundamental design and development of the system (see SA-08, SC-02, and SC-03).

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 180, 186, 202; NIST SP 800-167; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-03, AC-04, CA-07, CM-02, CM-05, CM-06, CM-11, RA-05, SA-04, SA-05, SA-08, SA-09, SA-15, SC-02, SC-03, SC-07, SI-04

CM-07(01) Periodic Review

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Review the system annually or as system changes or incidents occur to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and

b. Disable or remove all functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.

Implementation Standards

None.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, CM-07(01)b. is superseded by PCI DSS requirement 2.2.5:

Std.01 PCI — If any insecure services, protocols, or daemons are present:

a. Business justification is documented.

b. Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.

[Source: PCI DSS 2.2.5]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Review the system annually as incidents occur to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services. [Source: CJIS CM-07(01)]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 requirements.

For systems subject to TX-RAMP Level 2, the following standard applies:

Std.02 TX-RAMP — Review the system [at least quarterly] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services. [Source: TX-RAMP Manual CM-7(1)]

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organizations review functions, ports, protocols, and services provided by systems or system components to determine the functions and services that are candidates for elimination. Such reviews are especially important during transition periods from older technologies to newer technologies (e.g., transition from IPv4 to IPv6). These technology transitions may require implementing the older and newer technologies simultaneously during the transition period and returning to minimum essential functions, ports, protocols, and services at the earliest opportunity. Organizations can either decide the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Unsecure protocols include Bluetooth, FTP, and peer-to-peer networking.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 180, 186, 202; NIST SP 800-167; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-18

CM-07(02) Prevent Program Execution

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions and rules authorizing the terms and conditions of software program usage.

Implementation Standards

Std.01 — Employ automated mechanisms to prevent program execution in accordance with defined lists of authorized programs (whitelists), defined lists of unauthorized programs (blacklists), access control policies, and CM-10.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CM-07(02).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Prevention of program execution addresses organizational policies, rules of behavior, and/or access agreements that restrict software usage and the terms and conditions imposed by the developer or manufacturer, including software licensing and copyrights. Restrictions include prohibiting auto-execute features, restricting roles allowed to approve program execution, permitting or prohibiting specific software programs, or restricting the number of program instances executed at the same time.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

This control refers to software deployment by Cloud Service Provider (CSP) personnel into the production environment. The control requires a policy that states conditions for deploying software. This control shall be implemented in a technical manner on the information system to only allow programs to run that adhere to the policy (i.e. allow-listing). This control is not to be based off of strictly written policy on what is allowed or not allowed to run. [Source: FedRAMP Security Controls Baseline CM-7(2)]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 180, 186, 202; NIST SP 800-167; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CM-03, CM-08, PL-04, PL-09, PM-05, PS-06

CM-07(04) Unauthorized Software — Deny-by-Exception

Baselines

Moderate, High

Overlays

N/A

Requirements

a. Identify software programs not authorized to execute on the system as identified in the System Security Plan (SSP);

b. Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; and

c. Review and update the list of unauthorized software programs at least annually and when new threats are identified.

Implementation Standards

Std.01 — Configure systems to prevent installation or execution of unapproved, unauthorized, or unmanaged software; and to send alerts when such software is detected.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Unauthorized software programs can be limited to specific versions or from a specific source. The concept of prohibiting the execution of unauthorized

software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses.

TxDOT Discussion

CM-07(05) may be used in place of CM-07(04).

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FIPS 140, 180, 186, 202; NIST SP 800-167

Related Controls

CM-06, CM-08, CM-10, PL-09, PM-05

CM-07(05) Authorized Software — Allow-by-Exception

Baselines

N/A

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Identify software programs authorized to execute on the system as identified in the baseline configuration;

b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and

c. Review and update the list of authorized software programs annually.

Implementation Standards

Std.01 — Wherever applicable, employ application whitelisting technologies to permit the execution of explicitly allowed (whitelisted) software and block

execution of everything else on systems and business networks; in particular, business servers such as mail servers and domain controllers.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirements CM-07(05) and 5.20.4.2.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.02 FedRAMP — Review and update the list of authorized software programs at least quarterly or when there is a change. [Source: FedRAMP Security Controls Baseline CM-7(5)]

Discussion

Authorized software programs can be limited to specific versions or from a specific source. To facilitate a comprehensive authorized software process and increase the strength of protection for attacks that bypass application level authorized software, software programs may be decomposed into and monitored at different levels of detail. These levels include applications, application programming interfaces, application modules, scripts, system processes, system services, kernel functions, registries, drivers, and dynamic link libraries. The concept of permitting the execution of authorized software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses. Organizations consider verifying the integrity of authorized software programs using digital signatures, cryptographic checksums, or hash functions. Verification of authorized software can occur either prior to execution or at system startup. The identification of authorized URLs for websites is addressed in CA-03(05) and SC-07.

TxDOT Discussion

CM-07(05) may be used in place of CM-07(04).

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 180, 186, 202; NIST SP 800-167; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

CM-02, CM-03, CM-06, CM-08, CM-10, PL-09, PM-05, SA-10, SI-07

CM-08 System Component Inventory

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop and document an inventory of system components that:

1. Accurately reflects the system;

2. Includes all components within the system;

3. Does not include duplicate accounting of components or components assigned to any other system;

4. Is at the level of granularity deemed necessary for tracking and reporting; and

5. Includes the following information to achieve system component accountability: information as defined in Std.03 below; and

b. Review and update the system component inventory at least annually in accordance with PM-05, and whenever a change is made to the inventory.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. [Source: SP 800-171 3.4.1]

Std.03 — The inventory of information system components must include any information determined to be necessary by the organization to achieve effective property accountability including, but not limited to:

a. Manufacturer;

b. Type;

c. Model;

d. Serial number;

e. Physical location;

f. Software license information;

g. Information system/component owner;

h. Associated component configuration standard;

i. Software/firmware version information; and

j. Networked component/device machine name or network address.

Std.04 — The component inventory must be consistent with the authorization boundary of the system, and is subject to annual review. All components within the authorization boundary of the system must be verified either as part of the system or recognized by another system as a component within that system.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.05 PCI — An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current. [Source: PCI DSS 12.5.1]

Std.06 PCI — An inventory of authorized wireless access points is maintained, including a documented business justification. [Source: PCI DSS 11.2.2]

Std.11 PCI — An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management. [Source: PCI DSS 6.3.2]

Std.12 PCI — An up-to-date list of Point of Interaction (POI) devices is maintained, including:

a. Make and model of the device.

b. Location of device.

c. Device serial number or other methods of unique identification.

[Source: PCI DSS 9.5.1.1]

Std.13 PCI — Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following:

a. Analysis that the technologies continue to receive security fixes from vendors promptly.

b. Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance.

c. Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology.

d. Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans.

[Source: PCI DSS 12.3.4]

Std.14 PCI — PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes:

a. Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and

acceptance channels (for example, card-present, card-not-present, and e-commerce).

b. Updating all data-flow diagrams per Requirement 1.2.4.

c. Identifying all locations where account data is stored, processed, and transmitted, including but not limited to:

1. Any locations outside of the currently defined Cardholder Data Environment (CDE);

2. Applications that process Cardholder Data (CHD);

3. Transmissions between systems and networks; and

4. File backups.

d. Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE.

e. Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope.

f. Identifying all connections from third-party entities with access to the CDE.

g. Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.

[Source: PCI DSS 12.5.2]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CM-08.

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.07 CJIS — For all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI, maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices. [Source: CJIS 5.20.1.1]

TX-RAMP Correspondence

For systems subject to TX-RAMP Level 1 or Level 2 requirements, the following standard applies:

Std.08 TX-RAMP — Review and update the system component inventory at least quarterly. [Source: TX-RAMP Manual CM-8]

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standards apply:

Std.09 FedRAMP — Review and update the system component inventory at least monthly. [Source: FedRAMP Security Controls Baseline CM-8]

Std.10 FedRAMP — The system component inventory must be provided monthly or when there is a change. [Source: FedRAMP Security Controls Baseline CM-8]

Discussion

System components are discrete, identifiable information technology assets that include hardware, software, and firmware. Organizations may choose to implement centralized system component inventories that include components from all organizational systems. In such situations, organizations ensure that the inventories include system-specific information required for component accountability. The information necessary for effective accountability of system components includes the system name, software owners, software version numbers, hardware inventory specifications, software license information, and for networked components, the machine names and network addresses across all implemented protocols (e.g., IPv4, IPv6). Inventory specifications include date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location.

Preventing duplicate accounting of system components addresses the lack of accountability that occurs when component ownership and system association is not known, especially in large or complex connected systems. Effective prevention of duplicate accounting of system components necessitates use of a unique identifier for each component. For software inventory, centrally managed software that is accessed via other systems is addressed as a component of the system on which it is installed and managed. Software installed on multiple organizational systems and managed at the system level is addressed for each individual system and may appear more than once in a centralized component inventory,

necessitating a system association for each software instance in the centralized inventory to avoid duplicate accounting of components. Scanning systems implementing multiple network protocols (e.g., IPv4 and IPv6) can result in duplicate components being identified in different address spaces. The implementation of CM-08(07) can help to eliminate duplicate accounting of components.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-57-1, 800-57-2, 800-57-3, 800-128; NIST IR 8011-2, 8011-3; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

CM-02, CM-07, CM-09, CM-10, CM-11, CP-02, CP-09, MA-02, MA-06, PL-09, PM-05, PM-16, SA-04, SA-05, SI-02, SR-04

CM-08(01) Updates During Installation and Removal

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Update the inventory of system components as part of component installations, removals, and system updates.

Implementation Standards

Std.01 — When installing, updating, or removing an information system, information system component, or network component, the enterprise needs to update the inventory to ensure traceability for tracking critical components. In addition, the information system's configuration needs to be updated to ensure an accurate inventory of supply chain protections and then re-baselined accordingly. [Source: SP 800-161]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CM-08(01).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate or High baselines.

Discussion

Organizations can improve the accuracy, completeness, and consistency of system component inventories if the inventories are updated as part of component installations or removals or during general system updates. If inventories are not updated at these key times, there is a greater likelihood that the information will not be appropriately captured and documented. System updates include hardware, software, and firmware components.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-57-1, 800-57-2, 800-57-3, 800-128; NIST IR 8011-2, 8011-3; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

PM-16

CM-08(02) Automated Maintenance

Baselines

High

Overlays

FedRAMP High

Requirements

Maintain the currency, completeness, accuracy, and availability of the inventory of system components using automated mechanisms as identified in applicable System Security Plans (SSPs).

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Organizations maintain system inventories to the extent feasible. For example, virtual machines can be difficult to monitor because such machines

are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and accurate an inventory as is deemed reasonable. Automated maintenance can be achieved by the implementation of CM-02(02) for organizations that combine system component inventory and baseline configuration activities.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; NIST SP 800-57-1, 800-57-2, 800-57-3, 800-128; NIST IR 8011-2, 8011-3; FedRAMP Security Controls Baseline

Related Controls

None.

CM-08(03) Automated Unauthorized Component Detection

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

a. Detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms as identified in the System Security Plan (SSP) continuously; and

b. Take the following actions when unauthorized components are detected: disable network access by such components; isolate the components; and notify personnel as identified in the incident response plan.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CM-08(03).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.01 FedRAMP — Detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms with a maximum five-minute delay in detection continuously. [Source: FedRAMP Security Controls Baseline CM-8(3)]

Discussion

Automated unauthorized component detection is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms may also be used to prevent the connection of unauthorized components (see CM-07(09)). Automated mechanisms can be implemented in systems or in separate system components. When acquiring and implementing automated mechanisms, organizations consider whether such mechanisms depend on the ability of the system component to support an agent or supplicant in order to be detected since some types of components do not have or cannot support agents (e.g., IoT devices, sensors). Isolation can be achieved, for example, by placing unauthorized system components in separate domains or subnets or quarantining such components. This type of component isolation is commonly referred to as "sandboxing."

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; NIST SP 800-57-1, 800-57-2, 800-57-3, 800-128; NIST IR 8011-2, 8011-3; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-19, CA-07, RA-05, SC-03, SC-39, SI-03, SI-04, SI-07

CM-08(04) Accountability Information

Baselines

High

Overlays

FedRAMP High

Requirements

Include in the system component inventory information, a means for identifying by position or role at a minimum, individuals responsible and accountable for administering those components.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Identifying individuals who are responsible and accountable for administering system components ensures that the assigned components are properly administered and that organizations can contact those individuals if some action is required (e.g., when the component is determined to be the source of a breach, needs to be recalled or replaced, or needs to be relocated).

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; NIST SP 800-57-1, 800-57-2, 800-57-3, 800-128; NIST IR 8011-2, 8011-3; FedRAMP Security Controls Baseline

Related Controls

AC-03

CM-09 Configuration Management Plan

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Develop, document, and implement a configuration management plan for the system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

c. Defines the configuration items for the system and places the configuration items under configuration management;

d. Is reviewed and approved by personnel as identified in the System Security Plan (SSP); and

e. Protects the configuration management plan from unauthorized disclosure and modification.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CM-09.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Configuration management activities occur throughout the system development life cycle. As such, there are developmental configuration management activities (e.g., the control of code and software libraries) and operational configuration management activities (e.g., control of installed components and how the components are configured). Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual systems. Configuration management plans define processes and procedures for how configuration management is used to support system development life cycle activities.

Configuration management plans are generated during the development and acquisition stage of the system development life cycle. The plans describe how to advance changes through change management processes; update configuration settings and baselines; maintain component inventories; control development, test, and operational environments; and develop, release, and update key documents.

Organizations can employ templates to help ensure the consistent and timely development and implementation of configuration management plans. Templates can represent a configuration management plan for the organization with subsets of the plan implemented on a system by system basis. Configuration management approval processes include the designation of key stakeholders responsible for reviewing and approving proposed changes to systems, and personnel who conduct security and privacy impact analyses prior to the implementation of changes to the systems. Configuration items are the system components, such as the hardware, software, firmware, and documentation to be configuration-managed. As systems continue through the system development life cycle, new configuration items may be identified, and some existing configuration items may no longer need to be under configuration control.

TxDOT Discussion

Configuration management plans may be part of System Security Plans or maintained as separate documents. No system may be authorized for operation without a configuration management plan.

Responsibility for developing the configuration management process should not be assigned to personnel that are directly involved in information system development.

Note for systems subject to FedRAMP Requirements:

FedRAMP does not provide a template for the Configuration Management Plan. However, NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, provides guidelines for the implementation of CM controls as well as a sample CMP outline in Appendix D of the Guide. [Source: FedRAMP Security Controls Baseline CM-9]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-128; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

CM-02, CM-03, CM-04, CM-05, CM-08, PL-02, RA-08, SA-10, SI-12

CM-10 Software Usage Restrictions

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Use software and associated documentation in accordance with contract agreements and copyright laws;

b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Implementation Standards

Std.01 — Acquire software only through known and reputable sources; maintain evidence of ownership of licenses and material; and carry out annual checks that only authorized software and licensed products are installed. [Source: Hitrust 06.b Intellectual Property Rights]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CM-10.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Software license tracking can be accomplished by manual or automated methods, depending on organizational needs. Examples of contract agreements include software license agreements and non-disclosure agreements.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-17, AU-06, CM-07, CM-08, PM-30, SC-07

CM-11 User-Installed Software

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Establish configuration management and acceptable use policies governing the installation of software by users;

b. Enforce software installation policies through the following methods: organization-defined methods including system configuration settings and manual oversight; and

c. Monitor policy compliance at frequencies as specified in the Continuous Monitoring Program.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Monitoring for user-installed software must be in compliance with information security continuous monitoring (ISCM) requirements.

Std.03 — Ensure that unauthorized software is either removed from use on enterprise managed devices or receives a documented exception. [Source: CIS 2.3]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CM-11.

TX-RAMP Correspondence

For systems subject to TX-RAMP Level 1 or Level 2 requirements, the following standard applies:

Std.04 TX-RAMP — Monitor policy compliance at least monthly. [Source: TX-RAMP Manual CM-11]

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

If provided the necessary privileges, users can install software in organizational systems. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software

installation. Permitted software installations include updates and security patches to existing software and downloading new applications from organization-approved "app stores." Prohibited software installations include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. Policies selected for governing user-installed software are organization-developed or provided by some external entity. Policy enforcement methods can include procedural methods and automated methods.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-03, AU-06, CM-02, CM-03, CM-05, CM-06, CM-07, CM-08, PL-04, SI-04, SI-07

CM-12 Information Location

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Identify and document the location of all TxDOT information not classified as Public and the specific system components on which the information is processed and stored;

b. Identify and document the users who have access to the system and system components where the information is processed and stored; and

c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.02 CJIS — Identify and document the location of CJI and the specific system components on which the information is processed, stored, or transmitted. [Source: CJIS CM-12]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baseline, the following standard applies:

Std.01 FedRAMP — Cloud Service Providers (CSPs) must account for and include within an authorization boundary all federal data populated or generated by a federal customer within the Cloud Service Offering (CSO), including metadata. [Source: FedRAMP Authorization Boundary Guidance]

Discussion

Information location addresses the need to understand where information is being processed and stored. Information location includes identifying where specific information types and information reside in system components and how information is being processed so that information flow can be understood and adequate protection and policy management provided for such information and system components. The security category of the information is also a factor in determining the controls necessary to protect the information and the system component where the information resides (see FIPS 199). The location of the information and system components is also a factor in the architecture and design of the system (see SA-04, SA-08, SA-17).

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

TX-RAMP Program Manual

Federal References

FIPS 199; NIST SP 800-60-1, 800-60-2; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-02, AC-03, AC-04, AC-06, CM-08, PM-05, RA-02, SA-04, SA-08, SA-17, SC-04, SC-28, SI-04, SI-07

CM-12(01) Automated Tools to Support Information Location

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Use automated tools to identify all TxDOT information not classified as Public by information type on all system components under configuration management to ensure controls are in place to protect organizational information and individual privacy.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.02 CJIS — Use automated tools to identify CJI on software and hardware system components to ensure controls are in place to protect organizational information and individual privacy. [Source: CJIS CM-12(01)]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baseline, the following standard applies:

Std.01 FedRAMP — Use automated tools to identify Federal data and system data that must be protected at the High or Moderate impact levels according to FedRAMP Authorization Boundary Guidance. [Source: FedRAMP Security Controls Baseline CM-12(1)]

Discussion

The use of automated tools helps to increase the effectiveness and efficiency of the information location capability implemented within the system. Automation also helps organizations manage the data produced during information location activities and share such information across the organization. The output of automated information location tools can be used to guide and inform system architecture and design decisions.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

FIPS 199; NIST SP 800-60-1, 800-60-2; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

CM-14 Signed Components

Baselines

High

Overlays

FedRAMP High

Requirements

Prevent the installation of all software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Software and firmware components prevented from installation unless signed with recognized and approved certificates include software and firmware version updates, patches, service packs, device drivers, and basic input/output system updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of

both. Digital signatures and organizational verification of such signatures is a method of code authentication.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

If digital signatures/certificates are unavailable, alternative cryptographic integrity checks (hashes, self-signed certs, etc.) can be utilized. [Source: FedRAMP Security Controls Baseline CM-14]

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

NIST IR 8062; FedRAMP Security Controls Baseline

Related Controls

CM-07, SC-12, SC-13, SI-07

CP — Contingency Planning

CP-01 Policy and Procedures

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level contingency planning policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;

b. Designate a senior management official as defined in the contingency planning policy to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and

c. Review and update the current contingency planning:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Review and update the current contingency planning policy and procedures following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. [Source: CJIS CP-01]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Contingency planning policy and procedures address the controls in the CP family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of contingency planning policy and procedures. Security and privacy program policies and procedures at the

organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to contingency planning policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-12, 800-30, 800-34, 800-39, 800-50, 800-100; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

PM-09, PS-08, SI-12

CP-02 Contingency Plan

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop a contingency plan for the system that:

1. Identifies essential mission and business functions and associated contingency requirements;

2. Provides recovery objectives, restoration priorities, and metrics;

3. Addresses contingency roles, responsibilities, assigned individuals with contact information;

4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;

5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;

6. Addresses the sharing of contingency information; and

7. Is reviewed and approved by key personnel or roles and entities identified in the contingency plan;

b. Distribute copies of the contingency plan to key contingency personnel (identified by name and/or by role) and organizational elements as identified in the contingency plan;

c. Coordinate contingency planning activities with incident handling activities;

d. Review the contingency plan for the system at least annually as part of the annual risk assessment (see CP-04);

e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicate contingency plan changes to key contingency personnel (identified by name and/or by role) and organizational elements as identified in the contingency plan;

g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and

h. Protect the contingency plan from unauthorized disclosure and modification.

Implementation Standards

Std.01 — The plan shall be distributed to key personnel and a copy stored offsite. Elements of the plan for information resources shall include:

a. Business Impact Analysis to systematically assess the potential impacts of a loss of business functionality due to an interruption of computing and/or infrastructure support services resulting from various events or incidents. The analysis shall identify the following elements:

1. Mission-Critical Information Resources (specific system resources required to perform critical functions) to include:

(a) Internal and external points of contact for personnel that provide or receive data or support interconnected systems.

(b) Supporting infrastructure such as electric power, telecommunications connections, and environmental controls.

2. Disruption impacts and allowable outage times to include:

(a) Effects of an outage over time to assess the maximum allowable time that a resource may be denied before it prevents or inhibits the performance of an essential function.

(b) Effects of an outage across related resources and dependent systems to assess cascading effects on associated systems or processes.

3. Recovery priorities that consider geographic areas, accessibility, security, environment, and cost and may include a combination of:

(a) Preventive controls and processes such as backup power, excess capacity, environmental sensors and alarms.

(b) Recovery techniques and technologies such as backup methodologies, alternate sites, software and hardware equipment replacement, implementation roles and responsibilities.

b. Risk Assessment to weigh the cost of implementing preventative measures against the risk of loss from not taking action.

c. Implementation, testing, and maintenance management program addressing the initial and ongoing testing and maintenance activities of the plan.

d. Disaster Recovery Plan — Each state organization shall maintain a written disaster recovery plan for major or catastrophic events that deny access to

information resources for an extended period. Information learned from tests conducted since the plan was last updated will be used in updating the disaster recovery plan. The disaster recovery plan will:

1. Contain measures which address the impact and magnitude of loss or harm that will result from an interruption;

2. Identify recovery resources and a source for each;

3. Contain step-by-step implementation instructions;

4. Include provisions for annual testing. [Source: DIR Control Standards Catalog CP-2]

Std.02 — Rescinded in V4.0.

Std.03 — Define and document within contingency plans:

a. Maximum Tolerable Downtime (MTD) — The MTD represents the total amount of time organizations are willing to accept for a mission/business process outage or disruption and includes all impact considerations;

b. Recovery Time Objective (RTO) — RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business functions, and the MTD; and

c. Recovery Point Objective (RPO) — The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data shall be recovered (given the most recent backup copy of the data) after an outage.

Std.04 — Copies of the business continuity plans are distributed to the Information System Security Officer, System Owner, Contingency Plan Coordinator, System Administrator, and Database Administrator (or the organization's functional equivalents). [Source: Hitrust 12.c Developing and Implementing Continuity Plans Including Information Security]

Std. 05 — State agencies shall maintain written Continuity of Operations Plans in compliance with Texas Labor Code Sec. 412.054 that address information resources so that the effects of a disaster will be minimized and the state agency will be able either to maintain or quickly resume mission-critical functions. [Source: DIR Control Standards Catalog CP-2]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CP-02.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.06 FedRAMP — For Joint Authorization Board (JAB) authorizations the contingency lists include designated FedRAMP personnel. [Source: FedRAMP Security Controls Baseline CP-2]

Std.07 FedRAMP — Cloud Service Providers (CSPs) must use the FedRAMP Information System Contingency Plan (ISCP) Template (available on the fedramp.gov: https://www.fedramp.gov/assets/resources/templates/SSP-A06-FedRAMP-ISCP-Template.docx). [Source: FedRAMP Security Controls Baseline CP-2]

Discussion

Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached. Contingency planning is considered throughout the system development life cycle and is a fundamental part of the system design. Systems can be designed for redundancy, to provide backup capabilities, and for resilience. Contingency plans reflect the degree of restoration required for organizational systems since not all systems need to fully recover to achieve the level of continuity of operations desired. System recovery objectives reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, organizational risk tolerance, and system impact level.

Actions addressed in contingency plans include orderly system degradation, system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By coordinating contingency planning with incident handling activities, organizations ensure that the necessary planning activities are in place and activated in the event of an incident. Organizations consider whether continuity of operations during an incident conflicts with the capability to

automatically disable the system, as specified in IR-04(05). Incident response planning is part of contingency planning for organizations and is addressed in the IR (Incident Response) family.

TxDOT Discussion

The planning process focuses on the required business objectives (e.g., restoring of specific communication services to customers in an acceptable amount of time). The procedures for obtaining necessary electronic covered information during an emergency are defined. The services and resources facilitating this are identified, including staffing, non-information processing resources, as well as fallback arrangements for information processing facilities. Such fallback arrangements may include arrangements with third parties in the form of reciprocal agreements, or commercial subscription services. The organization coordinates contingency planning activities with incident handling activities. [Source: Hitrust CSF 12.c Developing and Implementing Continuity Plans Including Information Security]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-34; NIST IR 8179; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CP-03, CP-04, CP-06, CP-07, CP-08, CP-09, CP-10, IR-04, IR-06, IR-08, MA-06, MP-02, MP-04, MP-05, PL-02, PM-08, PM-11, SA-15, SC-07, SC-23, SI-12

CP-02(01) Coordinate with Related Plans

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Coordinate contingency plan development with organizational elements responsible for related plans.

Implementation Standards

Std.01 — Ensure that results of tests are shared with personnel responsible for related plans. Agency-wide full-scale simulations and exercises include personnel responsible for all applicable plans.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CP-02(01).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Plans that are related to contingency plans include Business Continuity Plans, Disaster Recovery Plans, Critical Infrastructure Plans, Continuity of Operations Plans, Crisis Communications Plans, Insider Threat Implementation Plans, Data Breach Response Plans, Cyber Incident Response Plans, Breach Response Plans, and Occupant Emergency Plans.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-34; NIST IR 8179; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

SC-13

CP-02(02) Capacity Planning

Baselines

High

Overlays

FedRAMP High

Requirements

Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Capacity planning is needed because different threats can result in a reduction of the available processing, telecommunications, and support

services intended to support essential mission and business functions. Organizations anticipate degraded operations during contingency operations and factor the degradation into capacity planning. For capacity planning, environmental support refers to any environmental factor for which the organization determines that it needs to provide support in a contingency situation, even if in a degraded state. Such determinations are based on an organizational assessment of risk, system categorization (impact level), and organizational risk tolerance.

TxDOT Discussion

Identify the services and resources facilitating obtaining necessary electronic covered information during an emergency, including staffing, non-information processing resources, as well as fallback arrangements for information processing facilities. Such fallback arrangements may include arrangements with third parties in the form of reciprocal agreements, or commercial subscription services. [Source: Hitrust CSF 12.c Developing and Implementing Continuity Plans Including Information Security]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-34; NIST IR 8179; FedRAMP Security Controls Baseline

Related Controls

PE-11, PE-12, PE-13, PE-14, PE-18, SC-05

CP-02(03) Resume Mission and Business Functions

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Plan for the resumption of essential mission and business functions within the time period defined in the contingency plan of contingency plan activation.

Implementation Standards

Std.01 — Plans must address internal and external business dependencies. Fallback arrangements may include arrangements with third parties in the form of reciprocal agreements or commercial subscription services.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CP-02(03).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.02 FedRAMP — Plan for the resumption of all mission and business functions within time period defined in service provider and organization SLA of contingency plan activation. [Source: FedRAMP Security Controls Baseline CP-2(3)]

Discussion

Organizations may choose to conduct contingency planning activities to resume mission and business functions as part of business continuity planning or as part of business impact analyses. Organizations prioritize the resumption of mission and business functions. The time period for resuming mission and business functions may be dependent on the severity and extent of the disruptions to the system and its supporting infrastructure.

TxDOT Discussion

Plans for the resumption of essential missions and business functions, and for resumption of all missions and business functions, take into account the effects of the disruption on the environment of operation. Restoration and resumption plans should include prioritization of efforts.

Disruptions may affect the quality and quantity of resources in the environment, such as electric power, fuel, fresh water and wastewater, and the ability of these suppliers to also resume provision of essential mission and business functions. Contingency plans for widespread disruption may involve specialized organizations (e.g., FEMA, emergency services, regulatory authorities). [Source: SP 800-82]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-34; NIST IR 8179; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

CP-02(05) Continue Mission and Business Functions

Baselines

High

Overlays

FedRAMP High

Requirements

Plan for the continuance of essential mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Organizations may choose to conduct the contingency planning activities to continue mission and business functions as part of business continuity planning or business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-34; NIST IR 8179; FedRAMP Security Controls Baseline

Related Controls

None.

CP-02(08) Identify Critical Assets

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Identify critical system assets supporting essential mission and business functions.

Implementation Standards

Std.01 —

a. Criticality analysis is required for:

1. All moderate- and high-baseline systems in accordance with RA-09;

2. All systems supporting any essential mission or business function (see CP-02);

3. All systems identified in contingency plans.

b. Indicate whether assets are critical in System Security Plans (SSPs).

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CP-02(08).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organizations may choose to identify critical assets as part of criticality analysis, business continuity planning, or business impact analyses. Organizations identify critical system assets so that additional controls can be employed (beyond the controls routinely implemented) to help ensure that organizational mission and business functions can continue to be conducted during contingency operations. The identification of critical information assets also facilitates the prioritization of organizational resources. Critical system assets include technical and operational aspects. Technical aspects include system components, information technology services, information technology products, and mechanisms. Operational

aspects include procedures (i.e., manually executed operations) and personnel (i.e., individuals operating technical controls and/or executing manual procedures). Organizational program protection plans can assist in identifying critical assets. If critical assets are resident within or supported by external service providers, organizations consider implementing CP-02(07) as a control enhancement.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-34; NIST IR 8179; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CM-08, RA-09

CP-03 Contingency Training

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Provide contingency training to system users consistent with assigned roles and responsibilities:

1. Within 60 days of assuming a contingency role or responsibility;

2. When required by system changes; and

3. Annually thereafter; and

b. Review and update contingency training content annually and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — Rescinded in V2.2.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, CP-03 is superseded by CJIS requirement CP-03:

Std.04 CJIS —

a. Provide contingency training to system users consistent with assigned roles and responsibilities:

1. Within thirty (30) days of assuming a contingency role or responsibility;

2. When required by system changes; and

3. Annually thereafter; and

b. Review and update contingency training content annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or training simulations or exercises. [Source: CJIS CP-03]

TX-RAMP Correspondence

For systems subject to TX-RAMP Level 1 or Level 2 requirements, the following standard applies:

Std.02 TX-RAMP — Provide contingency training to system users consistent with assigned roles and responsibilities:

a. Within 14 days of assuming a contingency role or responsibility;

b. When required by system changes; and

c. Annually thereafter. [Source: TX-RAMP Manual CP-3]

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.03 FedRAMP —

a. Privileged admins and engineers must take the basic contingency training within 10 days.

b. Consideration must be given for those privileged admins and engineers with critical contingency-related roles, to gain enough system context and situational awareness to understand the full impact of contingency training as it applies to their respective level.

c. Newly hired critical contingency personnel must take this more in-depth training within 60 days of hire date when the training will have more impact.

[Source: FedRAMP Security Controls Baseline CP-3]

Discussion

Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, some individuals may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to establish systems at alternate processing and storage sites; and organizational officials may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles or responsibilities reflects the specific continuity requirements in the contingency plan. Events that may precipitate an update to contingency training content include, but are not limited to, contingency plan testing or an actual contingency (lessons learned), assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. At the discretion of the organization, participation in a contingency plan test or exercise, including lessons learned sessions subsequent to the test or exercise, may satisfy contingency plan training requirements.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-50; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AT-02, AT-03, AT-04, CP-02, CP-04, CP-08, IR-02, IR-04

CP-03(01) Simulated Events

Baselines

High

Overlays

FedRAMP High

Requirements

Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Document results of training and update contingency plans accordingly.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

The use of simulated events creates an environment for personnel to experience actual threat events, including cyber-attacks that disable websites, ransomware attacks that encrypt organizational data on servers, hurricanes that damage or destroy organizational facilities, or hardware or software failures.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-50; FedRAMP Security Controls Baseline

Related Controls

None.

CP-04 Contingency Plan Testing

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Test the contingency plan for the system at the frequency specified in the contingency plan, at least annually using the following tests to determine the

effectiveness of the plan and the readiness to execute the plan: agency-approved tests as identified in the contingency plan.

b. Review the contingency plan test results; and

c. Initiate corrective actions, if needed.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Contingency plans for all new systems must be tested prior to the system's being deployed to an operational state in the production environment.

Std.03 — Major deficiencies discovered as a result of testing must be addressed in accordance with CA-05.

Std.04 —

a. A formal test need not be conducted if the organization actively exercises its contingency plan capability during real contingencies.

b. Any response capability not exercised during real contingencies must be formally tested.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.07 CJIS — Test the contingency plan for the system annually using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), or comprehensive exercises. [Source: CJIS CP-04]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standards apply:

Std.05 FedRAMP — The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended); plans are approved by the Joint Authorization Board (JAB)/Authorizing Official (AO) prior to initiating testing. [Source: FedRAMP Security Controls Baseline CP-4]

Std.06 FedRAMP — The service provider must include the Contingency Plan test results with the security package within the Contingency Plan-designated appendix (Appendix G, Contingency Plan Test Report). [Source: FedRAMP Security Controls Baseline CP-4]

Discussion

Methods for testing contingency plans to determine the effectiveness of the plans and identify potential weaknesses include checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), and comprehensive exercises. Organizations conduct testing based on the requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.

TxDOT Discussion

Business continuity plan tests ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when a plan is invoked.

The test schedule for business continuity plan(s) indicates how and when each element of the plan is tested. These techniques are applied on a 'programmatic' basis such that the tests build upon one another, and in a way that is relevant to the specific response and recovery plan. The results of tests are recorded and actions taken to improve the plans, where necessary. Updates will also consider lessons learned from implementation of the business continuity plan(s). [Source: Hitrust 12.e Testing, Maintaining and Re-Assessing Business Continuity Plans]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 199; NIST SP 800-34, 800-84, 800-160-2; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AT-03, CA-05, CP-02, CP-03, CP-08, CP-09, IR-03, IR-04, PL-02, PM-14, SR-02

CP-04(01) Coordinate with Related Plans

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Coordinate contingency plan testing with organizational elements responsible for related plans.

Implementation Standards

Std.01 — Ensure that results of tests are shared with personnel responsible for related plans. Agency-wide full-scale simulations and exercises include personnel responsible for all applicable plans.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CP-04(01).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Plans related to contingency planning for organizational systems include Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. Coordination of contingency plan testing does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. However, it does require that if such organizational elements are responsible for related plans, organizations coordinate with those elements.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FIPS 199; NIST SP 800-34, 800-84, 800-160-2; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

IR-08, PM-08

CP-04(02) Alternate Processing Site

Baselines

High

Overlays

FedRAMP High

Requirements

Test the contingency plan at the alternate processing site:

a. To familiarize contingency personnel with the facility and available resources; and

b. To evaluate the capabilities of the alternate processing site to support contingency operations.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Conditions at the alternate processing site may be significantly different than the conditions at the primary site. Having the opportunity to visit the alternate site and experience the actual capabilities available at the site can provide valuable information on potential vulnerabilities that could affect essential organizational mission and business functions. The on-site visit can also provide an opportunity to refine the contingency plan to address the vulnerabilities discovered during testing.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FIPS 199; NIST SP 800-34, 800-84, 800-160-2; FedRAMP Security Controls Baseline

Related Controls

CP-07

CP-06 Alternate Storage Site

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and

b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

Implementation Standards

Std.01 — Mission-critical information shall be backed up on a scheduled basis and stored in a manner logically and physically segmented from the production environment accessible only to authorized individuals. [Source: DIR Control Standards Catalog CP-6]

Std.02 — Ensure that SLAs are consistent with contingency plans, including regional disaster event plans.

Std.03 — Document alternate storage sites in contingency plans.

Std.04 — If alternative temporary locations are used, the level of implemented security controls at these locations is to have logical and physical access controls that are equivalent to the primary site. [Source: Hitrust 12.c Developing and Implementing Continuity Plans Including Information Security]

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.05 PCI —

a. Offline media backups with cardholder data are stored in a secure location. [Source: PCI DSS 9.4.1.1]

b. The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months. [Source: PCI DSS 9.4.1.2]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CP-06.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Alternate storage sites are geographically distinct from primary storage sites and maintain duplicate copies of information and data if the primary storage site is not available. Similarly, alternate processing sites provide processing capability if the primary processing site is not available. Geographically distributed architectures that support contingency requirements may be considered alternate storage sites. Items covered by alternate storage site agreements include environmental conditions at the alternate sites, access rules for systems and facilities, physical and environmental protection requirements, and coordination of delivery and retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential mission and business functions despite compromise, failure, or disruption in organizational systems.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-34; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CP-02, CP-07, CP-08, CP-09, CP-10, MP-04, MP-05, PE-03

CP-06(01) Separation from Primary Site

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

Implementation Standards

Std.01 — Ensure that the risk of a disruption affecting both the primary and alternate storage site is low, or otherwise is at an acceptable level based on an assessment of risk, and document acceptance of risk in System Security Plans (SSPs).

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CP-06(01).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Threats that affect alternate storage sites are defined in organizational risk assessments and include natural disasters, structural failures, hostile attacks, and errors of omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-34; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

RA-03

CP-06(02) Recovery Time and Recovery Point Objectives

Baselines

High

Overlays

FedRAMP High

Requirements

Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

Implementation Standards

Std.01 — Ensure that Service Level Agreements (SLAs) for alternate storage sites align with organizational recovery time objectives (RTOs) and recovery point objectives (RPOs) in accordance with CP-02.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Organizations establish recovery time and recovery point objectives as part of contingency planning. Configuration of the alternate storage site includes physical facilities and the systems supporting recovery operations that ensure accessibility and correct execution.

TxDOT Discussion

Back-up copies of information and software are stored in a physically secure remote location, at a sufficient distance to make them reasonably immune from damage to data at the primary site. Physical and environmental controls are in place for the back-up copies. The organization ensures that backups, including remote and cloud-based backups, are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. Inventory records for the back-up copies, including content and current location, are maintained. [Source: Hitrust CSF 09.l Back-Up]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-34; FedRAMP Security Controls Baseline

Related Controls

CP-02

CP-06(03) Accessibility

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CP-06(03).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites or planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-34; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

RA-03

CP-07 Alternate Processing Site

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of all system operations identified in contingency plans for essential mission and business functions within a time period consistent with recovery time and recovery point objectives in accordance with CP-02 when the primary processing capabilities are unavailable;

b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and

c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

Implementation Standards

Std.01 — Develop alternate processing site agreements (which may include Memoranda of Understanding (MOUs) and service level agreements (SLAs)) that are consistent with contingency plans.

Std.02 — Document alternate processing sites in contingency plans.

Std.03 — Alternate sites must be located sufficiently apart to prevent one disaster from affecting multiple facilities. The sites are designated either hot, warm, or cold based on the amount of time necessary to make the services available.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CP-07.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.04 FedRAMP — The service provider defines a time period consistent with the recovery time objectives and business impact analysis. [Source: FedRAMP Security Controls Baseline CP-7]

Discussion

Alternate processing sites are geographically distinct from primary processing sites and provide processing capability if the primary processing site is not available. The alternate processing capability may be addressed using a physical processing site or other alternatives, such as failover to a cloud-based service provider or other internally or externally provided

processing service. Geographically distributed architectures that support contingency requirements may also be considered alternate processing sites. Controls that are covered by alternate processing site agreements include the environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and the coordination for the transfer and assignment of personnel. Requirements are allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential mission and business functions despite disruption, compromise, or failure in organizational systems.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-34; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CP-02, CP-06, CP-08, CP-09, CP-10, MA-06, PE-03, PE-11, PE-12, PE-17

CP-07(01) Separation from Primary Site

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CP-07(01).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Threats that affect alternate processing sites are defined in organizational assessments of risk and include natural disasters, structural failures, hostile attacks, and errors of omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

The service provider may determine what is considered a sufficient degree of separation between the primary and alternate processing sites, based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites will be less relevant. [Source: FedRAMP Security Controls Baseline CP-7(1)]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-34; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

RA-03

CP-07(02) Accessibility

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CP-07(02).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-34; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

RA-03

CP-07(03) Priority of Service

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

Implementation Standards

Std.01 — Ensure that support and service metrics in service level agreements (SLAs) for priority-of-service provisions are consistent with recovery time objectives (RTOs) in contingency plans (see CP-02).

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CP-07(03).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Priority of service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources for logical alternate processing and/or at the physical alternate processing site. Organizations establish recovery time objectives as part of contingency planning.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-34; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CP-02

CP-07(04) Preparation for Use

Baselines

High

Overlays

FedRAMP High

Requirements

Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions.

Implementation Standards

Std.01 — Document site preparation requirements in the contingency plan.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Site preparation includes establishing configuration settings for systems at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and logistical considerations are in place.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-34; FedRAMP Security Controls Baseline

Related Controls

CM-02, CM-06, CP-04

CP-08 Telecommunications Services

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Establish alternate telecommunications services, including necessary agreements to permit the resumption of all system operations identified in contingency plans for essential mission and business functions within the time period specified in contingency plans when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CP-08.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baseline, the following standard applies:

Std.01 FedRAMP — The service provider defines a time period consistent with the recovery time objectives and business impact analysis.[Source: FedRAMP Security Controls Baseline CP-8]

Discussion

Telecommunications services (for data and voice) for primary and alternate processing and storage sites are in scope for CP-08. Alternate telecommunications services reflect the continuity requirements in

contingency plans to maintain essential mission and business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary or alternate sites. Alternate telecommunications services include additional organizational or commercial ground-based circuits or lines, network-based approaches to telecommunications, or the use of satellites. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.

TxDOT Discussion

Telecommunications restoration plans must provide adequate capabilities for channels of communication between the agency and other organizations involved in the coordination and support of the contingency plan. The contingency plan must document the following:

1. The timeframe for the alternate telecommunications services to begin providing telecommunications capabilities when the primary telecommunications capabilities are unavailable;

2. Channels for necessary communications within the agency and between the agency and other organizations involved;

3. The names of the primary and the alternate telecommunications services providers and points of contact; and

4. The agreements with the primary and alternate telecommunications service providers.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 207; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-34; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CP-02, CP-06, CP-07, SC-07

CP-08(01) Priority of Service Provisions

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

a. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and

b. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

Implementation Standards

Std.01 — Define priority-of-service provisions based on availability requirements and include in the telecommunications service agreement.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CP-08(01).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organizations consider the potential mission or business impact in situations where telecommunications service providers are servicing other organizations with similar priority of service provisions. Telecommunications Service Priority (TSP) is a Federal Communications Commission (FCC)

program that directs telecommunications service providers (e.g., wireline and wireless phone companies) to give preferential treatment to users enrolled in the program when they need to add new lines or have their lines restored following a disruption of service, regardless of the cause. The FCC sets the rules and policies for the TSP program, and the Department of Homeland Security manages the TSP program. The TSP program is always in effect and not contingent on a major disaster or attack taking place. Federal sponsorship is required to enroll in the TSP program.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-34; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

CP-08(02) Single Points of Failure

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Implementation Standards

Std.01 — Ensure that the alternate telecommunication services (for example, telephone service) are separate from the primary service (for

example, internet access) and does not share physical transmission equipment.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CP-08(02).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

In certain circumstances, telecommunications service providers or services may share the same physical lines, which increases the vulnerability of a single failure point. It is important to have provider transparency for the actual physical transmission capability for telecommunication services.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-34; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

CP-08(03) Separation of Primary and Alternate Providers

Baselines

High

Overlays

FedRAMP High

Requirements

Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Threats that affect telecommunications services are defined in organizational assessments of risk and include natural disasters, structural failures, cyber or physical attacks, and errors of omission or commission. Organizations can reduce common susceptibilities by minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide

alternate telecommunications services that meet the separation needs addressed in the risk assessment.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-34; FedRAMP Security Controls Baseline

Related Controls

None.

CP-08(04) Provider Contingency Plan

Baselines

High

Overlays

FedRAMP High

Requirements

a. Require primary and alternate telecommunications service providers to have contingency plans;

b. Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and

c. Obtain evidence of contingency testing and training by providers annually.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security and state and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-34; FedRAMP Security Controls Baseline

Related Controls

CP-03, CP-04

CP-09 System Backup

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Conduct backups of user-level information contained in any component of the system at a frequency set in accordance with the system's recovery point objectives;

b. Conduct backups of system-level information contained in the system in accordance with the recovery point objective (RPO) as defined in the contingency plan (see CP-02);

c. Conduct backups of system documentation, including security- and privacy-related documentation when created or received, when updated, or as defined in the contingency plan, System Security Plan (SSP), or both when both are available; and

d. Protect the confidentiality, integrity, and availability of backup information.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Backups, including remote and cloud-based backups, must be compliant with TxDOT requirements for encryption (see SC-13) and protecting data at rest (see SC-28).

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CP-09.

TX-RAMP Correspondence

For systems subject to TX-RAMP Level 1 or Level 2 requirements, the following standard applies:

Std.03 TX-RAMP —

a. Conduct daily incremental and weekly full backups of user-level information contained in system components;

b. Conduct daily incremental and weekly full backups of system-level information contained in the system.

[Source: TX-RAMP Manual CP-9]

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standards apply:

Std.04 FedRAMP —

a. Conduct backups of user-level information contained in any components of the system at the following frequency: daily incremental, weekly full;

b. Conduct backups of system-level information contained in the system at the following frequency: daily incremental, weekly full;

c. Conduct backups of system documentation, including security- and privacy-related documentation at the following frequency: daily incremental, weekly full; and

d. Protect the confidentiality, integrity, and availability of backup information.

[Source: FedRAMP Security Controls Baseline CP-9]

Std.05 FedRAMP — The service provider shall determine what elements of the cloud environment require the Information System Backup control. The service provider shall determine how Information System Backup is going to be verified and appropriate periodicity of the check. [Source: FedRAMP Security Controls Baseline CP-9]

Std.06 FedRAMP — The service provider maintains at least three backup copies of user-level information (at least one of which is available online) or provides an equivalent alternative. [Source: FedRAMP Security Controls Baseline CP-9]

Std.07 FedRAMP — The service provider maintains at least three backup copies of system-level information (at least one of which is available online) or provides an equivalent alternative. [Source: FedRAMP Security Controls Baseline CP-9]

Std.08 FedRAMP — The service provider maintains at least three backup copies of information system documentation including security information (at least one of which is available online) or provides an equivalent alternative. [Source: FedRAMP Security Controls Baseline CP-9]

Discussion

System-level information includes system state information, operating system software, middleware, application software, and licenses. User-level information includes information other than system-level information. Mechanisms employed to protect the integrity of system backups include digital signatures and cryptographic hashes. Protection of system backup information while in transit is addressed by MP-05 and SC-08. System backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Organizations may be subject to laws, executive orders, directives, regulations, or policies with requirements regarding specific categories of information (e.g., personal health information). Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 186; NIST SP 800-34, 800-130, 800-152; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CP-02, CP-06, CP-10, MP-04, MP-05, SC-08, SC-12, SC-13, SI-04, SR-02

CP-09(01) Testing for Reliability and Integrity

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Test backup information at the frequency defined in the contingency plan, or monthly if not otherwise specified, to verify media reliability and information integrity.

Implementation Standards

Std.01 — Test all backup information technologies, including full system restoration, when new backup technologies are initially implemented; and when equipment is relocated.

Std.02 —

a. Test the complete backup information of critical information systems at least annually and of non-critical systems using a risk-based approach.

b. For non-critical systems, testing may be conducted on random files versus entire system restoration.

c. Virus scans must be performed on backups unless real-time scanning is performed on the information system where backups are retained.

Std.03 — A formal test need not be conducted if the organization completed a real-world restore of the information system during the year.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CP-09(01).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organizations need assurance that backup information can be reliably retrieved. Reliability pertains to the systems and system components where the backup information is stored, the operations used to retrieve the information, and the integrity of the information being retrieved.

Independent and specialized tests can be used for each of the aspects of reliability. For example, decrypting and transporting (or transmitting) a random sample of backup files from the alternate storage or backup site and comparing the information to the same information at the primary processing site can provide such assurance.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 186; NIST SP 800-34, 800-130, 800-152; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CP-04

CP-09(02) Test Restoration Using Sampling

Baselines

High

Overlays

FedRAMP High

Requirements

Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Organizations need assurance that system functions can be restored correctly and can support established organizational missions. To ensure that the selected system functions are thoroughly exercised during contingency plan testing, a sample of backup information is retrieved to determine whether the functions are operating as intended. Organizations can determine the sample size for the functions and backup information based on the level of assurance needed.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FIPS 140, 186; NIST SP 800-34, 800-130, 800-152; FedRAMP Security Controls Baseline

Related Controls

CP-04

CP-09(03) Separate Storage for Critical Information

Baselines

High

Overlays

FedRAMP High

Requirements

Store backup copies of critical system software and other security-related information as defined in the System Security Plan (SSP) or contingency plan in a separate facility or in a fire rated container that is not collocated with the operational system.

Implementation Standards

Std.01 — Ensure that backups, including remote and cloud-based backups, are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. [Source: Hitrust 09.l Back-up]

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Separate storage for critical information applies to all critical information regardless of the type of backup storage media. Critical system software includes operating systems, middleware, cryptographic key management systems, and intrusion detection systems. Security-related information

includes inventories of system hardware, software, and firmware components. Alternate storage sites, including geographically distributed architectures, serve as separate storage facilities for organizations. Organizations may provide separate storage by implementing automated backup processes at alternative storage sites (e.g., data centers). The General Services Administration (GSA) establishes standards and specifications for security and fire rated containers.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FIPS 140, 186; NIST SP 800-34, 800-130, 800-152; FedRAMP Security Controls Baseline

Related Controls

CM-02, CM-06, CM-08

CP-09(05) Transfer to Alternate Storage Site

Baselines

High

Overlays

FedRAMP High

Requirements

Transfer system backup information to the alternate storage site at a time period and transfer rate consistent with the recovery time and recovery point objectives as defined in the contingency plan or System Security Plan (SSP).

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.01 FedRAMP — Transfer system backup information to the alternate storage site at a time period and transfer rate consistent with the recovery time and recovery point objectives defined in the service provider and organization SLA. [Source: FedRAMP Security Controls Baseline CP-9(5)]

Discussion

System backup information can be transferred to alternate storage sites either electronically or by the physical shipment of storage media.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FIPS 140, 186; NIST SP 800-34, 800-130, 800-152; FedRAMP Security Controls Baseline

Related Controls

CP-07, MP-03, MP-04, MP-05

CP-09(08) Cryptographic Protection

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of backup information as identified in the contingency plan or applicable System Security Plan (SSP).

Implementation Standards

Std.01 — Implement encryption algorithms in accordance with SC-13.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.03 CJIS — Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of CJI. [Source: CJIS CP-09(08)]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.02 FedRAMP — Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of all backup files. [Source: FedRAMP Security Controls Baseline CP-9(8)]

Discussion

The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. The strength of

mechanisms selected is commensurate with the security category or classification of the information. Cryptographic protection applies to system backup information in storage at both primary and alternate locations. Organizations that implement cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

Note that this enhancement requires the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13.) [Source: FedRAMP Security Controls Baseline CP-9(8)]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 186; NIST SP 800-34, 800-130, 800-152; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

SC-12, SC-13, SC-28

CP-10 System Recovery and Reconstitution

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Provide for the recovery and reconstitution of the system to a known state within the time period consistent with recovery time and recovery point

objectives as defined in the contingency plan after a disruption, compromise, or failure.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Recovery of the system after a failure or other contingency must be done in a trusted, secure, and verifiable manner.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CP-10.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities; recovery point, recovery time, and reconstitution objectives; and organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities, reestablishment of continuous monitoring activities, system reauthorization (if required), and activities to prepare the system and organization for future disruptions, breaches, compromises, or failures. Recovery and reconstitution capabilities can include automated mechanisms and manual procedures. Organizations establish recovery time and recovery point objectives as part of contingency planning.

TxDOT Discussion

Secure information system recovery and reconstitution may include, but is not limited to:

1. Resetting all system parameters (either default or organization-established) to secure values;

2. Reinstalling patches;

3. Reestablishing configuration settings;

4. Reinstalling application and system software;

5. Loading information from the most recent, known secure backups; and

6. Testing the system.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-34; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CP-02, CP-04, CP-06, CP-07, CP-09, IR-04, SA-08, SC-24

CP-10(02) Transaction Recovery

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Implement transaction recovery for systems that are transaction-based.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement CP-10(02).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journaling.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-34; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

CP-10(04) Restore Within Time Period

Baselines

High

Overlays

FedRAMP High

Requirements

Provide the capability to restore system components within restoration time periods as defined in the contingency plan from configuration-controlled and integrity-protected information representing a known, operational state for the components.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.01 FedRAMP — Provide the capability to restore system components within a time period consistent with the restoration time-periods defined in the service provider and organization SLA from configuration-controlled and integrity-protected information representing a known, operational state for the components. [Source: FedRAMP Security Controls Baseline CP-10(4)]

Discussion

Restoration of system components includes reimaging, which restores the components to known, operational states.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-34; FedRAMP Security Controls Baseline

Related Controls

CM-02, CM-06

CP-11 Alternate Communications Protocols

Baselines

Low, Moderate, High

Overlays

N/A

Requirements

Provide the capability to employ alternative communications protocols as defined in contingency plans in support of maintaining continuity of operations.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Contingency plans and the contingency training or testing associated with those plans incorporate an alternate communications protocol capability as part of establishing resilience in organizational systems. Switching communications protocols may affect software applications and operational aspects of systems. Organizations assess the potential side effects of introducing alternate communications protocols prior to implementation.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

None.

Related Controls

CP-02, CP-08

IA — Identification and Authentication

IA-01 Policy and Procedures

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level identification and authentication policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;

b. Designate a senior management official as defined in the identification and authentication policy to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and

c. Review and update the current identification and authentication:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 8.1.1 and 8.1.2.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.03 PCI — Authentication policies and procedures are documented and communicated to all users including:

a. Guidance on selecting strong authentication factors.

b. Guidance for how users should protect their authentication factors.

c. Instructions not to reuse previously used passwords/passphrases.

d. Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.

[Source: PCI DSS 8.3.8]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.04 CJIS — Review and update the current identification and authentication policy and procedures following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. [Source: CJIS IA-01]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Identification and authentication policy and procedures address the controls in the IA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of identification and authentication policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to identification and authentication policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; FIPS 201; NIST SP 800-12, 800-30, 800-39, 800-63-3, 800-73-4, 800-76-2, 800-78-4, 800-100; NIST IR 7874; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-01, PM-09, PS-08, SI-12

IA-02 Identification and Authentication (Organizational Users)

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

Implementation Standards

Std.01 — Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification shall be authenticated before the information resources system may grant that user access. [Source: DIR Control Standards Catalog IA-2]

Std.02 — Each system's identification and authentication mechanisms must comply with the TxDOT Identification and Authentication Standard.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.08 PCI — All users are assigned a unique ID before access to system components or cardholder data is allowed. [Source: PCI DSS 8.2.1]

Std.09 PCI — MFA systems are implemented as follows:

a. The MFA system is not susceptible to replay attacks.

b. MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period.

c. At least two different types of authentication factors are used.

d. Success of all authentication factors is required before access is granted.

[Source: PCI DSS 8.5.1]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IA-02.

Std.03 CJIS — Rescinded in V4.0.

Std.04 CJIS — Rescinded in V4.0.

Std.05 CJIS — Rescinded in V4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standards apply:

Std.06 FedRAMP — Multi-factor authentication must be phishing-resistant. [Source: FedRAMP Security Controls Baseline IA-2]

Std.07 FedRAMP — All uses of encrypted virtual private networks must meet all applicable Federal requirements and architecture, dataflow, and security and privacy controls must be documented, assessed, and authorized to operate. [Source: FedRAMP Security Controls Baseline IA-2]

Discussion

Organizations can satisfy the identification and authentication requirements by complying with the requirements in Homeland Security Presidential Directive 12. Organizational users include employees or individuals who organizations consider to have an equivalent status to employees (e.g., contractors and guest researchers). Unique identification and authentication of users applies to all accesses other than those that are explicitly identified in AC-14 and that occur through the authorized use of group authenticators without individual authentication. Since processes execute on behalf of groups and roles, organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity.

Organizations employ passwords, physical authenticators, or biometrics to authenticate user identities or, in the case of multi-factor authentication, some combination thereof. Access to organizational systems is defined as either local access or network access. Local access is any access to organizational systems by users or processes acting on behalf of users, where access is obtained through direct connections without the use of networks. Network access is access to organizational systems by users (or processes acting on behalf of users) where access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks.

The use of encrypted virtual private networks for network connections between organization-controlled endpoints and non-organization-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network. Identification and authentication requirements for non-organizational users are described in IA-08.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

"Phishing-resistant" authentication refers to authentication processes designed to detect and prevent disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system. [Source: FedRAMP Security Controls Baseline IA-2]

TxDOT References

Identification and Authentication Standard; Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 201, 202; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4, 800-79-2, 800-156, 800-166; NIST IR 7539, 7676, 7817, 7849, 7870, 7874, 7966; CJIS Security Policy; FedRAMP Security Controls Baseline; PCI DSS

Related Controls

AC-02, AC-03, AC-04, AC-14, AC-17, AC-18, AU-01, AU-06, IA-04, IA-05, IA-08, MA-04, MA-05, PE-02, PL-04, SA-04, SA-08

IA-02(01) Multi-Factor Authentication to Privileged Accounts

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Implement multi-factor authentication for access to privileged accounts.

Implementation Standards

Std.01 — For access to privileged accounts, implement multi-factor authentication in accordance with the TxDOT Identification and Authentication Standard.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 8.3.1 and 8.4.1.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IA-02(01).

Std.02 CJIS — Rescinded in v4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.03 FedRAMP — Multi-factor authentication must be phishing-resistant. [Source: FedRAMP Security Controls Baseline IA-2(1)]

Discussion

Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification (PIV) card or the Department of Defense (DoD) Common Access Card (CAC). In addition to authenticating users at the system level (i.e., at logon), organizations may employ authentication mechanisms at the application level, at their discretion, to provide increased security. Regardless of the type of access (i.e., local, network, remote), privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

Multi-factor authentication to subsequent components in the same user domain is not required. [Source: FedRAMP Security Controls Baseline IA-2(1)]

TxDOT References

Identification and Authentication Standard; Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 201, 202; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4, 800-79-2, 800-156, 800-166; NIST IR 7539, 7676, 7817, 7849, 7870, 7874, 7966; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-05, AC-06

IA-02(02) Multi-Factor Authentication to Non-Privileged Accounts

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Implement multi-factor authentication for access to non-privileged accounts.

Implementation Standards

None.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 8.4.2.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.01 PCI — Rescinded in V3.0.

Std.02 PCI — MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the Cardholder Data Environment (CDE) as follows:

a. All remote access by all personnel, both users and administrators, originating from outside the entity's network.

b. All remote access by third parties and vendors.

[Source: PCI DSS 8.4.3]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirements IA-02(02).

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user unless the access to CJI is indirect as described in Identification and Authentication (IA). [Source: CJIS 5.20.7.2]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.04 FedRAMP — Multi-factor authentication must be phishing-resistant. [Source: FedRAMP Security Controls Baseline IA-2(2)]

Discussion

Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification card or the DoD Common Access Card. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access (i.e., local, network, remote), non-privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can provide additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

Multi-factor authentication to subsequent components in the same user domain is not required. [Source: FedRAMP Security Controls Baseline IA-2(2)]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FIPS 140, 201, 202; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4, 800-79-2, 800-156, 800-166; NIST IR 7539, 7676, 7817, 7849, 7870, 7874, 7966; PCI DSS; CJIS Security Policy

Related Controls

AC-05

IA-02(05) Individual Authentication with Group Authentication

Baselines

N/A

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Individual authentication prior to shared group authentication mitigates the risk of using group accounts or authenticators.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

IA-02(06) Access to Accounts — Separate Device

Baselines

N/A

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

Implement multi-factor authentication for local, network, and remote access to privileged accounts and non-privileged accounts such that:

a. One of the factors is provided by a device separate from the system gaining access; and

b. The device meets FIPS-validated or NSA-approved cryptography.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

The purpose of requiring a device that is separate from the system to which the user is attempting to gain access for one of the factors during multi-factor authentication is to reduce the likelihood of compromising authenticators or credentials stored on the system. Adversaries may be able to compromise such authenticators or credentials and subsequently impersonate authorized users. Implementing one of the factors on a separate device (e.g., a hardware token), provides a greater strength of mechanism and an increased level of assurance in the authentication process.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

PIV=separate device. Please refer to NIST SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials.

See SC-13 Guidance for more information on FIPS-validated or NSA-approved cryptography.

[Source: FedRAMP Security Controls Baseline IA-2(6)]

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

AC-06

IA-02(08) Access to Accounts — Replay Resistant

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Implement replay-resistant authentication mechanisms for access to accounts requiring IAL-2 or IAL-3 level authentication as described in the TxDOT Identification and Authentication Standard.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IA-02(08).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low baseline.

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.01 FedRAMP — Implement replay-resistant authentication mechanisms for access to privileged accounts and non-privileged accounts. [Source: FedRAMP Security Controls Baseline IA-2(8)]

Discussion

Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include protocols that use nonces or challenges such as time synchronous or cryptographic authenticators.

TxDOT Discussion

None.

TxDOT References

Identification and Authentication Standard; Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 201, 202; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4, 800-79-2, 800-156, 800-166; NIST IR 7539, 7676, 7817, 7849, 7870, 7874, 7966; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

IA-02(12) Acceptance of PIV Credentials

Baselines

N/A

Overlays

CJIS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Accept and electronically verify Personal Identity Verification-compliant credentials.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IA-02(12).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Acceptance of Personal Identity Verification (PIV)-compliant credentials applies to organizations implementing logical access control and physical access control systems. PIV-compliant credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. The adequacy and reliability of PIV card issuers are authorized using SP 800-79-2. Acceptance of PIV-compliant credentials includes derived PIV credentials, the use of which is addressed in SP 800-166. The DOD Common Access Card (CAC) is an example of a PIV credential.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

Include Common Access Card (CAC), i.e., the DoD technical implementation of PIV/FIPS 201/HSPD-12. [Source: FedRAMP Security Controls Baseline IA-2(12)]

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

IA-03 Device Identification and Authentication

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Uniquely identify and authenticate all network-connected endpoint devices before establishing a remote or network connection.

Implementation Standards

Std.01 — Document the protocols used for device identification and authentication in the applicable System Security Plan (SSP).

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.02 CJIS — Uniquely identify and authenticate agency-managed devices before establishing network connections. In the instance of local connection, the device must be approved by the agency and the device must be identified and authenticated prior to connection to an agency asset. [Source: CJIS IA-03]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Devices that require unique device-to-device identification and authentication are defined by type, device, or a combination of type and device. Organization-defined device types include devices that are not owned by the organization. Systems use shared known information (e.g., Media Access Control [MAC], Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and wide area networks. Organizations determine the required strength of authentication mechanisms based on the security categories of systems and mission or business requirements. Because of the challenges of implementing device authentication on a large scale, organizations can restrict the application of the control to a limited number/type of devices based on mission or business needs.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-17, AC-18, AC-19, AU-06, CA-03, CA-09, IA-04, IA-05, IA-11, SI-04

IA-04 Identifier Management

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Manage system identifiers by:

a. Receiving authorization from personnel or roles as defined in the applicable System Security Plan (SSP) to assign an individual, group, role, service, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, service, or device;

c. Assigning the identifier to the intended individual, group, role, service, or device; and

d. Preventing reuse of identifiers for at least one year for individuals, groups, roles, services, or devices.

Implementation Standards

Std.01 — A user's access authorization shall be appropriately modified or removed when the user's employment or job responsibilities within the state organization change. [Source: DIR Control Standards Catalog PS-4]

Std.02 —

a. Sensitive Personal Information, to include SSNs and parts of SSNs, must not be used as system identifiers.

b. Identifier management must ensure that any access to, or action involving, personally identifiable information (PII) is attributable to a unique individual.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.03 PCI — Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows:

a. Account use is prevented unless needed for an exceptional circumstance.

b. Use is limited to the time needed for the exceptional circumstance.

c. Business justification for use is documented.

d. Use is explicitly approved by management.

e. Individual user identity is confirmed before access to an account is granted.

f. Every action taken is attributable to an individual user.

[Source: PCI DSS 8.2.2]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IA-04.

Std.04 CJIS — Rescinded in V4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Common device identifiers include Media Access Control (MAC) addresses, Internet Protocol (IP) addresses, or device-unique token identifiers. The management of individual identifiers is not applicable to shared system

accounts. Typically, individual identifiers are the usernames of the system accounts assigned to those individuals. In such instances, the account management activities of AC-02 use account names provided by IA-04. Identifier management also addresses individual identifiers not necessarily associated with system accounts. Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 201; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-05, IA-02, IA-03, IA-05, IA-08, IA-12, MA-04, PE-02, PE-03, PE-04, PL-04, PM-12, PS-03, PS-04, PS-05

IA-04(04) Identify User Status

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Manage individual identifiers by uniquely identifying each individual as possessing (or not possessing) specific individual status characteristics including, but not limited to, contractor or foreign national.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.01 CJIS — Manage individual identifiers by uniquely identifying each individual as agency or nonagency. [Source: CJIS IA-04(04)]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Characteristics that identify the status of individuals include contractors, foreign nationals, and non-organizational users. Identifying the status of individuals by these characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 201; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

IA-05 Authenticator Management

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;

b. Establishing initial authenticator content for any authenticators issued by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;

e. Changing default authenticators prior to first use;

f. Changing or refreshing authenticators at the frequency defined in the TxDOT Identification and Authentication Standard or when major changes to legislation or security requirements occur;

g. Protecting authenticator content from unauthorized disclosure and modification;

h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and

i. Changing authenticators for group or role accounts when membership to those accounts changes.

Implementation Standards

Std.01 — Rescinded in V2.2.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 2.2.2.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.02 PCI — User identity is verified before modifying any authentication factor. [Source: PCI DSS 8.3.3]

Std.05 PCI — If accounts used by systems or applications can be used for interactive login, they are managed as follows:

a. Interactive use is prevented unless needed for an exceptional circumstance.

b. Interactive use is limited to the time needed for the exceptional circumstance.

c. Business justification for interactive use is documented.

d. Interactive use is explicitly approved by management.

e. Individual user identity is confirmed before access to account is granted.

f. Every action taken is attributable to an individual user.

[Source: PCI DSS 8.6.1]

Std.06 PCI — Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code. [Source: PCI DSS 8.6.2]

Std.07 PCI — Passwords/passphrases for any application and system accounts are protected against misuse as follows:

a. Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise.

b. Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases. [Source: PCI DSS 8.6.3]

For systems processing PCI DSS data, or that support PCI DSS processes, IA-05b. is superseded by the assignment defined in PCI DSS requirement 8.3.11:

Std.03 PCI — Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used:

a. Factors are assigned to an individual user and not shared among multiple users.

b. Physical and/or logical controls ensure only the intended user can use that factor to gain access.

[Source: PCI DSS 8.3.11]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.08 CJIS — Manage system authenticators by: changing or refreshing authenticators annually or when there is evidence of authenticator compromise.

j. AAL2 Specific Requirements

All credential service providers (CSPs) authenticating claimants at Authenticator Assurance Level 2 (AAL2) SHALL be assessed on the following criteria:

(1) Authentication SHALL occur by the use of either a multi-factor authenticator or a combination of two single-factor authenticators.

(2) If the multi-factor authentication process uses a combination of two single-factor authenticators, then it SHALL include a Memorized Secret authenticator and a possession-based authenticator.

(3) Cryptographic authenticators used at AAL2 SHALL use approved cryptography.

(4) At least one authenticator used at AAL2 SHALL be replay resistant.

(5) Communication between the claimant and verifier SHALL be via an authenticated protected channel.

(6) Verifiers operated by government agencies at AAL2 SHALL be validated to meet the requirements of FIPS 140 Level 1.

(7) Authenticators procured by government agencies SHALL be validated to meet the requirements of FIPS 140 Level 1.

(8) If a device such as a smartphone is used in the authentication process, then the unlocking of that device (typically done using a PIN or biometric) SHALL NOT be considered one of the authentication factors.

(9) If a biometric factor is used in authentication at AAL2, then the performance requirements stated in IA-5 m Biometric Requirements SHALL be met.

(10) Reauthentication of the subscriber SHALL be repeated at least once per 12 hours during an extended usage session.

(11) Reauthentication of the subscriber SHALL be repeated following any period of inactivity lasting 30 minutes or longer.

(12) The CSP SHALL employ appropriately tailored security controls from the moderate baseline of security controls defined in the CJISSECPOL.

The CSP SHALL ensure that the minimum assurance-related controls for moderate-impact systems are satisfied.

(13) The CSP SHALL comply with records retention policies in accordance with applicable laws and regulations.

(14) If the CSP opts to retain records in the absence of any mandatory requirements, then the CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine how long records should be retained and SHALL inform subscribers of that retention policy.

k. Privacy requirements that apply to all CSPs, verifiers, and RPs

(1) The CSP SHALL employ appropriately tailored privacy controls from the CJISSECPOL.

(2) If the CSP processes attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, or to comply with law or legal process, then the CSP SHALL

implement measures to maintain predictability and manageability commensurate with the associated privacy risk.

l. General requirements applicable to AAL2 authentication process

(1) CSPs SHALL provide subscriber instructions on how to appropriately protect a physical authenticator against theft or loss.

(2) The CSP SHALL provide a mechanism to revoke or suspend the authenticator immediately upon notification from subscriber that loss or theft of the authenticator is suspected.

(3) If required by the authenticator type descriptions in IA-5(1), then the verifier SHALL implement controls to protect against online guessing attacks.

(4) If required by the authenticator type descriptions in IA-5(1) and the description of a given authenticator does not specify otherwise, then the verifier SHALL limit consecutive failed authentication attempts on a single account to no more than 100.

(5) If signed attestations are used, then they SHALL be signed using a digital signature that provides at least the minimum security strength specified in the latest revision of 112 bits as of the date of this publication.

(6) If the verifier and CSP are separate entities (as shown by the dotted line in Figure 8 Digital Identity Model), then communications between the verifier and CSP SHALL occur through a mutually-authenticated secure channel (such as a client-authenticated TLS connection).

(7) If the CSP provides the subscriber with a means to report loss, theft, or damage to an authenticator using a backup or alternate authenticator, then that authenticator SHALL be either a memorized secret or a physical authenticator.

(8) If the CSP chooses to verify an address of record (i.e., email, telephone, postal) and suspend authenticator(s) reported to have been compromised, then...The suspension SHALL be reversible if the subscriber successfully authenticates to the CSP using a valid (i.e., not suspended) authenticator and requests reactivation of an authenticator suspended in this manner.

(9) If and when an authenticator expires, it SHALL NOT be usable for authentication.

(10) The CSP SHALL have a documented process to require subscribers to surrender or report the loss of any physical authenticator containing

attribute certificates signed by the CSP as soon as practical after expiration or receipt of a renewed authenticator.

(11) CSPs SHALL revoke the binding of authenticators immediately upon notification when an online identity ceases to exist (e.g., subscriber's death, discovery of a fraudulent subscriber), when requested by the subscriber, or when the CSP determines that the subscriber no longer meets its eligibility requirements.

(12) The CSP SHALL have a documented process to require subscribers to surrender or report the loss of any physical authenticator containing certified attributes signed by the CSP within five (5) days after revocation or termination takes place.

m. Biometric Requirements

(1) Biometrics SHALL be used only as part of multi-factor authentication with a physical authenticator (something you have).

(2) An authenticated protected channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and verifier SHALL be established.

(3) The sensor or endpoint SHALL be authenticated prior to capturing the biometric sample from the claimant.

(4) The biometric system SHALL operate with an FMR [ISO/IEC 2382-37] of 1 in 1000 or better. This FMR SHALL be achieved under conditions of a conformant attack (i.e., zero-effort impostor attempt) as defined in [ISO/IEC 30107-1].

(5) The biometric system SHALL allow no more than 5 consecutive failed authentication attempts or 10 consecutive failed attempts if PAD demonstrating at least 90% resistance to presentation attacks is implemented.

(6) Once the limit on authentication failures has been reached, the biometric authenticator SHALL either:

i. Impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt, or

ii. Disable the biometric user authentication and offer another factor (e.g., a different biometric modality or a PIN/Passcode if it is not already a required factor) if such an alternative method is already available.

(7) The verifier SHALL make a determination of sensor and endpoint performance, integrity, and authenticity.

(8) If biometric comparison is performed centrally, then use of the biometric as an authentication factor SHALL be limited to one or more specific devices that are identified using approved cryptography.

(9) If biometric comparison is performed centrally, then a separate key SHALL be used for identifying the device.

(10) If biometric comparison is performed centrally, then biometric revocation, referred to as biometric template protection in ISO/IEC 24745, SHALL be implemented.

(11) If biometric comparison is performed centrally, all transmission of biometrics SHALL be over the authenticated protected channel.

(12) Biometric samples and any biometric data derived from the biometric sample such as a probe produced through signal processing SHALL be zeroized immediately after any training or research data has been derived.

n. Authenticator binding refers to the establishment of an association between a specific authenticator and a subscriber's account, enabling the authenticator to be used — possibly in conjunction with other authenticators — to authenticate for that account.

(1) Authenticators SHALL be bound to subscriber accounts by either issuance by the CSP as part of enrollment or associating a subscriber-provided authenticator that is acceptable to the CSP.

(2) Throughout the digital identity lifecycle, CSPs SHALL maintain a record of all authenticators that are or have been associated with each identity.

(3) The CSP or verifier SHALL maintain the information required for throttling authentication attempts.

(4) The CSP SHALL also verify the type of user-provided authenticator so verifiers can determine compliance with requirements at each AAL.

(5) The record created by the CSP SHALL contain the date and time the authenticator was bound to the account.

(6) When any new authenticator is bound to a subscriber account, the CSP SHALL ensure that the binding protocol and the protocol for provisioning the associated key(s) are done at AAL2.

(7) Protocols for key provisioning SHALL use authenticated protected channels or be performed in person to protect against MitM attacks.

(8) Binding of multi-factor authenticators SHALL require multi-factor authentication (or equivalent) at identity proofing.

(9) At enrollment, the CSP SHALL bind at least one, and SHOULD bind at least two, physical (something you have) authenticators to the subscriber's online identity, in addition to a memorized secret or one or more biometrics.

(10) At enrollment, authenticators at AAL2 and IAL2 SHALL be bound to the account.

(11) If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then the applicant SHALL identify themselves in each new binding transaction by presenting a temporary secret which was either established during a prior transaction, or sent to the applicant's phone number, email address, or postal address of record.

(12) If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then long-term authenticator secrets are delivered to the applicant within a protected session.

(13) If enrollment and binding are being done in person and cannot be completed in a single physical encounter, the applicant SHALL identify themselves in person by either using a secret as described in IA-5 n (12) above, or through use of a biometric that was recorded during a prior encounter.

(14) If enrollment and binding are being done in person and cannot be completed in a single physical encounter, temporary secrets SHALL NOT be reused.

(15) If enrollment and binding are being done in person and cannot be completed in a single physical encounter and the CSP issues long-term authenticator secrets during a physical transaction, they SHALL be loaded locally onto a physical device that is issued in person to the applicant or delivered in a manner that confirms the address of record.

(16) Before adding a new authenticator to a subscriber's account, the CSP SHALL first require the subscriber to authenticate at AAL2 (or a higher AAL) at which the new authenticator will be used.

(17) If the subscriber's account has only one authentication factor bound to it, the CSP SHALL require the subscriber to authenticate at AAL1 in order to bind an additional authenticator of a different authentication factor.

(18) If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2, that subscriber SHALL repeat the identity proofing process described in IA-12.

(19) If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2 or IAL3, the CSP SHALL require the claimant to authenticate using an authenticator of the remaining factor, if any, to confirm binding to the existing identity.

(20) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then it requires entry of a confirmation code sent to an address of record.

(21) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code SHALL consist of at least 6 random alphanumeric characters generated by an approved random bit generator [SP 800-90Ar1].

(22) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code SHALL be valid for a maximum of 7 days but MAY be made valid up to 21 days via an exception process to accommodate addresses outside the direct reach of the U.S. Postal Service. Confirmation codes sent by means other than physical mail SHALL be valid for a maximum of 5 minutes.

o. Session Management: The following requirements apply to applications where a session is maintained between the subscriber and relying party to allow multiple interactions without repeating the authentication event each time.

Once an authentication event has taken place, it is often desirable to allow the subscriber to continue using the application across multiple subsequent interactions without requiring them to repeat the authentication event. This requirement is particularly true for federation scenarios where the authentication event necessarily involves several components and parties coordinating across a network.

(1) Session Binding Requirements: A session occurs between the software that a subscriber is running — such as a browser, application, or operating system (i.e., the session subject) — and the RP or CSP that the subscriber is accessing (i.e., the session host).

a. A session is maintained by a session secret which SHALL be shared between the subscriber's software and the service being accessed.

b. The secret SHALL be presented directly by the subscriber's software or possession of the secret SHALL be proven using a cryptographic mechanism.

c. The secret used for session binding SHALL be generated by the session host in direct response to an authentication event.

d. A session SHALL NOT be considered at a higher AAL than the authentication event.

e. Secrets used for session binding SHALL be generated by the session host during an interaction, typically immediately following authentication.

f. Secrets used for session binding SHALL be generated by an approved random bit generator [SP 800-90Ar1].

g. Secrets used for session binding SHALL contain at least 64 bits of entropy.

h. Secrets used for session binding SHALL be erased or invalidated by the session subject when the subscriber logs out.

i. Secrets used for session binding SHALL be sent to and received from the device using an authenticated protected channel.

j. Secrets used for session binding SHALL time out and not be accepted after the times specified in IA-5 j (13) as appropriate for the AAL.

k. Secrets used for session binding SHALL NOT be available to insecure communications between the host and subscriber's endpoint.

l. Authenticated sessions SHALL NOT fall back to an insecure transport, such as from https to http, following authentication.

m. URLs or POST content SHALL contain a session identifier that SHALL be verified by the RP to ensure that actions taken outside the session do not affect the protected session.

n. Browser cookies SHALL be tagged to be accessible only on secure (HTTPS) sessions.

o. Browser cookies SHALL be accessible to the minimum practical set of hostnames and paths.

p. Expiration of browser cookies SHALL NOT be depended upon to enforce session timeouts.

q. The presence of an OAuth access token SHALL NOT be interpreted by the RP as presence of the subscriber, in the absence of other signals.

(2) Reauthentication Requirements

a. Continuity of authenticated sessions SHALL be based upon the possession of a session secret issued by the verifier at the time of authentication and optionally refreshed during the session.

b. Session secrets SHALL be non-persistent, i.e., they SHALL NOT be retained across a restart of the associated application or a reboot of the host device.

c. Periodic reauthentication of sessions (at least every 12 hours per session) SHALL be performed to confirm the continued presence of the subscriber at an authenticated session.

d. A session SHALL NOT be extended past the guidelines in IA-5 o (2) a – j based on presentation of the session secret alone.

e. Prior to session expiration, the reauthentication time limit SHALL be extended by prompting the subscriber for the authentication factor(s) of a memorized secret or biometric.

f. If federated authentication is being used, then since the CSP and RP often employ separate session management technologies, there SHALL NOT be any assumption of correlation between these sessions.

g. An RP requiring reauthentication through a federation protocol SHALL — if possible within the protocol — specify the maximum (see IA-5 j (10)) acceptable authentication age to the CSP.

h. If federated authentication if being used and an RP has specific authentication age (see IA-5 j [10]) requirements that it has communicated to the CSP, then the CSP SHALL reauthenticate the subscriber if they have not been authenticated within that time period.

i. If federated authentication is being used, the CSP SHALL communicate the authentication event time to the RP to allow the RP to decide if the assertion is sufficient for reauthentication and to determine the time for the next reauthentication event.[Source: CJIS IA-05]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.04 FedRAMP — Authenticators must be compliant with NIST SP 800-63-3 Digital Identity Guidelines IAL, AAL, FAL level 1.[Source: FedRAMP Security Controls Baseline IA-5]

Discussion

Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges. Device authenticators include certificates and passwords. Initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, the requirements for authenticator content contain specific criteria or characteristics (e.g., minimum password length). Developers may deliver system components with factory default authentication credentials (i.e., passwords) to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant risk. The requirement to protect individual authenticators may be implemented via control PL-04 or PS-06 for authenticators in the possession of individuals and by controls AC-03, AC-06, and SC-28 for authenticators stored in organizational systems, including passwords stored in hashed or encrypted formats or files containing encrypted or hashed passwords accessible with administrator privileges.

Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics (e.g., minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication). Actions can be taken to safeguard individual authenticators, including maintaining possession of authenticators, not sharing authenticators with others, and immediately reporting lost, stolen, or compromised authenticators. Authenticator management includes issuing and revoking authenticators for temporary access when no longer needed.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

SP 800-63C Section 6.2.3 Encrypted Assertion requires that authentication assertions be encrypted when passed through third parties, such as a browser. For example, a SAML assertion can be encrypted using XML-

Encryption, or an OpenID Connect ID Token can be encrypted using JSON Web Encryption (JWE). [Source: FedRAMP Security Controls Baseline IA-5]

TxDOT References

Identification and Authentication Standard; Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 180, 201, 202; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4; NIST IR 7539, 7817, 7849, 7870, 8040; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-03, AC-06, CM-06, IA-02, IA-04, IA-07, IA-08, MA-04, PE-02, PL-04, SC-12, SC-13

IA-05(01) Password-Based Authentication

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

For password-based authentication:

a. Maintain a list of commonly-used, expected, or compromised passwords and update the list at least every 90 days and when organizational passwords are suspected to have been compromised directly or indirectly;

b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-05(01)a;

c. Transmit passwords only over cryptographically-protected channels;

d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;

e. Require immediate selection of a new password upon account recovery;

f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;

g. Employ automated tools to assist the user in selecting strong password authenticators; and

h. Enforce the following composition and complexity rules: composition and complexity rules in accordance with the TxDOT Identification and Authentication Standard.

Implementation Standards

Std.01 — This control applies only to systems that use a memorized secret (passphrase, PIN, etc.).

Std.02 — For all requirements concerning the use of memorized secrets, see the TxDOT Identification and Authentication Standard.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 8.3.2 and 8.3.7.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.03 PCI — If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity:

a. A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters).

b. Contain both numeric and alphabetic characters.

[Source: PCI DSS 8.3.6]

Std.04 PCI — If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either:

a. Passwords/passphrases are changed at least once every 90 days; or

b. The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.

[Source: PCI DSS 8.3.9]

Std.05 PCI — If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows:

a. Set to a unique value for first-time use and upon reset.

b. Forced to be changed immediately after the first use.

[Source: PCI DSS 8.3.5]

Std.10 PCI — Rescinded in v4.0.

Std.11 PCI — Ensure that the following is included in contracts or SLAs for service providers:

If passwords/passphrases are used as the only authentication factor for customer user access (i.e., in any single-factor authentication implementation) then either:

a. Passwords/passphrases are changed at least once every 90 days; or

b. The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.

[Source: PCI DSS 8.3.10.1]

CJIS Correspondence

For systems processing CJIS data, IA-05(01) is superseded by CJIS requirement IA-05(01):

Std.12 CJIS —

a. Memorized Secret Authenticators and Verifiers:

1. Maintain a list of commonly-used, expected, or compromised passwords and update the list quarterly and when organizational passwords are suspected to have been compromised directly or indirectly;

(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list at least every 90 days and when organizational passwords are suspected to have been compromised directly or indirectly;

2. Require immediate selection of a new password upon account recovery;

3. Allow user selection of long passwords and passphrases, including spaces and all printable characters;

4. Employ automated tools to assist the user in selecting strong password authenticators;

5. Enforce the following composition and complexity rules when agencies elect to follow basic password standards:

(a) Not be a proper name.

(b) Not be the same as the Userid.

(c) Expire within a maximum of 90 calendar days.

(d) Not be identical to the previous ten (10) passwords.

(e) Not be displayed when entered.

6. If chosen by the subscriber, memorized secrets SHALL be at least 8 characters in length.

7. If chosen by the CSP or verifier using an approved random number generator, memorized secrets SHALL be at least 6 characters in length.

8. Truncation of the secret SHALL NOT be performed.

9. Memorized secret verifiers SHALL NOT permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant.

10. Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing memorized secrets.

11. When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly used, expected, or compromised.

12. If a chosen secret is found in the list, the CSP or verifier SHALL advise the subscriber that they need to select a different secret.

13. If a chosen secret is found in the list, the CSP or verifier SHALL provide the reason for rejection.

14. If a chosen secret is found in the list, the CSP or verifier SHALL require the subscriber to choose a different value.

15. Verifiers SHALL implement a rate-limiting mechanism that effectively limits failed authentication attempts that can be made on the subscriber's account to no more than five.

16. Verifiers SHALL force a change of memorized secret if there is evidence of compromise of the authenticator.

17. The verifier SHALL use approved encryption when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.

18. The verifier SHALL use an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.

19. Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks.

20. Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function.

21. The salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.

22. Both the salt value and the resulting hash SHALL be stored for each subscriber using a memorized secret authenticator.

23. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL be generated with an approved random bit generator and of sufficient length.

24. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL provide at least the minimum-security strength.

25. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL be stored separately from the memorized secrets.

b. Look-Up Secret Authenticators and Verifiers

1. CSPs creating look-up secret authenticators SHALL use an approved random bit generator to generate the list of secrets.

2. Look-up secrets SHALL have at least 20 bits of entropy.

3. If look-up secrets are distributed online, then they SHALL be distributed over a secure channel in accordance with the post-enrollment binding requirements in IA-5 'n' 17 through 25.

4. Verifiers of look-up secrets SHALL prompt the claimant for the next secret from their authenticator or for a specific (e.g., numbered) secret.

5. A given secret from an authenticator SHALL be used successfully only once.

6. If a look-up secret is derived from a grid (bingo) card, then each cell of the grid SHALL be used only once.

7. Verifiers SHALL store look-up secrets in a form that is resistant to offline attacks.

8. If look-up secrets have at least 112 bits of entropy, then they SHALL be hashed with an approved one-way function.

9. If look-up secrets have less than 112 bits of entropy, then they SHALL be salted and hashed using a suitable one-way key derivation function.

10. If look-up secrets have less than 112 bits of entropy, then the salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.

11. If look-up secrets have less than 112 bits of entropy, then both the salt value and the resulting hash SHALL be stored for each look-up secret.

12. If look-up secrets that have less than 64 bits of entropy, then the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account.

13. The verifier SHALL use approved encryption when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.

14. The verifier SHALL use an authenticated protected channel when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.

c. Out-of-Band Authenticators and Verifiers

1. The out-of-band authenticator SHALL establish a separate channel with the verifier in order to retrieve the out-of-band secret or authentication request.

2. Communication over the secondary channel SHALL be encrypted unless sent via the public switched telephone network (PSTN).

3. Methods that do not prove possession of a specific device, such as voice-over-IP (VoIP) or email, SHALL NOT be used for out-of-band authentication.

4. If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL uniquely authenticate itself by establishing an authenticated protected channel with the verifier.

5. If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL communicate with the verifier using approved cryptography.

6. If PSTN is not being used for out-of-band communication, then the key used to authenticate the out-of-band device SHALL be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, TEE, secure element).

7. If the PSTN is used for out-of-band authentication and a secret is sent to the out-of-band device via the PSTN, then the out-of-band authenticator SHALL uniquely authenticate itself to a mobile telephone network using a SIM card or equivalent that uniquely identifies the device.

8. If the out-of-band authenticator sends an approval message over the secondary communication channel, it SHALL either accept transfer of a secret from the primary channel to be sent to the verifier via the secondary communications channel, or present a secret received via the secondary channel from the verifier and prompt the claimant to verify the consistency of that secret with the primary channel, prior to accepting a yes/no response from the claimant which it sends to the verifier.

9. The verifier SHALL NOT store the identifying key itself, but SHALL use a verification method (e.g., an approved hash function or proof of possession of the identifying key) to uniquely identify the authenticator.

10. Depending on the type of out-of-band authenticator, one of the following SHALL take place: transfer of a secret to the primary channel, transfer of a secret to the secondary channel, or verification of secrets by the claimant.

11. If the out-of-band authenticator operates by transferring the secret to the primary channel, then the verifier SHALL transmit a random secret to

the out-of-band authenticator and then wait for the secret to be returned on the primary communication channel.

12. If the out-of-band authenticator operates by transferring the secret to the secondary channel, then the verifier SHALL display a random authentication secret to the claimant via the primary channel and then wait for the secret to be returned on the secondary channel from the claimant's out-of-band authenticator.

13. If the out-of-band authenticator operates by verification of secrets by the claimant, then the verifier SHALL display a random authentication secret to the claimant via the primary channel, send the same secret to the out-of-band authenticator via the secondary channel for presentation to the claimant, and then wait for an approval (or disapproval) message via the secondary channel.

14. The authentication SHALL be considered invalid if not completed within 10 minutes.

15. Verifiers SHALL accept a given authentication secret only once during the validity period.

16. The verifier SHALL generate random authentication secrets with at least 20 bits of entropy.

17. The verifier SHALL generate random authentication secrets using an approved random bit generator.

18. If the authentication secret has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 l (3) through (4).

19. If out-of-band verification is to be made using the PSTN, then the verifier SHALL verify that the pre-registered telephone number being used is associated with a specific physical device.

20. If out-of-band verification is to be made using the PSTN, then changing the pre-registered telephone number is considered to be the binding of a new authenticator and SHALL only occur as described in IA-5 n (17) through (25).

21. If PSTN is used for out-of-band authentication, then the CSP SHALL offer subscribers at least one alternate authenticator that is not RESTRICTED and can be used to authenticate at the required AAL.

22. If PSTN is used for out-of-band authentication, then the CSP SHALL Provide meaningful notice to subscribers regarding the security risks of the RESTRICTED authenticator and availability of alternative(s) that are not RESTRICTED.

23. If PSTN is used for out-of-band authentication, then the CSP SHALL address any additional risk to subscribers in its risk assessment.

24. If PSTN is used for out-of-band authentication, then the CSP SHALL develop a migration plan for the possibility that the RESTRICTED authenticator is no longer acceptable at some point in the future and include this migration plan in its digital identity acceptance statement.

d. OTP Authenticators and Verifiers

1. The secret key and its algorithm SHALL provide at least the minimum security strength of 112 bits as of the date of this publication.

2. The nonce SHALL be of sufficient length to ensure that it is unique for each operation of the device over its lifetime.

3. OTP authenticators — particularly software-based OTP generators — SHALL NOT facilitate the cloning of the secret key onto multiple devices.

4. The authenticator output SHALL have at least 6 decimal digits (approximately 20 bits) of entropy.

5. If the nonce used to generate the authenticator output is based on a real-time clock, then the nonce SHALL be changed at least once every 2 minutes.

6. The OTP value associated with a given nonce SHALL be accepted only once.

7. The symmetric keys used by authenticators are also present in the verifier and SHALL be strongly protected against compromise.

8. If a single-factor OTP authenticator is being associated with a subscriber account, then the verifier or associated CSP SHALL use approved cryptography to either generate and exchange or to obtain the secrets required to duplicate the authenticator output.

9. The verifier SHALL use approved encryption when collecting the OTP.

10. The verifier SHALL use an authenticated protected channel when collecting the OTP.

11. If a time-based OTP is used, it SHALL have a defined lifetime (recommended 30 seconds) that is determined by the expected clock drift — in either direction — of the authenticator over its lifetime, plus allowance for network delay and user entry of the OTP.

12. Verifiers SHALL accept a given time-based OTP only once during the validity period.

13. If the authenticator output has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 l (3) through (4).

14. If the authenticator is multi-factor, then each use of the authenticator SHALL require the input of the additional factor.

15. If the authenticator is multi-factor and a memorized secret is used by the authenticator for activation, then that memorized secret SHALL be a randomly chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of IA- 5 (1)(a).

16. If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in IA-5 l (3) through (4).

17. If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of IA-5 m, including limits on the number of consecutive authentication failures.

18. If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an OTP has been generated.

19. If the authenticator is multi-factor, the verifier or CSP SHALL establish, via the authenticator source, that the authenticator is a multi-factor device.

20. In the absence of a trusted statement that it is a multi-factor device, the verifier SHALL treat the authenticator as single-factor, in accordance with IA-5 (1) (d) (1) through (13).

e. Cryptographic Authenticators and Verifiers (including single- and multi-factor cryptographic authenticators, both hardware- and software-based)

1. If the cryptographic authenticator is software based, the key SHALL be stored in suitably secure storage available to the authenticator application.

2. If the cryptographic authenticator is software based, the key SHALL be strongly protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access.

3. If the cryptographic authenticator is software based, it SHALL NOT facilitate the cloning of the secret key onto multiple devices.

4. If the authenticator is single-factor and hardware-based, secret keys unique to the device SHALL NOT be exportable (i.e., cannot be removed from the device).

5. If the authenticator is hardware-based, the secret key and its algorithm SHALL provide at least the minimum-security length of 112 bits as of the date of this publication.

6. If the authenticator is hardware-based, the challenge nonce SHALL be at least 64 bits in length.

7. If the authenticator is hardware-based, approved cryptography SHALL be used.

8. Cryptographic keys stored by the verifier SHALL be protected against modification.

9. If symmetric keys are used, cryptographic keys stored by the verifier SHALL be protected against disclosure.

10. The challenge nonce SHALL be at least 64 bits in length.

11. The challenge nonce SHALL either be unique over the authenticator's lifetime or statistically unique (i.e., generated using an approved random bit generator).

12. The verification operation SHALL use approved cryptography.

13. If a multi-factor cryptographic software authenticator is being used, then each authentication requires the presentation of the activation factor.

14. If the authenticator is multi-factor, then any memorized secret used by the authenticator for activation SHALL be a randomly chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of IA-5 (1) (a).

15. If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in IA-5 l (3) through (4).

16. If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of IA-5 m, including limits on the number of consecutive authentication failures.

17. If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an authentication transaction has taken place. [Source: CJIS IA-05(01)]

Std.06 CJIS — Rescinded in V4.0.

Std.07 CJIS — Rescinded in V4.0.

Std.08 CJIS — Rescinded in V4.0.

TX-RAMP Correspondence

For systems subject to TX-RAMP Level 1 or Level 2 requirements, the following standard applies:

Std.09 TX-RAMP — Passwords must be case-sensitive and contain a minimum of twelve characters, including at least one upper-case letter, lower-case letter, number, and special character. [Source: TX-RAMP Manual IA-5(1)]

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Password-based authentication applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-05(01)(h). Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

Note that (c) and (d) require the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13.) [Source: FedRAMP Security Controls Baseline IA-5(1)]

For cases where technology doesn't allow multi-factor authentication, these rules should be enforced: must have a minimum length of 14 characters and must support all printable ASCII characters. [Source: FedRAMP Security Controls Baseline IA-5(1)]

TxDOT References

Identification and Authentication Standard; Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 180, 201, 202; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4; NIST IR 7539, 7817, 7849, 7870, 8040; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

IA-06

IA-05(02) Public Key-Based Authentication

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. For public key-based authentication:

1. Enforce authorized access to the corresponding private key; and

2. Map the authenticated identity to the account of the individual or group; and

b. When public key infrastructure (PKI) is used:

1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and

2. Implement a local cache of revocation data to support path discovery and validation.

Implementation Standards

Std.01 — Certificate use must comply with the TxDOT Identification and Authentication Standard.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IA-05(02).

Std.02 CJIS — Rescinded in V4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Public key cryptography is a valid authentication mechanism for individuals, machines, and devices. For PKI solutions, status information for certification paths includes certificate revocation lists or certificate status protocol responses. For PIV cards, certificate validation involves the construction and verification of a certification path to the Common Policy Root trust anchor, which includes certificate policy processing. Implementing a local cache of revocation data to support path discovery and validation also supports system availability in situations where organizations are unable to access revocation information via the network.

TxDOT Discussion

None.

TxDOT References

Identification and Authentication Standard; Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 180, 201, 202; NIST SP 800-63-3, 800-73-4, 800-76-2, 800-78-4; NIST IR 7539, 7817, 7849, 7870, 8040; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

IA-03, SC-17

IA-05(06) Protection of Authenticators

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

Implementation Standards

None.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.01 PCI —

a. Sensitive Authentication Data (SAD) is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process. [Source: PCI DSS 3.3.1]

b. SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography. [Source: PCI DSS 3.3.2]

Std.02 PCI — The full contents of any track are not retained upon completion of the authorization process. [Source: PCI DSS 3.3.1.1]

Std.03 PCI — The card verification code is not retained upon completion of the authorization process. [Source: PCI DSS 3.3.1.2]

Std.04 PCI — The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process. [Source: PCI DSS 3.3.1.3]

Std.05 PCI — Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used:

a. Factors are assigned to an individual user and not shared among multiple users.

b. Physical and/or logical controls ensure only the intended user can use that factor to gain access.

[Source: PCI DSS 8.3.11]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IA-05(06).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

For systems that contain multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the

highest security category of information on the systems. Security categories of information are determined as part of the security categorization process.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 180, 201, 202; SP 800-63-3, SP 800-73-4, SP 800-76-2, SP 800-78-4; IR 7539, IR 7817, IR 7849, IR 7870, IR 8040; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

RA-02

IA-05(07) No Embedded Unencrypted Static Authenticators

Baselines

N/A

Overlays

TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate or High baselines.

Discussion

In addition to applications, other forms of static storage include access scripts and function keys. Organizations exercise caution when determining whether embedded or stored authenticators are in encrypted or unencrypted form. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

In this context, prohibited static storage refers to any storage where unencrypted authenticators, such as passwords, persist beyond the time required to complete the access process. [Source: FedRAMP Security Controls Baseline IA-5(7)]

TxDOT References

Information Security and Privacy Policy

State References

TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

IA-05(08) Multiple System Accounts

Baselines

N/A

Overlays

FedRAMP High

Requirements

Implement different authenticators in different user authentication domains to manage the risk of compromise due to individuals having accounts on multiple systems.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

When individuals have accounts on multiple systems and use the same authenticators such as passwords, there is the risk that a compromise of one account may lead to the compromise of other accounts. Alternative approaches include having different authenticators (passwords) on all systems, employing a single sign-on or federation mechanism, or using some form of one-time passwords on all systems. Organizations can also use rules of behavior (see PL-04) and access agreements (see PS-06) to mitigate the risk of multiple system accounts.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

If a single user authentication domain is used to access multiple systems, such as in single-sign-on, then only a single authenticator is required. [Source: FedRAMP Security Controls Baseline IA-5(8)]

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

PS-06

IA-05(13) Expiration of Cached Authenticators

Baselines

N/A

Overlays

FedRAMP High

Requirements

Prohibit the use of cached authenticators after time periods defined in the Identification and Authentication Standard.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Cached authenticators are used to authenticate to the local machine when the network is not available. If cached authentication information is out of date, the validity of the authentication information may be questionable.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

For components subject to configuration baseline(s) (such as STIG or CIS,) the time period should conform to the baseline standard. [Source: FedRAMP Security Controls Baseline IA-5(13)]

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

IA-06 Authentication Feedback

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — All authenticators must be obscured in accordance with the TxDOT Identification and Authentication Standard.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IA-06.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Authentication feedback from systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems, such as desktops or notebooks with relatively large monitors, the threat (referred to as shoulder surfing) may be significant. For other types of systems, such as mobile devices with small displays, the threat may be less significant and is balanced against the increased likelihood of typographic input errors due to small keyboards. Thus, the means for obscuring authentication feedback is selected accordingly. Obscuring authentication feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before obscuring it.

TxDOT Discussion

None.

TxDOT References

Identification and Authentication Standard; Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-03

IA-07 Cryptographic Module Authentication

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Implement encryption algorithms in accordance with SC-13.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IA-07.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-03, IA-05, SA-04, SC-12, SC-13

IA-08 Identification and Authentication (Non-Organizational Users)

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Each system's identification and authentication mechanisms must comply with the TxDOT Identification and Authentication Standard.

Std.04 — Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification shall be authenticated before the information resources system may grant that user access. [Source: DIR Control Standards Catalog IA-8]

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.03 PCI — Ensure that the following is included in contracts or SLAs for service providers: Service providers with remote access to customer premises use unique authentication factors for each customer premises. [Source: PCI DSS 8.2.3]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IA-08.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Non-organizational users include system users other than organizational users explicitly covered by IA-02. Non-organizational users are uniquely identified and authenticated for accesses other than those explicitly identified and documented in AC-14. Identification and authentication of non-organizational users accessing federal systems may be required to

protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations consider many factors—including security, privacy, scalability, and practicality—when balancing the need to ensure ease of use for access to federal information and systems with the need to protect and adequately mitigate risk.

TxDOT Discussion

None.

TxDOT References

Identification and Authentication Standard; Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; Federal Public Key Infrastructure; FIPS 201; NIST SP 800-63-3, 800-79-2, 800-116; NIST IR 8062; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-02, AC-06, AC-14, AC-17, AC-18, AU-06, IA-02, IA-04, IA-05, IA-11, MA-04, RA-03, SA-04, SC-08

IA-08(01) Acceptance of PIV Credentials from Other Agencies

Baselines

N/A

Overlays

CJIS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.01 CJIS — Accept and electronically verify Personal Identity Verification-compliant credentials from other federal, state, local, tribal, or territorial (SLTT) agencies. [Source: CJIS IA-08(01)]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Acceptance of Personal Identity Verification (PIV) credentials from other federal agencies applies to both logical and physical access control systems. PIV credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidelines. The adequacy and reliability of PIV card issuers are addressed and authorized using SP 800-79-2.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

PE-03

IA-08(02) Acceptance of External Authenticators

Baselines

N/A

Overlays

CJIS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Accept only external authenticators that are NIST-compliant; and

b. Document and maintain a list of accepted external authenticators.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IA-08(02).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Acceptance of only NIST-compliant external authenticators applies to organizational systems that are accessible to the public (e.g., public-facing websites). External authenticators are issued by nonfederal government entities and are compliant with SP 800-63B. Approved external authenticators meet or exceed the minimum Federal Government-wide technical, security, privacy, and organizational maturity requirements.

Meeting or exceeding Federal requirements allows Federal Government relying parties to trust external authenticators in connection with an authentication transaction at a specified authenticator assurance level.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

IA-08(04) Use of Defined Profiles

Baselines

N/A

Overlays

CJIS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Conform to the following profiles for identity management identity management profiles as defined in the System Security Plan (SSP).

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, IA-08(04) is superseded by CJIS requirement IA-08(04):

Std.01 CJIS — Conform to the following profiles for identity management: Security Assertion Markup Language (SAML) or OpenID Connect. [Source: CJIS IA-08(04)]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Organizations define profiles for identity management based on open identity management standards. To ensure that open identity management standards are viable, robust, reliable, sustainable, and interoperable as documented, the Federal Government assesses and scopes the standards and technology implementations against applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

IA-11 Re-Authentication

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Require users to re-authenticate when circumstances or situations require re-authentication according to the TxDOT Identification and Authentication Standard.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.01 CJIS — Require users to re-authenticate when: roles, authenticators, or credentials change, security categories of systems change, the execution of privileged functions occur, or every 12 hours. [Source: CJIS IA-11]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

In addition to the re-authentication requirements associated with device locks, organizations may require re-authentication of individuals in certain situations, including when roles, authenticators or credentials change, when

security categories of systems change, when the execution of privileged functions occurs, after a fixed time period, or periodically.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

The fixed time period cannot exceed the limits set in SP 800-63. At this writing they are:

a. AAL3 (high baseline)

1. 12 hours, or

2. 15 minutes of inactivity

b. AAL2 (moderate baseline)

1. 12 hours, or

2. 30 minutes of inactivity

c. AAL1 (low baseline)

1. 30 days of extended session

2. No limit on inactivity.

[Source: FedRAMP Security Controls Baseline IA-11]

TxDOT References

Identification and Authentication Standard; Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-03, AC-11, IA-02, IA-03, IA-04, IA-08

IA-12 Identity Proofing

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;

b. Resolve user identities to a unique individual; and

c. Collect, validate, and verify identity evidence.

Implementation Standards

Std.01 — Ensure that evidence used for identity proofing complies with requirements as defined in the TxDOT Identification and Authentication Standard.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IA-12.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Identity proofing is the process of collecting, validating, and verifying a user's identity information for the purposes of establishing credentials for accessing a system. Identity proofing is intended to mitigate threats to the registration of users and the establishment of their accounts. Standards and

guidelines specifying identity assurance levels for identity proofing include SP 800-63-3 and SP 800-63A. Organizations may be subject to laws, executive orders, directives, regulations, or policies that address the collection of identity evidence. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

In accordance with NIST SP 800-63A Enrollment and Identity Proofing. [Source: FedRAMP Security Controls Baseline IA-12]

TxDOT References

Identification and Authentication Standard; Information Security and Privacy Policy

State References

None.

Federal References

FIPS 201; NIST SP 800-63-3, 800-63A, 800-79-2; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-05, IA-01, IA-02, IA-03, IA-04, IA-05, IA-06, IA-08

IA-12(02) Identity Evidence

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Require evidence of individual identification be presented to the registration authority.

Implementation Standards

Std.01 — Ensure that evidence meets requirements as defined in the TxDOT Identification and Authentication Standard.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IA-12(02).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Identity evidence, such as documentary evidence or a combination of documents and biometrics, reduces the likelihood of individuals using fraudulent identification to establish an identity or at least increases the work factor of potential adversaries. The forms of acceptable evidence are consistent with the risks to the systems, roles, and privileges associated with the user's account.

TxDOT Discussion

None.

TxDOT References

Identification and Authentication Standard; Information Security and Privacy Policy

State References

None.

Federal References

FIPS 201; NIST SP 800-63-3, 800-63A, 800-79-2; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

IA-12(03) Identity Evidence Validation and Verification

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Require that the presented identity evidence be validated and verified through methods of validation and verification in accordance with the assurance levels defined in the TxDOT Identification and Authentication Standard.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.01 CJIS —

a. Require that the presented identity evidence be validated and verified through agency-defined resolution, validation, and verification methods.

b. Identity proofing SHALL NOT be performed to determine suitability or entitlement to gain access to services or benefits.

c.

1. Collection of PII SHALL be limited to the minimum necessary to resolve to a unique identity in a given context.

2. Collection of PII SHALL be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the applicant providing identity evidence for appropriate identity resolution, validation, and verification.

d. The CSP SHALL provide explicit notice to the applicant at the time of collection regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory to complete the identity proofing process, and the consequences for not providing the attributes.

e. If CSPs process attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, or to comply with law or legal process, then CSPs SHALL implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the additional processing.

f. If the CSP employs consent as part of its measures to maintain predictability and manageability, …then it SHALL NOT make consent for the additional processing a condition of the identity service.

g. The CSP SHALL provide mechanisms for redress of applicant complaints or problems arising from the identity proofing.

These [redress] mechanisms SHALL be easy for applicants to find and use.

h. The CSP SHALL assess the [redress] mechanisms for their efficacy in achieving resolution of complaints or problems.

i. The identity proofing and enrollment processes SHALL be performed according to an applicable written policy or *practice statement* that specifies the particular steps taken to verify identities.

j. The *practice statement* SHALL include control information detailing how the CSP handles proofing errors that result in an applicant not being successfully enrolled.

k. The CSP SHALL maintain a record, including audit logs, of all steps taken to verify the identity of the applicant as long as the identity exists in the information system.

l. The CSP SHALL record the types of identity evidence presented in the proofing process.

m. The CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine:

1. Any steps that it will take to verify the identity of the applicant beyond any mandatory requirements specified herein;

2. The PII, including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing (Note: Specific federal requirements may apply); and

3. The schedule of retention for these records.

n. All PII collected as part of the enrollment process SHALL be protected to ensure confidentiality, integrity, and attribution of the information source.

o. The entire proofing transaction, including transactions that involve a third party, SHALL occur over authenticated protected channels.

p. If the CSP uses fraud mitigation measures, then the CSP SHALL conduct a privacy risk assessment for these mitigation measures.

Such assessments SHALL include any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography), and be documented per requirement IA-12(3) k – m above.

q. In the event a CSP ceases to conduct identity proofing and enrollment processes, then the CSP SHALL be responsible for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention.

r. Regardless of whether the CSP is a federal agency or non-federal entity, the following requirements apply to the federal agency offering or using the proofing service:

1. The agency SHALL consult with their Senior Agency Official for Privacy (SAOP) to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers Privacy Act requirements.

2. The agency SHALL publish a System of Records Notice (SORN) to cover such collection, as applicable.

3. The agency SHALL consult with their SAOP to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers E-Government Act of 2002 requirements.

4. The agency SHALL publish a Privacy Impact Assessment (PIA) to cover such collection, as applicable.

s. An enrollment code SHALL be comprised of one of the following:

1. Minimally, a random six character alphanumeric or equivalent entropy. For example, a code generated using an approved random number generator or a serial number for a physical hardware authenticator; OR

2. A machine-readable optical label, such as a QR Code, that contains data of similar or higher entropy as a random six character alphanumeric.

t. Training requirements for personnel validating evidence SHALL be based on the policies, guidelines, or requirements of the CSP or RP.

u. This criterion applies to CSPs that provide identity proofing and enrollment services to minors (under the age of 18):

If the CSP provides identity proofing and enrollment services to minors (under the age of 18), then…the CSP SHALL give special consideration to the legal restrictions of interacting with minors unable to meet the evidence requirements of identity proofing [to ensure compliance with the Children's Online Privacy Protection Act of 1998 (COPPA), and other laws, as applicable].

v. The CSP SHALL have the operator view the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process.

w. The CSP SHALL collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject. All biometric performance requirements in IA-5 m (1) through (12) apply.

x. The CSP SHALL support in-person or remote identity proofing, or both.

y. The CSP SHALL collect the following from the applicant:

1. One piece of SUPERIOR or STRONG evidence if the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence and the CSP validates the evidence directly with the issuing source; OR

2. Two pieces of STRONG evidence; OR

3. One piece of STRONG evidence plus two pieces of FAIR evidence

z. The CSP SHALL validate each piece of evidence with a process that can achieve the same strength as the evidence presented (see 'y' above). For

example, if two forms of STRONG identity evidence are presented, each piece of evidence will be validated at a strength of STRONG.

aa. The CSP SHALL verify identity evidence as follows: At a minimum, the applicant's binding to identity evidence must be verified by a process that is able to achieve a strength of STRONG.

bb. For IAL2 remote proofing: The collection of biometric characteristics for physical or biometric comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity performed remotely SHALL adhere to all requirements as specified in IA-5 m.

cc. Knowledge-based verification (KBV) SHALL NOT be used for in-person (physical or supervised remote) identity verification.

dd. The CSP SHALL employ appropriately tailored security controls, to include control enhancements, from the moderate or high baseline of security controls defined in the CJISSECPOL.

The CSP SHALL ensure that the minimum assurance-related controls for moderate-impact systems are satisfied.

ee. Supervised Remote Identity Proofing: Supervised remote identity proofing is intended to provide controls for comparable levels of confidence and security to in-person IAL3 identity proofing for identity proofing processes that are performed remotely. Supervised remote identity proofing is optional for CSPs; that is, if a CSP chooses to use supervised remote identity proofing, then the following requirements, (1) through (8), would apply. It should be noted that the term "supervised remote identity proofing" has specialized meaning and is used only to refer to the specialized equipment and the following control requirements, (1) through (8). In addition to those requirements presented in this document, as well as the applicable identity validation and verification requirements, CSPs that provide supervised remote identity proofing services must demonstrate conformance with the requirements contained in this section. The following requirements for supervised remote proofing apply specifically to IAL3. If the equipment/facilities used for supervised remote proofing are used for IAL2 identity proofing, the following requirements, (1) through (8), for supervised remote proofing do not apply. In this case, the requirements for conventional remote identity proofing are applicable.

1. Supervised remote identity proofing and enrollment transactions SHALL meet the following requirements, in addition to the IAL3 validation and verification requirements specified in IA-12(3)s.

2. The CSP SHALL monitor the entire identity proofing session, from which the applicant SHALL NOT depart — for example, by a continuous high-resolution video transmission of the applicant.

3. The CSP SHALL have a live operator participate remotely with the applicant for the entirety of the identity proofing session.

4. The CSP SHALL require all actions taken by the applicant during the identity proofing session to be clearly visible to the remote operator.

5. The CSP SHALL require that all digital validation of evidence (e.g., via chip or wireless technologies) be performed by integrated scanners and sensors.

6. The CSP SHALL require operators to have undergone a training program to detect potential fraud and to properly perform a supervised remote proofing session.

7. The CSP SHALL employ physical tamper detection and resistance features appropriate for the environment in which it is located.

8. The CSP SHALL ensure that all communications occur over a mutually authenticated protected channel.

ff. Trusted Referee: The use of trusted referees is optional for CSPs; that is, if a CSP chooses to use trusted referees for identity proofing and enrollment, then the following requirements, (1) through (3), would apply. The use of trusted referees is intended to assist in the identity proofing and enrollment for populations that are unable to meet IAL2 identity proofing requirements, or otherwise would be challenged to perform identity proofing and enrollment process requirements. Such populations may include, but are not limited to:

• Disabled individuals;

• Elderly individuals;

• Homeless individuals;

• Individuals with little or no access to online services or computing devices;

• Unbanked and individuals with little or no credit history;

• Victims of identity theft;

•Children under 18; and

• Immigrants.

In addition to those requirements presented in the General section of this document, as well as the applicable IAL requirements, CSPs that use trusted referees in their identity proofing services must demonstrate conformance with the requirements contained in this section.

1. If the CSP uses trusted referees, then…The CSP SHALL establish written policy and procedures as to how a trusted referee is determined and the lifecycle by which the trusted referee retains their status as a valid referee, to include any restrictions, as well as any revocation and suspension requirements.

2. If the CSP uses trusted referees, then…The CSP SHALL proof the trusted referee at the same IAL as the applicant proofing.

3. If the CSP uses trusted referees, then…The CSP SHALL determine the minimum evidence required to bind the relationship between the trusted referee and the applicant.

[Source: CJIS IA-12(03)]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Validation and verification of identity evidence increases the assurance that accounts and identifiers are being established for the correct user and authenticators are being bound to that user. Validation refers to the process of confirming that the evidence is genuine and authentic, and the data contained in the evidence is correct, current, and related to an individual. Verification confirms and establishes a linkage between the claimed identity and the actual existence of the user presenting the evidence. Acceptable methods for validating and verifying identity evidence are consistent with the risks to the systems, roles, and privileges associated with the user's account.

TxDOT Discussion

Note for systems subject to CJIS requirements:

CSPs may be subject to specific retention policies in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply.

[Source: CJIS IA-12(03)]

TxDOT References

Identification and Authentication Standard; Information Security and Privacy Policy

State References

None.

Federal References

FIPS 201; NIST SP 800-63-3, 800-63A, 800-79-2; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

IA-12(04) In-Person Validation and Verification

Baselines

N/A

Overlays

FedRAMP High

Requirements

Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

In-person proofing reduces the likelihood of fraudulent credentials being issued because it requires the physical presence of individuals, the presentation of physical identity documents, and actual face-to-face interactions with designated registration authorities.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

IA-12(05) Address Confirmation

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the user's address (physical or digital) of record.

Implementation Standards

Std.01 — Ensure that contact information used to send confirmation of registration is retrieved from a data source, not solicited from the user.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.02 CJIS —

a. Require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

b. The CSP SHALL confirm address of record.

c. Valid records to confirm address SHALL be issuing source(s) or authoritative source(s).

Self-asserted address data that has not been confirmed in records SHALL NOT be used for confirmation.

d. Note that IAL2-7 applies only to in-person proofing at IAL2.

If the CSP performs in-person proofing for IAL2 and provides an enrollment code directly to the subscriber for binding to an authenticator at a later time, then the enrollment code…SHALL be valid for a maximum of seven (7) days.

e. For remote identity proofing at IAL2: The CSP SHALL send an enrollment code to a confirmed address of record for the applicant.

f. For remote identity proofing at IAL2: The applicant SHALL present a valid enrollment code to complete the identity proofing process.

g. Note that the following enrollment code validity periods apply to enrollment codes sent to confirmed addresses of record for IAL2 remote in-person proofing only.

Enrollment codes shall have the following maximum validities:

1. 10 days, when sent to a postal address of record within the contiguous United States;

2. 30 days, when sent to a postal address of record outside the contiguous United States;

3. 10 minutes, when sent to a telephone of record (SMS or voice);

4. 24 hours, when sent to an email address of record.

h. If the enrollment code sent to the confirmed address of record as part of the remote identity proofing process at IAL2 is also intended to be an authentication factor, then…it SHALL be reset upon first use.

i. If the CSP performs remote proofing at IAL2 and optionally sends notification of proofing in addition to sending the required enrollment code, then…The CSP SHALL ensure the enrollment code and notification of proofing are sent to different addresses of record.

[Source: CJIS IA-12(05)]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate or High baselines.

Discussion

To make it more difficult for adversaries to pose as legitimate users during the identity proofing process, organizations can use out-of-band methods to ensure that the individual associated with an address of record is the same individual that participated in the registration. Confirmation can take the form of a temporary enrollment code or a notice of proofing. The delivery address for these artifacts is obtained from records and not self-asserted by the user. The address can include a physical or digital address. A home address is an example of a physical address. Email addresses and telephone numbers are examples of digital addresses.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

In accordance with NIST SP 800-63A Enrollment and Identity Proofing. [Source: FedRAMP Security Controls Baseline IA-12(5)]

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

FIPS 201; NIST SP 800-63-3, 800-63A, 800-79-2; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

IR — Incident Response

IR-01 Policy and Procedures

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level incident response policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;

b. Designate a senior management official as defined in the incident response policy to manage the development, documentation, and dissemination of the incident response policy and procedures; and

c. Review and update the current incident response:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — Moved to IR-08 Std.03 in V2.4.

Std.02 — The Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Review and update the current incident response policy and procedures following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. [Source: CJIS IR-01]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Incident response policy and procedures address the controls in the IR family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of incident response policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or

system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to incident response policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-12, 800-30, 800-39, 800-50, 800-61, 800-83, 800-100; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

PM-09, PS-08, SI-12

IR-02 Incident Response Training

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Provide incident response training to system users consistent with assigned roles and responsibilities:

1. Within 60 days of assuming an incident response role or responsibility or acquiring system access;

2. When required by system changes; and

3. Annually thereafter; and

b. Review and update incident response training content annually and following major changes to the environment of operation, including legislation and threats.

Implementation Standards

Std.01 — TxDOT shall train personnel in their incident response roles and responsibilities with respect to the information system and provide training at least annually. [Source: DIR Control Standards Catalog IR-2]

Std.02 — Include content on incident identification and reporting in awareness training for all employees and contractors in accordance with AT-02.

Std.03 — Provide role-based training to personnel assigned incident response roles in accordance with AT-03.

Std.04 — Formally track personnel participating in incident response training in accordance with AT-04.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.07 PCI — The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1; at a minimum, at least once a year and at the start of employment. [Source: PCI DSS 12.10.4.1; PCI DSS v4.x: Targeted Risk Analysis Guidance]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.08 CJIS — Provide incident response training to system users consistent with assigned roles and responsibilities prior to assuming an incident response role or responsibility or acquiring system access. [Source: CJIS IR-02]

TX-RAMP Correspondence

For systems subject to TX-RAMP Level 1 or Level 2 requirements, the following standard applies:

Std.05 TX-RAMP — Provide incident response training to system users consistent with assigned roles and responsibilities:

a. Within 14 days of assuming an incident response role or responsibility or acquiring system access;

b. When required by system changes; and

c. Annually thereafter. [Source: TX-RAMP Manual IR-2]

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.06 FedRAMP — Provide incident response training to system users consistent with assigned roles and responsibilities within ten (10) days for privileged users, and thirty (30) days for Incident Response roles, of assuming an incident response role or responsibility or acquiring system access. [Source: FedRAMP Security Controls Baseline IR-2]

Discussion

Incident response training is associated with the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail are included in such training. For example, users may only need to know who to call or how to recognize an incident; system administrators may require additional training on how to handle incidents; and incident responders may receive more specific training on forensics, data collection techniques, reporting, system recovery, and system restoration. Incident response training includes user training in identifying and reporting suspicious activities from external and internal sources. Incident response training for users may be provided as part of AT-02 or AT-03. Events that may precipitate an update to incident response training content include, but are not limited to, incident response plan testing or response to an actual incident (lessons learned), assessment or audit

findings, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB M-17-12; NIST SP 800-50; CJIS Security Policy; FedRAMP Security Controls Baseline; PCI DSS

Related Controls

AT-02, AT-03, AT-04, CP-03, IR-03, IR-04, IR-08

IR-02(01) Simulated Events

Baselines

High

Overlays

FedRAMP High

Requirements

Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.

Implementation Standards

Std.01 — Document results of training and update training plans and plans of action and milestones (POAMs) accordingly.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Organizations establish requirements for responding to incidents in incident response plans. Incorporating simulated events into incident response training helps to ensure that personnel understand their individual responsibilities and what specific actions to take in crisis situations.

TxDOT Discussion

Simulated events may include fake phishing campaigns targeted toward users; tabletop exercises for incident response staff; and off-site exercises as part of incident response testing.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB M-17-12; NIST SP 800-50; FedRAMP Security Controls Baseline

Related Controls

None.

IR-02(02) Automated Training Environments

Baselines

High

Overlays

FedRAMP High

Requirements

Provide an incident response training environment using automated mechanisms as identified in applicable System Security Plans (SSPs).

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Automated mechanisms can provide a more thorough and realistic incident response training environment. This can be accomplished, for example, by providing more complete coverage of incident response issues, selecting more realistic training scenarios and environments, and stressing the response capability.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB M-17-12; NIST SP 800-50

Related Controls

None.

IR-02(03) Breach

Baselines

N/A

Overlays

CJIS; PCI DSS; Privacy

Requirements

Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.

Implementation Standards

Std.01 — Ensure that awareness training includes breach awareness and reporting.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 12.10.4.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IR-02(03).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

For federal agencies, an incident that involves personally identifiable information is considered a breach. A breach results in the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or a similar occurrence where a person other than an authorized user accesses or

potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes. The incident response training emphasizes the obligation of individuals to report both confirmed and suspected breaches involving information in any medium or form, including paper, oral, and electronic. Incident response training includes tabletop exercises that simulate a breach. See IR-02(01).

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB M-17-12; NIST SP 800-50; PCI DSS; CJIS Security Policy

Related Controls

None.

IR-03 Incident Response Testing

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; Privacy; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Test the effectiveness of the incident response capability for the system at least annually using the following tests: approved tests as identified in the incident response plan.

Implementation Standards

Std.01 — The written incident response plan must include provisions for annual testing.

Std.02 — Incident response plans for all new systems must be tested prior to the system's being deployed to an operational state in the production environment.

Std.03 — Major deficiencies discovered as a result of testing must be addressed in accordance with CA-05.

Std.04 —

a. A formal test need not be conducted if the organization actively exercises its response capability during real incidents.

b. Any response capability not exercised during real incidents must be formally tested.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 12.10.2.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.07 CJIS — Test the effectiveness of the incident response capability for the system annually using the following tests: tabletop or walk-through exercises; simulations; or other agency-appropriate tests. [Source: CJIS IR-03]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate baseline, the following standard applies:

Std.05 FedRAMP — The service provider defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended). Functional testing must occur prior to testing for initial authorization. Annual functional testing may be concurrent with required penetration tests (see CA-8). The service provider provides test plans to the Joint Authorization Board (JAB)/Authorizing Official (AO) annually. Test plans are approved and accepted by the JAB/AO prior to test commencing. [Source: FedRAMP Security Controls Baseline IR-3]

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.06 FedRAMP — Test the effectiveness of the incident response capability for the system at least every six (6) months, including functional at least annually using the following tests: The service provider defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended). Functional testing must occur prior to testing for initial authorization. Annual functional testing may be concurrent with required penetration tests (see CA-8). The service provider provides test plans to the Joint Authorization Board (JAB)/Authorizing Official (AO) annually. Test plans are approved and accepted by the JAB/AO prior to test commencing. [Source: FedRAMP Security Controls Baseline IR-3]

Discussion

Organizations test incident response capabilities to determine their effectiveness and identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, and simulations (parallel or full interrupt). Incident response testing can include a determination of the effects on organizational operations and assets and individuals due to incident response. The use of qualitative and quantitative data aids in determining the effectiveness of incident response processes.

TxDOT Discussion

The organization maintains a list of incident response activities and mitigations for each user in accordance with the provisions of the organization incident response policy and procedures. Users need to be notified when their testing is scheduled and informed as to how it will be conducted. Several methods for testing and/or exercising continuity of operations plans exist for identifying potential weaknesses (e.g., full-scale business continuity plan testing, functional/tabletop exercises). Following the preparation of the various plans, a schedule needs to be developed to review and test each plan and ensure that each still meets the objectives. [Source: Catalog of Control Systems Security: Recommendations for Standards Developers 2.12.5 Continuity of Operations Plan Testing]

State Implementation Details

Testing includes, but is not limited to the use of checklists, walk-through or tabletop exercises, and simulations (parallel or full interrupt). Incident response testing can include a determination of the effects on organizational operations and assets and individuals due to incident response and the use

of qualitative and quantitative data aids in determining the effectiveness of incident response processes.

Incident response plans shall be exercised or tested at least annually. [Source: DIR Control Standards Catalog IR-3]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-84, 800-115; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CP-03, CP-04, IR-02, IR-04, IR-08, PM-14

IR-03(02) Coordination with Related Plans

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Coordinate incident response testing with organizational elements responsible for related plans.

Implementation Standards

Std.01 — Ensure that results of tests are shared with personnel responsible for related plans. Agency-wide full-scale simulations and exercises include personnel responsible for all applicable plans.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IR-03(02).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organizational plans related to incident response testing include business continuity plans, disaster recovery plans, continuity of operations plans, contingency plans, crisis communications plans, critical infrastructure plans, and occupant emergency plans.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-84, 800-115; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

IR-04 Incident Handling

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinate incident handling activities with contingency planning activities;

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and

d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Ensure that personnel investigating incidents are adequately trained and meet personnel security requirements appropriate to the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.

Std.03 — Maintain appropriate contacts with relevant authorities. Include key law enforcement contacts for reporting security incidents and external third parties authorized to take action against attack sources (for example, internet service providers), and designate a point of contact to review the list at least annually to keep it current. [Source: Hitrust 05.f Contact with Authorities]

Std.04 — Put mechanisms in place to monitor and quantify the types, volumes, and costs of information security incidents. Use the information gained from evaluation of information security incidents to identify recurring or high-impact incidents and update the incident response and recovery strategy. [Source: Hitrust 11.d Learning from Information Security Incidents]

Std.05 — Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented in support of potential

legal action in accordance with the rules for evidence in the relevant jurisdiction(s). [Source: Hitrust 11.e Collection of Evidence]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 12.10.6.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.06 PCI — Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents. [Source: PCI DSS 12.10.3]

Std.09 PCI — Incident response procedures are in place, to be initiated upon the detection of stored primary account number (PAN) anywhere it is not expected, and include:

a. Determining what to do if PAN is discovered outside the Cardholder Data Environment (CDE), including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable.

b. Identifying whether sensitive authentication data is stored with PAN.

c. Determining where the account data came from and how it ended up where it was not expected.

d. Remediating data leaks or process gaps that resulted in the account data being where it was not expected.

[Source: PCI DSS 12.10.7]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IR-04.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standards apply:

Std.07 FedRAMP — The FISMA definition of "incident" shall be used: "An occurrence that actually or imminently jeopardizes, without lawful authority,

the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." [Source: FedRAMP Security Controls Baseline IR-4]

Std.08 FedRAMP — The service provider ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system. [Source: FedRAMP Security Controls Baseline IR-4]

Discussion

Organizations recognize that incident response capabilities are dependent on the capabilities of organizational systems and the mission and business processes being supported by those systems. Organizations consider incident response as part of the definition, design, and development of mission and business processes and systems. Incident-related information can be obtained from a variety of sources, including audit monitoring, physical access monitoring, and network monitoring; user or administrator reports; and reported supply chain events. An effective incident handling capability includes coordination among many organizational entities (e.g., mission or business owners, system owners, authorizing officials, human resources offices, physical security offices, personnel security offices, legal departments, risk executive [function], operations personnel, procurement offices). Suspected security incidents include the receipt of suspicious email communications that can contain malicious code. Suspected supply chain incidents include the insertion of counterfeit hardware or malicious code into organizational systems or system components. For federal agencies, an incident that involves personally identifiable information is considered a breach. A breach results in unauthorized disclosure, the loss of control, unauthorized acquisition, compromise, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

Secure Technology Act; 41 CFR 201; OMB M-17-12; NIST SP 800-61, 800-86, 800-101, 800-150, 800-160-2, 800-184; NIST IR 7559; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-19, AU-06, AU-07, CM-06, CP-02, CP-03, CP-04, IR-02, IR-03, IR-05, IR-06, IR-08, PE-06, PL-02, PM-12, SA-08, SC-05, SC-07, SI-03, SI-04, SI-07

IR-04(01) Automated Incident Handling Processes

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Support the incident handling process using automated mechanisms as defined in the Incident Response Program.

Implementation Standards

Std.01 — Automated mechanisms support the exchange of incident handling information with TxDOT Information Security:

a. Information must be provided to TxDOT Information Security in a format compliant with TxDOT and, if applicable, federal requirements;

b. Incident handling information sources include systems, appliances, devices, services, and applications (including databases);

c. Incident handling information sources that do not support the exchange of information with TxDOT Information Security must be documented in the applicable risk assessment and System Security Plan (SSP); and

d. TxDOT Information Security-directed incident handling information collection rules/requests (for example, sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IR-04(01).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Automated mechanisms that support incident handling processes include online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

Secure Technology Act; 41 CFR 201; OMB M-17-12; NIST SP 800-61, 800-86, 800-101, 800-150, 800-160-2, 800-184; NIST IR 7559; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

None.

IR-04(02) Dynamic Reconfiguration

Baselines

N/A

Overlays

FedRAMP High

Requirements

Include the following types of dynamic reconfiguration for all network, data storage, and computing devices as part of the incident response capability: types of dynamic reconfiguration as defined in the Incident Response Plan (IRP).

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Dynamic reconfiguration includes changes to router rules, access control lists, intrusion detection or prevention system parameters, and filter rules for guards or firewalls. Organizations may perform dynamic reconfiguration of systems to stop attacks, misdirect attackers, and isolate components of systems, thus limiting the extent of the damage from breaches or compromises. Organizations include specific time frames for achieving the reconfiguration of systems in the definition of the reconfiguration capability, considering the potential need for rapid response to effectively address cyber threats.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

AC-02, AC-04, CM-02

IR-04(04) Information Correlation

Baselines

High

Overlays

FedRAMP High

Requirements

Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

Implementation Standards

Std.01 — Ensure that system-specific incident information is reported and correlated across business areas and across events.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Sometimes, a threat event, such as a hostile cyber-attack, can only be observed by bringing together information from different sources, including various reports and reporting procedures established by organizations.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

Secure Technology Act; 41 CFR 201; OMB M-17-12; NIST SP 800-61, 800-86, 800-101, 800-150, 800-160-2, 800-184; NIST IR 7559; FedRAMP Security Controls Baseline

Related Controls

None.

IR-04(06) Insider Threats

Baselines

N/A

Overlays

FedRAMP High

Requirements

Implement an incident handling capability for incidents involving insider threats.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Explicit focus on handling incidents involving insider threats provides additional emphasis on this type of threat and the need for specific incident handling capabilities to provide appropriate and timely responses.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

IR-04(11) Integrated Incident Response Team

Baselines

High

Overlays

FedRAMP High

Requirements

Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in a time period as defined in the incident response plan.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

An integrated incident response team is a team of experts that assesses, documents, and responds to incidents so that organizational systems and networks can recover quickly and implement the necessary controls to avoid future incidents. Incident response team personnel include forensic and malicious code analysts, tool developers, systems security and privacy engineers, and real-time operations personnel. The incident handling capability includes performing rapid forensic preservation of evidence and analysis of and response to intrusions. For some organizations, the incident response team can be a cross-organizational entity.

An integrated incident response team facilitates information sharing and allows organizational personnel (e.g., developers, implementers, and operators) to leverage team knowledge of the threat and implement defensive measures that enable organizations to deter intrusions more effectively. Moreover, integrated teams promote the rapid detection of intrusions, the development of appropriate mitigations, and the deployment of effective defensive measures. For example, when an intrusion is detected, the integrated team can rapidly develop an appropriate response for operators to implement, correlate the new incident with information on past intrusions, and augment ongoing cyber intelligence development. Integrated incident response teams are better able to identify adversary tactics, techniques, and procedures that are linked to the operations tempo or specific mission and business functions and to define responsive actions in a way that does not disrupt those mission and business functions. Incident response teams can be distributed within organizations to make the capability resilient.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

Secure Technology Act; 41 CFR 201; OMB M-17-12; NIST SP 800-61, 800-86, 800-101, 800-150, 800-160-2, 800-184; NIST IR 7559; FedRAMP Security Controls Baseline

Related Controls

AT-03

IR-05 Incident Monitoring

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Track and document incidents.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Monitor logs per CA-07. Log, report, investigate, and respond to all verified signs of incidents in accordance with the system-specific incident response plan.

Std.03 — Forward information system security and privacy incident and breach information:

a. In accordance with reporting requirements defined under the current TxDOT Incident Response Plan; and

b. Provide incident and breach information in a format compliant with TxDOT, state, and, if applicable, federal (for example, Continuous Diagnostics and Mitigation) requirements.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirements IR-05.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics as well as evaluating incident details, trends, and handling.

Incident information can be obtained from a variety of sources, including network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports. IR-04 provides information on the types of incidents that are appropriate for monitoring.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-61; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AU-06, AU-07, CA-07, IR-04, IR-06, IR-08, PE-06, PM-05, SC-05, SC-07, SI-03, SI-04, SI-07

IR-05(01) Automated Tracking, Data Collection, and Analysis

Baselines

High

Overlays

FedRAMP High

Requirements

Track incidents and collect and analyze incident information using automated mechanisms as defined in the Incident Response Program.

Implementation Standards

Std.01 — Monitor and quantify the types, volumes, and costs of information security incidents. [Source: Hitrust 11.d Learning from Information Security Incidents]

Std.02 — Ensure that incident records are restricted to only authorized personnel.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Automated mechanisms for tracking incidents and collecting and analyzing incident information include Computer Incident Response Centers or other electronic databases of incidents and network monitoring devices.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-61; FedRAMP Security Controls Baseline

Related Controls

None.

IR-06 Incident Reporting

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Require personnel to report suspected incidents to the organizational incident response capability within 15 minutes; and

b. Report incident information to appropriate individuals in accordance with the organization incident response policy and procedures.

Implementation Standards

Std.01 — Urgent Incident Report.

a. TxDOT shall assess the significance of a security incident based on the business impact on the affected resources and the current and potential technical effect of the incident (e.g., loss of revenue, productivity, access to services, reputation, unauthorized disclosure of confidential information, or propagation to other networks). Security incidents shall be promptly reported to immediate supervisors and the agency Information Security Officer. Confirmed or suspected security incidents shall be reported to the Department of Information Resources (DIR) within 48 hours of discovery in the form and manner specified by DIR where the security incident is assessed to:

(1) Propagate to other state systems;

(2) Result in criminal violations that shall be reported to law enforcement in accordance with state or federal information security or privacy laws;

(3) Involve the unauthorized disclosure or modification of confidential information, e.g., sensitive personal information as defined in Texas Business and Commerce Code Sec. 521.002(a)(2) and other applicable laws that may require public notification; or

(4) Be an unauthorized incident that compromises, destroys, or alters information systems, applications, or access to such systems or applications in any way. [Source: 1 TAC 202.3(d), (d)(1)]

Std.02 — If the security incident is assessed to involve suspected criminal activity (e.g., violations of Texas Penal Code Chapter 33 or Texas Penal Code Chapter 33A, TxDOT shall contact law enforcement, as required, and the security incident shall be investigated, reported, and documented in accordance with the legal requirements for handling of evidence. [Source: 1 TAC 202.3(d)(2)]

Std.03 — Summary reports of security-related events shall be sent to DIR on a monthly basis no later than nine calendar days after the end of the month. TxDOT shall submit summary security incident reports in the form and manner specified by DIR. Supporting vendors or other third parties that report security incident information to TxDOT shall submit such reports to TxDOT in the form and manner specified by DIR, unless otherwise directed by TxDOT. [Source: DIR Control Standards Catalog IR-6]

Std.04 — Security Incident Notification by State Agency or Local Government

a. In this section:

1. "Security incident" means:

(A) A breach or suspected breach of system security as defined by Section 521.053 (Notification Required Following Breach of Security of Computerized Data), Business & Commerce Code; and

(B) The introduction of ransomware, as defined by Section 33.023 (Electronic Data Tampering), Penal Code, into a computer, computer network, or computer system.

2. "Sensitive personal information" has the meaning assigned by Section 521.002 (Definitions), Business & Commerce Code.

b. A state agency or local government that owns, licenses, or maintains computerized data that includes sensitive personal information, confidential information, or information the disclosure of which is regulated by law shall, in the event of a security incident:

1. Comply with the notification requirements of Section 521.053 (Notification Required Following Breach of Security of Computerized Data), Business & Commerce Code, to the same extent as a person who conducts business in this state;

2. Not later than 48 hours after the discovery of the security incident, notify:

(A) The department, including the chief information security officer; or

(B) If the security incident involves election data, the secretary of state; and

3. Comply with all department rules relating to reporting security incidents as required by this section. [Source: TGC 2054.603(a)-(b)]

Std.05 — Ten days after the date of the eradication, closure, and recovery from a security incident, a state agency shall notify the department and the chief information security officer in the form and manner prescribed by the department of the security incident details and an analysis of the security incident cause. [Source: TAC 202.3(d)(4)]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IR-06.

Std.06 CJIS — Rescinded in V4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.07 FedRAMP —

a. Require personnel to report suspected incidents to the organizational incident response capability within US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended); and

b. Report incident information according to FedRAMP Incident Communications Procedure.

[Source: FedRAMP Security Controls Baseline IR-6]

Discussion

The types of incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Incident information can inform risk assessments, control effectiveness assessments, security requirements for acquisitions, and selection criteria for technology products.

TxDOT Discussion

State agencies are required to report security incidents (i.e. breaches or suspected breaches) to DIR in order to comply with TAC 202. TxDOT shall comply with DIR's reporting requirements presented in incident reporting applications or through supplemental guidance, including the types of incidents requiring urgent and routine incident reports, in accordance with 1 TAC 202.3(d) and TGC 2054.603(c). Where any conflict between these codes exists, TxDOT adheres to whichever is more restrictive.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; TGC 2054; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

Secure Technology Act; 41 CFR 201; US-CERT Federal Incident Notification Guidelines; NIST SP 800-61; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

CM-06, CP-02, IR-04, IR-05, IR-08

IR-06(01) Automated Reporting

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Report incidents using automated mechanisms as defined in the Incident Response Program.

Implementation Standards

Std.01 — Employ secure automated mechanisms to support the incident reporting process in accordance with the incident response plan.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IR-06(01).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

The recipients of incident reports are specified in IR-06b. Automated reporting mechanisms include email, posting on websites (with automatic updates), and automated incident response tools and programs.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

Secure Technology Act; 41 CFR 201; US-CERT Federal Incident Notification Guidelines; NIST SP 800-61; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

IR-07

IR-06(03) Supply Chain Coordination

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

Implementation Standards

Std.01 — Ensure that information is reviewed and approved for sending based on agreements with the suppliers. (Any escalation of or exception from this reporting should be clearly defined in the agreement.) Ensure that incident reporting data is adequately protected for transmission and received by approved individuals only. [Source: SP 800-161]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IR-06(03).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organizations involved in supply chain activities include product developers, system integrators, manufacturers, packagers, assemblers, distributors,

vendors, and resellers. Entities that provide supply chain governance include the Federal Acquisition Security Council (FASC). Supply chain incidents include compromises or breaches that involve information technology products, system components, development processes or personnel, distribution processes, or warehousing facilities. Organizations determine the appropriate information to share and consider the value gained from informing external organizations about supply chain incidents, including the ability to improve processes or to identify the root cause of an incident.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

Secure Technology Act; 41 CFR 201; US-CERT Federal Incident Notification Guidelines; NIST SP 800-61; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

SR-08

IR-07 Incident Response Assistance

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

Implementation Standards

Std.01 — Rescinded in V2.4.

Std.02 — Ensure basic awareness training (see AT-02) includes content on identification and reporting of potential incidents.

Std.03 — Provide monitored communication methods (for example, e-mail boxes) for reporting potential incidents.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IR-07.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Incident response support resources provided by organizations include help desks, assistance groups, automated ticketing systems to open and track incident response tickets, and access to forensics services or consumer redress services, when required.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST IR 7559; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AT-02, AT-03, IR-04, IR-06, IR-08, PM-22, PM-26, SA-09

IR-07(01) Automation Support for Availability of Information and Support

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Increase the availability of incident response information and support using automated mechanisms as identified in applicable System Security Plans (SSPs).

Implementation Standards

Std.01 — Provide automated mechanisms for tracking the status of potential incidents.

Std.02 — When incident response activities may affect users, where feasible provide near-real-time announcements including incident response-related information on websites, ticketing systems, or by e-mail.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — If the automated mechanisms include external assistance that will give unescorted physical or logical access to CJI, it is imperative to ensure that the appropriate controls/procedures (CJIS Security Addendum/Outsourcing Standard) are in place. Examples would include Cyber Incident Response Vendors (IT Security/Law Firms). [Source: CJIS IR-07(01)]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Automated mechanisms can provide a push or pull capability for users to obtain incident response assistance. For example, individuals may have access to a website to query the assistance capability, or the assistance capability can proactively send incident response information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; NIST IR 7559; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

IR-08 Incident Response Plan

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability;

2. Describes the structure and organization of the incident response capability;

3. Provides a high-level approach for how the incident response capability fits into the overall organization;

4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;

5. Defines reportable incidents;

6. Provides metrics for measuring the incident response capability within the organization;

7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;

8. Addresses the sharing of incident information;

9. Is reviewed and approved by the Chief Information Security Officer (CISO) (or equivalent) on an annual basis and when significant changes to the plan are made; and

10. Explicitly designates responsibility for incident response to entities, personnel, or roles as defined within the incident response policy.

b. Distribute copies of the incident response plan to entities, personnel, or roles as identified within the incident response policy;

c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;

d. Communicate incident response plan changes to entities, personnel, or roles as identified within the incident response policy; and

e. Protect the incident response plan from unauthorized disclosure and modification.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.03 — TxDOT shall assess the significance of a security incident based on the business impact on the affected resources and the current and potential technical effect of the incident, e.g., loss of revenue, productivity, access to services, reputation, unauthorized disclosure of confidential information, or propagation to other networks. [Source: DIR Control Standards Catalog IR-8]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 12.10.2.

Std.02 PCI — Rescinded in V3.0.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement IR-08.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at Low, Moderate, or High baselines, the following standard applies:

Std.04 FedRAMP —

a. The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements.

b. The incident response list includes designated FedRAMP personnel.

c. The incident response plan is distributed to the incident response list above, and changes to that plan are communicated to the individuals so listed.

[Source: FedRAMP Security Controls Baseline IR-8]

Discussion

It is important that organizations develop and implement a coordinated approach to incident response. Organizational mission and business functions determine the structure of incident response capabilities. As part of

the incident response capabilities, organizations consider the coordination and sharing of information with external organizations, including external service providers and other organizations involved in the supply chain. For incidents involving personally identifiable information (i.e., breaches), include a process to determine whether notice to oversight organizations or affected individuals is appropriate and provide that notice accordingly.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130, M-17-12; NIST SP 800-61; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-02, CP-02, CP-04, IR-04, IR-07, PE-06, PL-02, SA-15, SI-12, SR-08

IR-08(01) Breaches

Baselines

N/A

Overlays

CJIS; PCI DSS; Privacy

Requirements

Include the following in the Incident Response Plan for breaches involving personally identifiable information:

a. A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;

b. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and

c. Identification of applicable privacy requirements.

Implementation Standards

Std.01 —

a. Where TxDOT computerized data includes sensitive personal information (SPI), TxDOT shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system. [Source: TBC 521.053(b)]

b. Where TxDOT computerized data includes sensitive personal information (SPI), TxDOT shall notify the attorney general of that breach not later than the 60th day after the date on which the person determines that the breach occurred if the breach involves at least 250 residents of this state. The notification under this subsection must include:

1. A detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach;

2. The number of residents of this state affected by the breach at the time of notification;

3. The number of affected residents that have been sent a disclosure of the breach by mail or other direct method of communication at the time of notification

4. The measures taken by the person regarding the breach;

5. Any measures the person intends to take regarding the breach after the notification under this subsection; and

6. Information regarding whether law enforcement is engaged in investigating the breach. [Source: TBC 521.053(i)]

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.02 PCI — An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to:

a. Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum.

b. Incident response procedures with specific containment and mitigation activities for different types of incidents.

c. Business recovery and continuity procedures.

d. Data backup processes.

e. Analysis of legal requirements for reporting compromises.

f. Coverage and responses of all critical system components.

g. Reference or inclusion of incident response procedures from the payment brands.

[Source: PCI DSS 12.10.1]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirements IR-08(01).

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. [Source: CJIS 5.20.5]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Organizations may be required by law, regulation, or policy to follow specific procedures relating to breaches, including notice to individuals, affected organizations, and oversight bodies; standards of harm; and mitigation or other specific requirements.

TxDOT Discussion

Note for systems subject to CJIS requirements:

Special reporting procedures for mobile devices shall apply in any of the following situations:

a. Loss of device control. For example:

1. Device known to be locked, minimal duration of loss;

2. Device lock state unknown, minimal duration of loss;

3. Device lock state unknown, extended duration of loss; or

4. Device known to be unlocked, more than momentary duration of loss.

b. Total loss of device;

c. Device compromise; or

d. Device loss or compromise outside the United States. [Source: CJIS 5.20.5]

TxDOT References

Information Security and Privacy Policy

State References

TBC 521; DIR Security Control Standards Catalog

Federal References

OMB A-130, M-17-12; NIST SP 800-61; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

PT-01, PT-02, PT-03, PT-04, PT-05, PT-07

IR-09 Information Spillage Response

Baselines

Low, Moderate, High

Overlays

TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Respond to information spills by:

a. Assigning personnel or roles as defined in the Incident Response Plan with responsibility for responding to information spills;

b. Identifying the specific information involved in the system contamination;

c. Alerting personnel or roles as defined in the Incident Response Plan of the information spill using a method of communication not associated with the spill;

d. Isolating the contaminated system or system component;

e. Eradicating the information from the contaminated system or component;

f. Identifying other systems or system components that may have been subsequently contaminated; and

g. Performing the following additional actions: actions as defined in the Incident Response Plan.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Information spillage refers to instances where information is placed on systems that are not authorized to process such information. Information spills occur when information that is thought to be a certain classification or impact level is transmitted to a system and subsequently is determined to be of a higher classification or impact level. At that point, corrective action is required. The nature of the response is based on the classification or impact level of the spilled information, the security capabilities of the system, the specific nature of the contaminated storage media, and the access authorizations of individuals with authorized access to the contaminated system. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline

Related Controls

CP-02, IR-06, PM-26, PM-27, PT-02, PT-03, PT-07, RA-07

IR-09(02) Training

Baselines

N/A

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

Provide information spillage response training at least annually.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organizations establish requirements for responding to information spillage incidents in incident response plans. Incident response training on a regular basis helps to ensure that organizational personnel understand their individual responsibilities and what specific actions to take when spillage incidents occur.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

AT-02, AT-03, CP-03, IR-02

IR-09(03) Post-spill Operations

Baselines

N/A

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

Implement the following procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions: procedures as defined in the Incident Response Plan (IRP).

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Corrective actions for systems contaminated due to information spillages may be time-consuming. Personnel may not have access to the contaminated systems while corrective actions are being taken, which may potentially affect their ability to conduct organizational business.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

IR-09(04) Exposure to Unauthorized Personnel

Baselines

N/A

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

Employ the following controls for personnel exposed to information not within assigned access authorizations: controls as defined in the Incident Response Plan (IRP).

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Controls include ensuring that personnel who are exposed to spilled information are made aware of the laws, executive orders, directives, regulations, policies, standards, and guidelines regarding the information and the restrictions imposed based on exposure to such information.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

MA — Maintenance

MA-01 Policy and Procedures

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level maintenance policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;

b. Designate a senior management official as defined in the maintenance policy to manage the development, documentation, and dissemination of the maintenance policy and procedures; and

c. Review and update the current maintenance:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Review and update the current maintenance policy and procedures following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. [Source: CJIS MA-01]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Maintenance policy and procedures address the controls in the MA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of maintenance policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or

system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to maintenance policy and procedures assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-12, 800-30, 800-39, 800-100; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

PM-09, PS-08, SI-12

MA-02 Controlled Maintenance

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;

c. Require that system owners or other authorized personnel as identified in the System Security Plan (SSP) explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;

d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: all TxDOT data;

e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and

f. Include the following information in organizational maintenance records: maintenance-related information as defined in Std.02.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Records of maintenance activity must be maintained in organization maintenance records or system maintenance logs and must include:

a. Date and time of maintenance;

b. Name(s) of individual(s) performing maintenance;

c. Name of escort, if necessary;

d. Description of maintenance performed; and

e. List of equipment removed or replaced, including identification numbers if applicable.

Std.03 — Where feasible, employ automated mechanisms to schedule and conduct maintenance as required, and to create current, correct, and

complete records of all maintenance actions whether needed, scheduled, in process, or performed.

Std.04 — Following maintenance or repair, check to ensure maintenance ports have been disabled and security features re-enabled.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.05 CJIS — Include the following information in organizational maintenance records: Component serial number. [Source: CJIS MA-02]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Controlling system maintenance addresses the information security aspects of the system maintenance program and applies to all types of maintenance to system components conducted by local or nonlocal entities. Maintenance includes peripherals such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes the date and time of maintenance, a description of the maintenance performed, names of the individuals or group performing the maintenance, name of the escort, and system components or equipment that are removed or replaced. Organizations consider supply chain-related risks associated with replacement components for systems.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST IR 8023; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CM-02, CM-03, CM-04, CM-05, CM-08, MA-04, MP-06, PE-16, SI-02, SR-03, SR-04, SR-11

MA-02(02) Automated Maintenance Activities

Baselines

High

Overlays

FedRAMP High

Requirements

a. Schedule, conduct, and document maintenance, repair, and replacement actions for the system using automated mechanisms as identified in applicable System Security Plans (SSPs); and

b. Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

The use of automated mechanisms to manage and control system maintenance programs and activities helps to ensure the generation of timely, accurate, complete, and consistent maintenance records.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; NIST IR 8023; FedRAMP Security Controls Baseline

Related Controls

MA-03

MA-03 Maintenance Tools

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Approve, control, and monitor the use of system maintenance tools; and

b. Review previously approved system maintenance tools at least annually as part of the review of the System Security Plan (SSP).

Implementation Standards

Std.01 —

a. Document approved maintenance tools in System Security Plans.

b. For each approved tool, list any system maintenance ports, services, and protocols that must be disabled according to configuration standards but are required by the tool.

Std.02 — Ensure that maintenance tools are included in maintenance schedules (see MA-02).

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.03 CJIS — Review previously approved system maintenance tools prior to each use. [Source: CJIS MA-03]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Approving, controlling, monitoring, and reviewing maintenance tools address security-related issues associated with maintenance tools that are not within system authorization boundaries and are used specifically for diagnostic and repair actions on organizational systems. Organizations have flexibility in determining roles for the approval of maintenance tools and how that approval is documented. A periodic review of maintenance tools facilitates the withdrawal of approval for outdated, unsupported, irrelevant, or no-longer-used tools. Maintenance tools can include hardware, software, and firmware items and may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website. Such tools can be vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into systems. Maintenance

tools can include hardware and software diagnostic test equipment and packet sniffers. The hardware and software components that support maintenance and are a part of the system (including the software implementing utilities such as "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not addressed by maintenance tools.

TxDOT Discussion

If, during an emergency maintenance situation, no approved tool is available, system owners can approve tools in writing for emergency use, and the tool can then be used. The tool must be removed from the system following emergency use, as approval should not be extended beyond the immediate emergency, but the tool's performance in the emergency may be considered when evaluating the tool for possible approval.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-88; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

MA-02, PE-16

MA-03(01) Inspect Tools

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement MA-03(01).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Maintenance tools can be directly brought into a facility by maintenance personnel or downloaded from a vendor's website. If, upon inspection of the maintenance tools, organizations determine that the tools have been modified in an improper manner or the tools contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-88; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

SI-07

MA-03(02) Inspect Media

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Check media containing diagnostic and test programs for malicious code before the media are used in the system.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement MA-03(02).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

If, upon inspection of media containing maintenance, diagnostic, and test programs, organizations determine that the media contains malicious code, the incident is handled consistent with organizational incident handling policies and procedures.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-88; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

SI-03

MA-03(03) Prevent Unauthorized Removal

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Prevent the removal of maintenance equipment containing organizational information by:

a. Verifying that there is no organizational information contained on the equipment;

b. Sanitizing or destroying the equipment;

c. Retaining the equipment within the facility; or

d. Obtaining an exemption from personnel or roles as identified in the System Security Plan (SSP) explicitly authorizing removal of the equipment from the facility.

Implementation Standards

Std.01 — Ensure all maintenance equipment with the capability of retaining information is sanitized as required by MP-06 before removal from organization-controlled facilities; or, if sanitization is not feasible, retain or destroy the equipment unless authorized to release.

Std.02 — Explicitly authorize, track, and audit any removal of maintenance tools. [Source: SP 800-161]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement MA-03(03).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organizational information includes all information owned by organizations and any information provided to organizations for which the organizations serve as information stewards.

TxDOT Discussion

Once tools are allowed access to an organization/information system, they should remain the property/asset of the information system owner and tracked if removed and used elsewhere in the organization. Maintenance tools either currently in use or in storage should not be allowed to leave the organization’s premises until they are properly vetted for removal. [Source: SP 800-161]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-88; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

MP-06

MA-04 Nonlocal Maintenance

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Approve and monitor nonlocal maintenance and diagnostic activities;

b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;

c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;

d. Maintain records for nonlocal maintenance and diagnostic activities; and

e. Terminate session and network connections when nonlocal maintenance is completed.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — When maintenance is to be conducted by a third party, personnel with appropriate authorizations and technical competence, as identified in the System Security Plan (SSP), shall:

a. Set up the required connection features;

b. Provide assistance to the third party as required during the session;

c. Monitor the process in real-time;

d. Verify the completion of the maintenance;

e. Verify that all temporarily enabled ports, services, accesses, protocols, and permissions are disabled; and

f. Verify the session termination.

Std.03 — Password-based authentication is permissible for use during remote maintenance only if passwords are changed following each remote maintenance service.

Std.04 — Media used during remote maintenance must be sanitized in accordance with SP 800-88.

Std.05 — Review records in accordance with AU-06.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement MA-04.

Std.06 CJIS — Rescinded in V4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Nonlocal maintenance and diagnostic activities are conducted by individuals who communicate through either an external or internal network. Local maintenance and diagnostic activities are carried out by individuals who are physically present at the system location and not communicating across a network connection. Authentication techniques used to establish nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-02. Strong authentication requires authenticators that are resistant to replay attacks and employ multi-factor authentication. Strong authenticators include PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-04 is accomplished, in part, by other controls. SP 800-63B provides additional guidance on strong authentication and authenticators.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 197, 201; NIST SP 800-63-3, 800-88; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-02, AC-03, AC-06, AC-17, AU-02, AU-03, AU-06, IA-02, IA-04, IA-05, IA-08, MA-02, MA-05, PL-02, SC-07, SC-10

MA-04(03) Comparable Security and Sanitization

Baselines

High

Overlays

FedRAMP High

Requirements

a. Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or

b. Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.

Implementation Standards

Std.01 — Ensure that contracts and statements of work (SOWs) include requirements for security controls.

Std.02 — Sanitize components in accordance with MP-06(03).

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Comparable security capability on systems, diagnostic tools, and equipment providing maintenance services implies that the implemented controls on those systems, tools, and equipment are at least as comprehensive as the controls on the system being serviced.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FIPS 140, 197, 201; NIST SP 800-63-3, 800-88; FedRAMP Security Controls Baseline

Related Controls

MP-06, SI-03, SI-07

MA-05 Maintenance Personnel

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and

c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Before allowing third-party maintenance personnel access to systems, verify that those personnel:

a. Have been validated to meet personnel requirements in accordance with PS-07;

b. Individually sign a confidentiality agreement or non-disclosure agreement (NDA);

c. Provide valid identification;

d. Are authorized to perform work on the specific system(s); and

e. Are expected, whether or not an escort is required.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement MA-05.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Maintenance personnel refers to individuals who perform hardware or software maintenance on organizational systems, while PE-02 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems. Technical competence of supervising individuals relates to the maintenance performed on the systems, while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel—such as information technology manufacturers, vendors, systems integrators, and consultants—may require privileged access to organizational systems, such as when they are required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.

TxDOT Discussion

Equipment is maintained in accordance with the supplier's recommended service intervals and specifications. Only authorized maintenance personnel should carry out repairs and service equipment. Appropriate controls should be implemented when equipment is scheduled for maintenance (e.g., authorization levels) taking into account whether this maintenance is performed by personnel on site or external to the organization. [Source: Hitrust CSF 08.j Equipment Maintenance]

Third-party maintenance providers under contract to perform maintenance/support services on information systems should provide a list of field service engineers assigned to support maintenance with the following information for each service representative:

1. Name;

2. Company represented;

3. Title;

4. Contact Info (phone number, e-mail);

5. Photo for identification purposes;

6. List of systems on which the individual is authorized to perform maintenance; and

7. List of maintenance tools the individual is authorized to use.

Maintenance tasks performed using a user's identification and authentication credentials should be performed only when the user is present. The user should log in and observe the maintenance actions at all times. Maintenance personnel shall not ask for, and users shall not share, individual authentication information (see PL-04).

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-02, AC-03, AC-05, AC-06, IA-02, IA-08, MA-04, MP-02, PE-02, PE-03, PS-07, RA-03

MA-05(01) Individuals Without Appropriate Access

Baselines

High

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

a. Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:

1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by

approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and

2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

b. Develop and implement alternate controls as specified in the System Security Plan (SSP) in the event a system component cannot be sanitized, removed, or disconnected from the system.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Procedures for individuals who lack appropriate security clearances or who are not U.S. citizens are intended to deny visual and electronic access to classified or controlled unclassified information contained on organizational systems. Procedures for the use of maintenance personnel can be documented in security plans for the systems.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FedRAMP Security Controls Baseline

Related Controls

MP-06, PL-02

MA-06 Timely Maintenance

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Obtain maintenance support and/or spare parts for system components as defined in contingency plans within time periods defined in contingency plans of failure.

Implementation Standards

Std.01 — For information systems and system components not identified in contingency plans (including systems not hosted on the infrastructure platform), obtain support or replacement according to procurement guidelines.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.03 CJIS — Obtain maintenance support and/or spare parts for critical system components that process, store, and transmit CJI within agency-defined recovery time and recovery point objectives of failure. [Source: CJIS MA-06]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.02 FedRAMP — Obtain maintenance support and/or spare parts for system components as defined in contingency plans within a timeframe to support advertised uptime and availability of failure. [Source: FedRAMP Security Controls Baseline MA-6]

Discussion

Organizations specify the system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support include having appropriate contracts in place.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CM-08, CP-02, CP-07, RA-07, SA-15, SR-02, SR-03, SR-04

MP — Media Protection

MP-01 Policy and Procedures

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level media protection policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;

b. Designate a senior management official as defined in the media protection policy to manage the development, documentation, and dissemination of the media protection policy and procedures; and

c. Review and update the current media protection:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 3.1.1 and 3.1.2.

Std.03 PCI — Rescinded in V3.0.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.04 CJIS — Review and update the current media protection policy and procedures following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. [Source: CJIS MP-01]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Media protection policy and procedures address the controls in the MP family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs

collaborate on the development of media protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to media protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-12, 800-30, 800-39, 800-100; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

MP-02, PM-09, PS-08, SI-12

MP-02 Media Access

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Restrict access to system media, whether digital or non-digital, that contains Sensitive, Confidential or Regulated data to only those personnel the Information Owner has determined need to access the data.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The Information Owner or their designated representative(s) are responsible for approving access to information resources and periodically reviewing access lists based on documented risk management decisions. [Source: 1 TAC 202.22(a)(1)(B)]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 9.4.4.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement MP-02.

Std.03 CJIS — Rescinded in V3.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers is an example of restricting access to non-digital media. Limiting access to the design

specifications stored on compact discs in the media library to individuals on the system development team is an example of restricting access to digital media.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; FIPS 199; NIST SP 800-111; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-19, AU-09, CP-02, CP-09, CP-10, MA-05, MP-01, MP-04, MP-06, PE-02, PE-03, SC-12, SC-13, SI-12

MP-03 Media Marking

Baselines

Moderate, High

Overlays

PCI DSS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

b. Exempt digital and non-digital media classified as Public from marking if the media remain within TxDOT-owned or managed facilities.

Implementation Standards

Std.01 — Classify all TxDOT data as specified in PM-05(01).

Std.02 — Mark all media that contains information that is not Public. [Source: DIR Data Classification Template]

Std.03 — All media marking must follow TxDOT media protection policy and procedures.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 9.4.2.

CJIS Correspondence

None.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.04 FedRAMP — Exempt no removable media types from marking. [Source: FedRAMP Security Controls Baseline MP-3]

Discussion

Security marking refers to the application or use of human-readable security attributes. Digital media includes diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), flash drives, compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Controlled unclassified information is defined by the National Archives and Records Administration along with the appropriate safeguarding and dissemination requirements for such information and is codified in 32 CFR 2002. Security markings are generally not required for media that contains information determined by organizations to be in the public domain or to be publicly releasable. Some organizations may require markings for public information indicating that the information is publicly releasable. System media marking reflects applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

32 CFR 2002; EO 13556; FIPS 199; PCI DSS; FedRAMP Security Controls Baseline

Related Controls

CP-09, MP-05, SI-12

MP-04 Media Storage

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Physically control and securely store system media, whether digital or non-digital, that contains Sensitive, Confidential, or Regulated data within areas where access is not restricted only to personnel authorized to access the media; and

b. Protect system media types defined in MP-04a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Implementation Standards

Std.01 — All TxDOT media storage must comply with MP-07.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 9.4.1.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement MP-04.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.02 FedRAMP — The service provider defines controlled areas within facilities where the information and information system reside. [Source: FedRAMP Security Controls Baseline MP-4]

Discussion

System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Physically controlling stored media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the library, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet or a controlled media library. The type of media storage is commensurate with the security category or classification of the information on the media. Controlled areas are spaces that provide physical and procedural controls to meet the requirements established for protecting information and systems. Fewer controls may be needed for media that contains information determined to be in the public domain, publicly releasable, or have limited adverse impacts on organizations, operations, or individuals if accessed by other than authorized personnel. In these situations, physical access controls provide adequate protection.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 199; NIST SP 800-56A, 800-56B, 800-56C, 800-57-1, 800-57-2, 800-57-3, 800-111; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-19, CP-02, CP-06, CP-09, CP-10, MP-02, MP-07, PE-03, PL-02, SC-12, SC-13, SC-28, SI-12

MP-05 Media Transport

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Protect and control digital and non-digital media containing TxDOT Sensitive, Confidential, or Regulated data during transport outside of controlled areas using methods outlined in Stds.02 & 03;

b. Maintain accountability for system media during transport outside of controlled areas;

c. Document activities associated with the transport of system media; and

d. Restrict the activities associated with the transport of system media to authorized personnel.

Implementation Standards

Std.01 — Permit only authorized personnel to perform activities associated with transport of media, and maintain records to document pickup, receipt, transfer, and delivery.

Std.02 — Media Security in Transport

a. For digital media, use encryption in accordance with SC-08 and SC-13 to secure the data while in transport.

b. Use tamper-evident packaging to secure the data while in transport.

Std.03 — Transport Method Requirements

a. If hand carried, use a securable container transported by authorized personnel.

b. If shipped, utilize a trackable receipt by a commercial carrier and require a signature for delivery.

Std.04 — All TxDOT media being transported must comply with MP-03 and MP-07.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 9.4.3.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement MP-05.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.05 FedRAMP — The service provider defines security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the Joint Authorization Board (JAB)/Authorizing Official (AO). [Source: FedRAMP Security Controls Baseline MP-5]

Discussion

System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state and magnetic), compact discs, and digital versatile discs. Non-digital media includes microfilm and paper. Controlled areas are spaces for which organizations provide physical or procedural controls to meet requirements established for protecting information and systems. Controls to protect media during transport include cryptography and locked containers. Cryptographic mechanisms can provide confidentiality and integrity protections depending on the mechanisms implemented. Activities associated with media transport include releasing media for transport, ensuring that media enters the appropriate transport processes, and the actual transport. Authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and/or obtaining records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of system media in

accordance with organizational assessments of risk. Organizations maintain the flexibility to define record-keeping methods for the different types of media transport as part of a system of transport-related records.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 199; NIST SP 800-60-1, 800-60-2; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-07, AC-19, CP-02, CP-09, MP-03, MP-04, PE-16, PL-02, SC-12, SC-13, SC-28

MP-06 Media Sanitization

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Sanitize all digital or non-digital systems or storage media that contains TxDOT data prior to disposal, release out of organizational control, or release for reuse using sanitization techniques outlined in Stds.01-10; and

b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Implementation Standards

Std.01 — Rescinded in V2.4.

Std.02 — Electronic state records shall be destroyed in accordance with Texas Government Code Sec. 441.185 and in compliance with TxDOT's records retention schedule. If the record retention period applicable for an electronic state record has not expired at the time the record is removed from data process equipment, TxDOT shall retain a hard copy or other electronic copy of the record for the required retention period.

Std.03 — Moved to TxDOT Discussion in V2.4.

Std.04 — TxDOT shall keep a record documenting the removal and completion of sanitization of media that stored confidential information with the following information:

a. Date;

b. Description of the item(s) and serial number(s);

c. Inventory number(s);

d. The process and sanitization tools used to remove the data or method of destruction; and

e. The name and address of the organization the equipment was transferred to.

[Source: DIR Controls Standard Catalog MP-6(1)]

Std.05 — A state record may not be destroyed if any litigation, claim, negotiation, audit, open records request, administrative review, or other action involving the record is initiated before the expiration of a retention period for the record set by the commission or in the approved records retention schedule of the agency until the completion of the action and the resolution of all issues that arise from the action, or until the expiration of the retention period, whichever is later. [Source: TGC 441.187(b)]

Std.06 — Ensure that an electronic state record scheduled for disposition is disposed of in a manner that ensures protection of confidential information. [Source: 13 TAC 6.97(b)]

Std.07 — Establish and implement procedures that address the disposition of electronic state records by staff in accordance with its certified records retention schedule as well as secure destruction requirements from the Department of Information Resources, including identifying and disposing of transitory information. [Source: 13 TAC 6.97(c)]

Std.08 — A state agency shall permanently remove data from data processing equipment before disposing of or otherwise transferring the equipment to a person who is not a state agency or other agent of the state. This section applies only to equipment that will not be owned by the state after the disposal or other transfer. [Source: TGC 2054.130(a)]

Std.09 — Sanitize equipment, including removing all labels, markings, and activity logs, degaussing, overwriting, or destroying media, in accordance with the guidance in SP 800-88.

Std.10 — Test sanitization equipment and procedures at least annually to ensure correct performance.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.11 PCI — Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following:

a. Coverage for all locations of stored account data.

b. Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization.

c. Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements.

d. Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification.

e. Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy.

f. A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.

[Source: PCI DSS 3.2.1]

Std.12 PCI —

a. Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows:

1. Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.

2. Materials are stored in secure storage containers prior to destruction.

[Source: PCI DSS 9.4.6]

b. Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following:

1. The electronic media is destroyed.

2. The cardholder data is rendered unrecoverable so that it cannot be reconstructed.

[Source: PCI DSS 9.4.7]

CJIS Correspondence

For systems processing CJIS data, MP-06a is superseded by CJIS requirement MP-06:

Std.13 CJIS — Sanitize or destroy digital and non-digital media prior to disposal, release out of agency control, or release for reuse using overwrite technology at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media will be destroyed (cut up, shredded, etc.). Physical media will be securely disposed of when no longer needed for investigative or security purposes, whichever is later. Physical media will be destroyed by crosscut shredding or incineration. [Source: CJIS MP-06]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Media sanitization applies to all digital and non-digital system media subject to disposal or reuse, whether or not the media is considered removable. Examples include digital media in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices, and non-digital media (e.g., paper and microfilm). The sanitization process removes

information from system media such that the information cannot be retrieved or reconstructed. Sanitization techniques—including clearing, purging, cryptographic erase, de-identification of personally identifiable information, and destruction—prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods, recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media that contains information deemed to be in the public domain or publicly releasable or information deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media that contains classified information. NARA policies control the sanitization process for controlled unclassified information.

TxDOT Discussion

If it is possible that restricted personal information, confidential information, mission critical information, intellectual property, or licensed software is contained on the storage device, the storage device should be sanitized or the storage device should be removed and destroyed. Additional information on sanitization tools and methods of destruction (that comply with the Department of Defense 5220.22-M standard) are provided in the "Sale or Transfer of Computers and Software" guidelines available at http://www.dir.texas.gov.

TxDOT References

Information Security and Privacy Policy

State References

TGC 441; TGC 2054; 13 TAC 6.97; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

32 CFR 2002; OMB A-130; NARA CUI Registry; FIPS 199; NIST SP 800-60-1, 800-60-2, 800-88, 800-124; NIST IR 8023; NSA Media Destruction Guidance; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-03, AC-07, AU-11, MA-02, MA-03, MA-04, MA-05, PM-22, SI-12, SI-19, SR-11

MP-06(01) Review, Approve, Track, Document, and Verify

Baselines

Moderate, High

Overlays

PCI DSS; FedRAMP High

Requirements

Review, approve, track, document, and verify media sanitization and disposal actions.

Implementation Standards

Std.01 — A state agency shall permanently remove data from data processing equipment before disposing of or otherwise transferring the equipment to a person who is not a state agency or other agent of the state. This section applies only to equipment that will not be owned by the state after the disposal or other transfer. [Source: TGC 2054.130(a)]

Std.02 —

a. Inventory logs of all electronic media with cardholder data are maintained. [Source: PCI DSS 9.4.5]

b. Inventories of electronic media with cardholder data are conducted at least once every 12 months. [Source: PCI DSS 9.4.5.1]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 9.4.5 and 9.4.5.1.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Organizations review and approve media to be sanitized to ensure compliance with records retention policies. Tracking and documenting actions include listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken and personnel who performed the verification, and the disposal actions taken. Organizations verify that the sanitization of the media was effective prior to disposal.

TxDOT Discussion

DIR rules for implementation for TGC 2054.130(a) includes rules that: specify the types of data processing equipment covered by the section, including computer hard drives and other memory components; explain the acceptable methods for removal of data; and adopt appropriate forms for use by state agencies in documenting the removal process, including forms for documenting completion of the process. [Source: TGC 2054.130(b)(1, 2, 3)]

TxDOT References

Information Security and Privacy Policy

State References

TGC 2054; DIR Security Control Standards Catalog

Federal References

32 CFR 2002; OMB A-130; NARA CUI Registry; FIPS 199; NIST SP 800-60-1, 800-60-2, 800-88, 800-124; NIST IR 8023; NSA Media Destruction Guidance; PCI DSS; FedRAMP Security Controls Baseline

Related Controls

None.

MP-06(02) Equipment Testing

Baselines

High

Overlays

FedRAMP High

Requirements

Test sanitization equipment and procedures at least annually to ensure that the intended sanitization is being achieved.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.01 FedRAMP — Test sanitization equipment and procedures at least every six (6) months to ensure that the intended sanitization is being achieved. [Source: FedRAMP Security Controls Baseline MP-6(2)]

Discussion

Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities, including federal agencies or external service providers.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

Equipment and procedures may be tested or validated for effectiveness. [Source: FedRAMP Security Controls Baseline MP-6(2)]

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

32 CFR 2002; OMB A-130; NARA CUI Registry; FIPS 199; NIST SP 800-60-1, 800-60-2, 800-88, 800-124; NIST IR 8023; NSA Media Destruction Guidance; FedRAMP Security Controls Baseline

Related Controls

None.

MP-06(03) Nondestructive Techniques

Baselines

Low, Moderate, High

Overlays

FedRAMP High

Requirements

Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: circumstances as defined in Std.01.

Implementation Standards

Std.01 — Sanitize devices:

a. Upon initial receipt;

b. Following any external maintenance or release from organizational control;

c. After any suspected or confirmed event involving the device, if disposal is not warranted; and

d. Prior to release for reuse.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Portable storage devices include external or removable hard disk drives (e.g., solid state, magnetic), optical discs, magnetic or optical tapes, flash memory devices, flash memory cards, and other external or removable disks. Portable storage devices can be obtained from untrustworthy sources and contain malicious code that can be inserted into or transferred to organizational systems through USB ports or other entry portals. While scanning storage devices is recommended, sanitization provides additional assurance that such devices are free of malicious code. Organizations consider nondestructive sanitization of portable storage devices when the devices are purchased from manufacturers or vendors prior to initial use or when organizations cannot maintain a positive chain of custody for the devices.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

32 CFR 2002; OMB A-130; NARA CUI Registry; FIPS 199; NIST SP 800-60-1, 800-60-2, 800-88, 800-124; NIST IR 8023; NSA Media Destruction Guidance; FedRAMP Security Controls Baseline

Related Controls

None.

MP-07 Media Use

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Restrict the use of digital and non-digital media on systems containing TxDOT Sensitive, Confidential or Regulated data using implementation requirements outlined in Stds.02 & 03; and

b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 —

a. Digital media cannot be used to store TxDOT Sensitive, Confidential or Regulated data unless all the requirements below are followed.

The digital media must be:

1. Encrypted in accordance with SC-28(01);

2. Marked in accordance with MP-03;

3. Stored when not in use in accordance with MP-04;

4. Transported in accordance with MP-05;

5. Disposed of in accordance with MP-06.

b. Non-digital media cannot be used to store TxDOT Sensitive, Confidential or Regulated data unless all the requirements below are followed. The non-digital media must be:

1. Marked in accordance with MP-03;

2. Stored when not in use in accordance with MP-04;

3. Transported in accordance with MP-05;

4. Disposed of in accordance with MP-06.

Std.03 — Personally owned digital media should not be used to store TxDOT Sensitive, Confidential or Regulated data, unless previously authorized by the Information Security Office.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.04 PCI — For removable electronic media, the anti-malware solution(s):

a. Performs automatic scans of when the media is inserted, connected, or logically mounted; or

b. Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.

[Source: PCI DSS 5.3.3]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.05 CJIS — Prohibit the use of personally owned digital media devices on all agency owned or controlled systems that store, process, or transmit criminal justice information. [Source: CJIS MP-07]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

System media includes both digital and non-digital media. Digital media includes diskettes, magnetic tapes, flash drives, compact discs, digital versatile discs, and removable hard disk drives. Non-digital media includes paper and microfilm. Media use protections also apply to mobile devices with information storage capabilities. In contrast to MP-02, which restricts user access to media, MP-07 restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Organizations use technical and nontechnical controls to restrict the use of system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports or disabling or removing the ability to insert, read, or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices, including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, such as by prohibiting the use of writeable, portable storage devices and implementing this restriction by disabling or removing the capability to write to such devices. Requiring identifiable owners for storage devices reduces the risk of using such devices by allowing organizations to assign responsibility for addressing known vulnerabilities in the devices.

TxDOT Discussion

None.

TxDOT References

TxDOT Acceptable Use Policy; Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 199; NIST SP 800-11; CJIS Security Policy; FedRAMP Security Controls Baseline; PCI DSS

Related Controls

AC-19, AC-20, PL-04, PM-12

PE — Physical and Environmental Protection

PE-01 Policy and Procedures

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level physical and environmental protection policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;

b. Designate a senior management official as defined in the physical and environmental protection policy to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and

c. Review and update the current physical and environmental protection:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 9.1.1 and 9.1.2.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Review and update the current physical and environmental protection policy and procedures following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. [Source: CJIS PE-01]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Physical and environmental protection policy and procedures address the controls in the PE family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of physical and environmental protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to physical and environmental protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-12, 800-30, 800-39, 800-100; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AT-03, PM-09, PS-08, SI-12

PE-02 Physical Access Authorizations

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;

b. Issue authorization credentials for facility access;

c. Review the access list detailing authorized facility access by individuals at the frequency specified in Std.02; and

d. Remove individuals from the facility access list when access is no longer required.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Access log review minimum frequency by system categorization:

a. Low — At least annually;

b. Moderate — At least quarterly;

c. High — Weekly.

Std.03 — Ensure authorization credential systems (for example, card/badge creation systems, card readers) are controlled and managed by authorized personnel.

Std.04 — Issue authorization credentials (for example, badges) providing only the level of access required to complete the individual's job responsibilities.

Std.05 — Revoke authorizations in accordance with PS-04, PS-05, and other applicable requirements.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 9.3.1.1.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PE-02.

Std.06 CJIS —Rescinded in V4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Physical access authorizations apply to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include ID badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Physical access authorizations may not be necessary to access certain areas within facilities that are designated as publicly accessible.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 201; NIST SP 800-73-4, 800-76-2, 800-78-4; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AT-03, AU-09, IA-04, MA-05, MP-02, PE-03, PE-04, PE-05, PE-08, PM-12, PS-03, PS-04, PS-05, PS-06

PE-03 Physical Access Control

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Enforce physical access authorizations at entry and exit points as defined in Std.01 by:

1. Verifying individual access authorizations before granting access to the facility; and

2. Controlling ingress and egress to the facility using physical access devices (for example, keys, locks, combinations, card readers) and/or guards;

b. Maintain physical access audit logs for entry and exit points as defined in Std.01;

c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: controls as defined in Std.02;

d. Escort visitors and control visitor activity in all areas of the facility not designated as publicly accessible;

e. Secure keys, combinations, and other physical access devices;

f. Inventory organization-owned physical access devices every 90 days; and

g. Change combinations and keys when first installed or before use if a default is provided by the vendor, annually, and whenever there is a theft or security violation in the area being protected, and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

Implementation Standards

Std.01 — Control all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations.

Std.02 — Control access to areas officially designated as publicly accessible in accordance with the assessment of risk. Use identification and/or access badges in conjunction with access control readers (card readers), security guards, closed-circuit TV cameras and monitors, and sign-in/sign-out sheets to control entry to district and HQ facilities. Restrict access to grounds/facilities to authorized persons only.

Std.03 — Retain access records, entry and exit logs, and visitor logs in accordance with records retention or other state or federal requirements.

Std.04 — Control data center/facility access by use of door and window locks and, for moderate- or high-baseline systems, security personnel or physical authentication devices, such as biometrics and/or smart card/PIN combination.

Std.05 — Store and operate servers in physically secure environments and, for moderate- or high-baseline servers, grant access to explicitly authorized personnel only. Access is monitored and recorded.

Std.06 — Physically secure access to computer, paper, or other systems containing TxDOT Sensitive, Confidential, or Regulated Information from unauthorized personnel and theft (for example, through the use of door locks, cable locks, storing laptops in the trunk of the car instead of the passenger area, etc.).

Std.07 — Record the date that keys and combinations are changed and the identity of the person making those changes in the system security plan. [Source: FedRAMP Continuous Monitoring Strategy & Guide]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 9.2.1.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.08 PCI — Procedures are implemented for authorizing and managing physical access of personnel to the Cardholder Data Environment (CDE), including:

a. Identifying personnel.

b. Managing changes to an individual's physical access requirements.

c. Revoking or terminating personnel identification.

d. Limiting access to the identification process or system to authorized personnel.

[Source: PCI DSS 9.3.1]

Std.12 PCI — Access to consoles in sensitive areas is restricted via locking when not in use. [Source: PCI DSS 9.2.4]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.09 CJIS — Rescinded in V4.0.

Std.10 CJIS — Rescinded in V4.0.

Std.13 CJIS — If the above conditions cannot be met refer to the requirements listed in PE-17. [Source: CJIS PE-03]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low and Moderate baselines.

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.11 FedRAMP —

a. Enforce physical access authorizations at Cloud Service Provider (CSP)-defined entry and exit points to the facility where the system resides by:

1. Verifying individual access authorizations before granting access to the facility; and

2. Controlling ingress and egress to the facility using CSP-defined physical access control systems/devices and guards;

b. Maintain physical access audit logs for all designated entry/exit points to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);

c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: controls as defined in Std.02;

d. Escort visitors and control visitor activity in all circumstances within restricted access area where the information system resides;

e. Secure keys, combinations, and other physical access devices;

f. Inventory organization-owned physical access devices at least annually; and

g. Change combinations and keys at least annually or earlier as required by a security relevant event and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

[Source: FedRAMP Security Controls Baseline PE-3]

Discussion

Physical access control applies to employees and visitors. Individuals with permanent physical access authorizations are not considered visitors. Physical access controls for publicly accessible areas may include physical access control logs/records, guards, or physical access devices and barriers to prevent movement from publicly accessible areas to non-public areas. Organizations determine the types of guards needed, including professional security staff, system users, or administrative staff. Physical access devices include keys, locks, combinations, biometric readers, and card readers. Physical access control systems comply with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof. Physical access points can include facility access points, interior access points to systems that require supplemental access controls, or both. Components of systems may be in areas designated as publicly accessible with organizations controlling access to the components.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 201; NIST SP 800-73-4, 800-76-2, 800-78-4, 800-116; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AT-03, AU-02, AU-06, AU-09, CP-10, IA-03, IA-08, MA-05, MP-02, MP-04, PE-02, PE-04, PE-05, PE-08, PS-02, PS-03, PS-06, PS-07, RA-03, SC-28, SI-04, SR-03

PE-03(01) System Access

Baselines

High

Overlays

FedRAMP High

Requirements

Enforce physical access authorizations to the system in addition to the physical access controls for the facility at all TxDOT-managed facilities containing one or more components of the system.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Control of physical access to the system provides additional physical security for those areas within facilities where there is a concentration of system components.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FIPS 201; NIST SP 800-73-4, 800-76-2, 800-78-4, 800-116; FedRAMP Security Controls Baseline

Related Controls

None.

PE-04 Access Control for Transmission

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Control physical access to network and information system distribution and transmission lines within organizational facilities using security safeguards defined in Stds.01-03.

Implementation Standards

Std.01 — For systems whether on TxDOT property or housed in infrastructure service provider's facilities, control physical access to moderate and high-impact systems' distribution and transmission lines by locking wire cabinets, disconnecting or locking spare jacks, and protecting cabling by conduit or cable trays.

Std.02 — Limit, monitor, and restrict physical access to moderate and high-impact systems and high-volume media storage areas through automated systems or guard stations.

Std.03 — Control physical access to sensitive areas for onsite personnel. Access must be authorized and based on individual job function in accordance with access control policy; revoked immediately upon termination; auditable; and processes must be in place to retrieve or disable physical access mechanisms such as keys and access cards at need.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 9.2.2.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.04 PCI — Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted. [Source: PCI DSS 9.2.3]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PE-04.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Security controls applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Security controls used to control physical access to system distribution and transmission lines include disconnected or locked spare jacks, locked wiring closets, protection of cabling by conduit or cable trays, and wiretapping sensors.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AT-03, IA-04, MP-02, MP-04, PE-02, PE-03, PE-05, PE-09, SC-07, SC-08

PE-05 Access Control for Output Devices

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Control physical access to output from devices defined in Std.01 to prevent unauthorized individuals from obtaining the output.

Implementation Standards

Std.01 — Secure physical access to paper, computers, or other systems containing TxDOT Sensitive, Confidential, or Regulated Information from

unauthorized personnel and from theft. This includes, but is not limited to, using door locks and cable locks, storing portable devices in locked containers during transportation, and refraining from displaying or leaving unsecured material in plain view.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.02 CJIS — Rescinded in V4.0.

Std.03 CJIS — Control physical access to output from monitors, printers, scanners, audio devices, facsimile machines, and copiers to prevent unauthorized individuals from obtaining the output. [Source: CJIS PE-05]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and allowing access to authorized individuals only, placing output devices in locations that can be monitored by personnel, installing monitor or screen filters, and using headphones. Examples of output devices include monitors, printers, scanners, audio devices, facsimile machines, and copiers.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST IR 8023; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

PE-02, PE-03, PE-04, PE-18

PE-06 Monitoring Physical Access

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;

b. Review physical access logs at the frequency specified in Std.02 and upon occurrence of events or potential indications of events as specified in the incident response policy and procedures; and

c. Coordinate results of reviews and investigations with the organizational incident response capability.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Access log review minimum frequency by system categorization:

a. Low — Every 90 days;

b. Moderate — Monthly;

c. High — Weekly.

Std.03 — Investigate and respond to detected physical access activities in accordance with the incident response policy.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.04 PCI — Individual physical access to sensitive areas within the Cardholder Data Environment (CDE) is monitored with either video cameras or physical access control mechanisms (or both) as follows:

a. Entry and exit points to/from sensitive areas within the CDE are monitored.

b. Monitoring devices or mechanisms are protected from tampering or disabling.

c. Collected data is reviewed and correlated with other entries.

d. Collected data is stored for at least three months, unless otherwise restricted by law.

[Source: PCI DSS 9.2.1.1]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.06 CJIS — Review physical access logs quarterly and upon occurrence of any physical, environmental, or security-related incidents involving CJI or systems used to process, store, or transmit CJI. [Source: CJIS PE-06]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low baseline.

For systems subject to FedRAMP requirements at the Moderate baseline, the following standard applies:

Std.05 FedRAMP — Review physical access logs at least monthly and upon occurrence of events or potential indications of events as specified in the incident response policy and procedures. [Source: FedRAMP Security Controls Baseline PE-6]

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Physical access monitoring includes publicly accessible areas within organizational facilities. Examples of physical access monitoring include the employment of guards, video surveillance equipment (i.e., cameras), and sensor devices. Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential threats. The reviews can be supported by audit logging controls, such as AU-02, if the access logs are part of an automated system. Organizational incident response capabilities include investigations of physical security incidents and responses to the incidents. Incidents include security violations or suspicious physical access activities. Suspicious physical access activities include accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, and out-of-sequence accesses.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AU-02, AU-06, AU-09, AU-12, CA-07, CP-10, IR-04, IR-08

PE-06(01) Intrusion Alarms and Surveillance Equipment

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

Implementation Standards

Std.01 — Provide real-time physical intrusion alarms and surveillance equipment for facilities hosting TxDOT systems.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PE-06(01).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Physical intrusion alarms can be employed to alert security personnel when unauthorized access to the facility is attempted. Alarm systems work in conjunction with physical barriers, physical access control systems, and security guards by triggering a response when these other forms of security have been compromised or breached. Physical intrusion alarms can include different types of sensor devices, such as motion sensors, contact sensors, and broken glass sensors. Surveillance equipment includes video cameras installed at strategic locations throughout the facility.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

PE-06(04) Monitoring Physical Access to Systems

Baselines

High

Overlays

FedRAMP High

Requirements

Monitor physical access to the system in addition to the physical access monitoring of the facility at all TxDOT-managed facilities containing one or more components of the system.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Monitoring physical access to systems provides additional monitoring for those areas within facilities where there is a concentration of system components, including server rooms, media storage areas, and

communications centers. Physical access monitoring can be coordinated with intrusion detection systems and system monitoring capabilities to provide comprehensive and integrated threat coverage for the organization.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

PE-08 Visitor Access Records

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Maintain visitor access records to the facility where the system resides for three years, as required by the Texas State Records Retention Schedule;

b. Review visitor access records at the frequency defined in Std.02; and

c. Report anomalies in visitor access records to personnel with facility security responsibilities.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 —

a. Access log review minimum frequency by system categorization:

1. Low — Twice per year;

2. Moderate — Every 90 days;

3. High — Weekly.

b. Report anomalies upon discovery.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.03 PCI — Procedures are implemented for authorizing and managing visitor access to the Cardholder Data Environment (CDE), including:

a. Visitors are authorized before entering.

b. Visitors are escorted at all times.

c. Visitors are clearly identified and given a badge or other identification that expires.

d. Visitor badges or other identification visibly distinguishes visitors from personnel.

[Source: PCI DSS 9.3.2]

e. Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration. [Source: PCI DSS 9.3.3]

f. A visitor log is used to maintain a physical record of visitor activity within the facility and within sensitive areas, including:

1. The visitor’s name and the organization represented.

2. The date and time of the visit.

3. The name of the personnel authorizing physical access.

4. Retaining the log for at least three months, unless otherwise restricted by law.

[Source: PCI DSS 9.3.4]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.05 CJIS — Review visitor access records quarterly. [Source: CJIS PE-08]

TX-RAMP Correspondence

For systems subject to TX-RAMP Level 1 or Level 2 requirements, the following standard applies:

Std.04 TX-RAMP — Review visitor access records at least quarterly. [Source: TX-RAMP Manual PE-8]

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low or Moderate baselines, the following standard applies:

Std.05 FedRAMP — Review visitor access records monthly. [Source: FedRAMP Security Controls Baseline PE-8]

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Visitor access records include the names and organizations of individuals visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purpose of visits, and the names and organizations of individuals visited. Access record reviews determine if access authorizations are current and are still required to support organizational mission and business functions. Access records are not required for publicly accessible areas.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

PE-02, PE-03, PE-06

PE-08(01) Automated Records Maintenance and Review

Baselines

High

Overlays

FedRAMP High

Requirements

Maintain and review visitor access records using automated mechanisms as identified in applicable System Security Plans (SSPs).

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Visitor access records may be stored and maintained in a database management system that is accessible by organizational personnel. Automated access to such records facilitates record reviews on a regular

basis to determine if access authorizations are current and still required to support organizational mission and business functions.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

PE-08(03) Limit Personally Identifiable Information Elements

Baselines

N/A

Overlays

CJIS; Privacy

Requirements

Limit personally identifiable information contained in visitor access records to the following elements identified in the privacy risk assessment: only those elements identified in Std.01.

Implementation Standards

Std.01 — Only retain the following elements of personally identifiable information (PII):

a. Name;

b. Organization;

c. Signature;

d. Forms of identification used to validate visitor;

e. Purpose of visit; and

f. Name and organization of person being visited.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PE-08(03).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Organizations may have requirements that specify the contents of visitor access records. Limiting personally identifiable information in visitor access records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

CJIS Security Policy

Related Controls

RA-03, SA-08

PE-09 Power Equipment and Cabling

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Protect power equipment and power cabling for the system from damage and destruction.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PE-09.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organizations determine the types of protection necessary for the power equipment and cabling employed at different locations that are both internal and external to organizational facilities and environments of operation. Types of power equipment and cabling include internal cabling and uninterruptable power sources in offices or data centers, generators and power cabling outside of buildings, and power sources for self-contained components such as satellites, vehicles, and other deployable systems.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

CJIS Security Policy

Related Controls

PE-04

PE-10 Emergency Shutoff

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Provide the capability of shutting off power to systems or individual system components as identified in contingency plans in emergency situations;

b. Place emergency shutoff switches or devices in location by system or system component as defined in Std.01 to facilitate access for authorized personnel; and

c. Protect emergency power shutoff capability from unauthorized activation.

Implementation Standards

Std.01 — Implement and maintain a master power switch or emergency cut-off switch, prominently marked, and protected against accidental activation by a cover, for data centers, servers, and mainframe rooms.

Std.02 — Document the location of emergency shutoff switches or devices in contingency plans.

Std.03 — Provide appropriate personnel with training on safe operation of emergency power shutoffs.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, PE-10a is superseded by CJIS requirement PE-10a:

Std.05 CJIS — Provide the capability of shutting off power to all information systems in emergency situations. [Source: CJIS 5.9: PE-10]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.04 FedRAMP — Place emergency shutoff switches or devices in near more than one egress point of the IT area and ensures it is labeled and protected by a cover to prevent accidental shut-off to facilitate access for authorized personnel. [Source: FedRAMP Security Controls Baseline PE-10]

Discussion

Emergency power shutoff primarily applies to organizational facilities that contain concentrations of system resources, including data centers, mainframe computer rooms, server rooms, and areas with computer-controlled machinery.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

PE-15

PE-11 Emergency Power

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Provide an uninterruptible power supply to facilitate an orderly shutdown of the system or transition of the system to long-term alternate power in the event of a primary power source loss.

Implementation Standards

Std.01 — Transition plans for critical systems must be documented in the contingency plan. UPS for critical systems may be installed centrally or locally, and must be sized to permit transition to long-term alternate power.

Std.02 — For non-critical systems, UPS must be sized, at a minimum, so that the system can be shut down safely. [Source: SP 800-82]

Std.03 — UPS must be tested at least annually and prior to seasons of expected events (for example, hurricane season).

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PE-11.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

An uninterruptible power supply (UPS) is an electrical system or mechanism that provides emergency power when there is a failure of the main power source. A UPS is typically used to protect computers, data centers, telecommunication equipment, or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious mission or business disruption, or loss of data or information. A UPS differs from an emergency power system or backup generator in that the UPS provides near-instantaneous protection from unanticipated power interruptions from the main power source by providing energy stored in batteries, supercapacitors, or flywheels. The battery duration of a UPS is relatively short but provides sufficient time to start a standby power source, such as a backup generator, or properly shut down the system.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AT-03, CP-02, CP-07

PE-11(01) Alternate Power Supply — Minimal Operational Capability

Baselines

High

Overlays

FedRAMP High

Requirements

Provide an alternate power supply for the system that is activated manually or automatically and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.

Implementation Standards

Std.01 — Test the equipment:

a. On a schedule that complies with manufacturer recommendations and local, state, and federal requirements;

b. As part of full-scale contingency testing;

c. After use during contingency events; and

d. At least once in every three-year period (if no test has been performed per requirements above).

Std.02 — Document the alternate power supply in the contingency plan for the system, including supporting systems for major applications.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate baseline.

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.03 FedRAMP — Provide an alternate power supply for the system that is activated automatically and that can maintain minimally required operational capability in the event of an extended loss of the primary power source. [Source: FedRAMP Security Controls Baseline PE-11(1)]

Discussion

Provision of an alternate power supply with minimal operating capability can be satisfied by accessing a secondary commercial power supply or other external power supply.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

PE-12 Emergency Lighting

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Implementation Standards

Std.01 — Rescinded in V2.2.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PE-12.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

The provision of emergency lighting applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Emergency lighting provisions for the system are described in the contingency plan for the organization. If emergency lighting for the system fails or cannot be provided, organizations consider alternate processing sites for power-related contingencies.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CP-02, CP-07

PE-13 Fire Protection

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

Implementation Standards

Std.01 — TxDOT shall train designated employees on environmental control procedures, monitoring, and equipment in case of emergencies or equipment problems. [Source: DIR Control Standards Catalog PE-1]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PE-13.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

The provision of fire detection and suppression systems applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Fire detection and suppression systems that may require an independent energy source include sprinkler systems and smoke detectors. An independent energy source is an energy source, such as a microgrid, that is separate, or can be separated, from the energy sources providing power for the other parts of the facility.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AT-03

PE-13(01) Detection Systems — Automatic Activation and Notification

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Employ fire detection systems that activate automatically and notify personnel as defined in the System Security Plan (SSP) and emergency responders as defined in the SSP or facility's safety plan in the event of a fire.

Implementation Standards

Std.01 — Ensure that fire detection systems are not tied into the facility's intrusion device system (IDS).

Std.02 — In accordance with local regulations, ensure facilities undergo fire marshal inspections and promptly resolve identified deficiencies.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PE-13(01).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.03 FedRAMP — Employ fire detection systems that activate automatically and notify service provider building maintenance/physical security personnel and service provider emergency responders with incident response responsibilities in the event of a fire. [Source: FedRAMP Security Controls Baseline PE-13(1)]

Discussion

Organizations can identify personnel, roles, and emergency responders if individuals on the notification list need to have access authorizations or clearances (e.g., to enter to facilities where access is restricted due to the classification or impact level of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

PE-13(02) Suppression Systems — Automatic Activation and Notification

Baselines

Moderate, High

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

a. Employ fire suppression systems that activate automatically and notify personnel as defined in the System Security Plan (SSP) and emergency responders as defined in the SSP or facility's safety plan; and

b. Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.

Implementation Standards

Std.01 — In accordance with local regulations, ensure the facility undergoes fire marshal inspections and promptly resolve identified deficiencies.

Std.02 — Ensure that contingency plans account for suppression system impacts.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organizations can identify specific personnel, roles, and emergency responders if individuals on the notification list need to have appropriate

access authorizations and/or clearances (e.g., to enter to facilities where access is restricted due to the impact level or classification of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

PE-14 Environmental Controls

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Maintain temperature and humidity levels within the facility where the system resides at acceptable levels as specified in the documentation for the equipment being protected; and

b. Monitor environmental control levels at an acceptable frequency as specified in the documentation for the equipment being protected.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Monitoring systems should be configured to generate an alert when environmental specifications such as temperature and humidity are exceeded. [Source: SP 800-82]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PE-14.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standards apply:

Std.03 FedRAMP —

a. Maintain temperature and humidity levels within the facility where the system resides consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments; and

b. Monitor environmental control levels continuously.

[Source: FedRAMP Security Controls Baseline PE-14]

Std.04 FedRAMP — The service provider measures temperature at server inlets and humidity levels by dew point. [Source: FedRAMP Security Controls Baseline PE-14]

Discussion

The provision of environmental controls applies primarily to organizational facilities that contain concentrations of system resources (e.g., data centers, mainframe computer rooms, and server rooms). Insufficient environmental controls, especially in very harsh environments, can have a significant adverse impact on the availability of systems and system components that are needed to support organizational mission and business functions.

TxDOT Discussion

Note for systems subject to CJIS requirements:

This control only applies to data centers as defined in Appendix A Terms and Definitions. [Source: CJIS PE-14]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AT-03, CP-02

PE-14(02) Monitoring with Alarms and Notifications

Baselines

N/A

Overlays

FedRAMP High

Requirements

Employ environmental control monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment to personnel as defined in the System Security Plan (SSP).

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

The alarm or notification may be an audible alarm or a visual message in real time to personnel or roles defined by the organization. Such alarms and notifications can help minimize harm to individuals and damage to organizational assets by facilitating a timely incident response.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

PE-15 Water Damage Protection

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Implementation Standards

Std.01 — Rescinded in V2.2.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PE-15.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

The provision of water damage protection primarily applies to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern without affecting entire organizations.

TxDOT Discussion

Note for systems subject to CJIS requirements:

This control only applies to data centers as defined in Appendix A Terms and Definitions. [Source: CJIS PE-15]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AT-03, PE-10

PE-15(01) Automation Support

Baselines

High

Overlays

FedRAMP High

Requirements

Detect the presence of water near the system and alert personnel or roles as identified in the System Security Plan (SSP) using automated mechanisms as identified in applicable SSPs.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.01 FedRAMP — Detect the presence of water near the system and alert service provider building maintenance/physical security personnel.

[Source: FedRAMP Security Controls Baseline PE-15(1)]

Discussion

Automated mechanisms include notification systems, water detection sensors, and alarms.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

PE-16 Delivery and Removal

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Authorize and control system components and related items entering and exiting the facility; and

b. Maintain records of the system components.

Implementation Standards

Std.01 — Rescinded in V2.2.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PE-16.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Enforcing authorizations for entry and exit of system components may require restricting access to delivery areas and isolating the areas from the system and media libraries.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

CM-03, CM-08, MA-02, MA-03, MP-05, SR-02, SR-03, SR-04, SR-06

PE-17 Alternate Work Site

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Determine and document the alternate work sites in contingency plans allowed for use by employees;

b. Employ the following controls at alternate work sites: security and privacy controls equivalent to those applicable at the primary work site;

c. Assess the effectiveness of controls at alternate work sites; and

d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

Implementation Standards

Std.01 — Alternate work sites (remote locations) must be identified in System Security Plans (SSPs) or contingency plans and available for business resumption activities in case of a disaster.

Std.02 — All equipment stored at alternate work sites must be secured when not in use and must be protected from damage and unauthorized access at all times.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Employ the following controls at alternate work sites:

a. Limit access to the area during CJI processing times to only those personnel authorized by the agency to access or view CJI.

b. Lock the area, room, or storage container when unattended.

c. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.

d. Follow the encryption requirements found in SC-13 and SC-28 for electronic storage (i.e., data at-rest) of CJI.

[Source: CJIS PE-17]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Alternate work sites include government facilities or the private residences of employees. While distinct from alternative processing sites, alternate work sites can provide readily available alternate locations during contingency operations. Organizations can define different sets of controls for specific alternate work sites or types of sites depending on the work-related activities conducted at the sites. Implementing and assessing the effectiveness of organization-defined controls and providing a means to communicate incidents at alternate work sites supports the contingency planning activities of organizations.

TxDOT Discussion

TxDOT defines a "remote location" as: A location outside the designated work location including, but not limited to, the employee’s home, a satellite office, or another location from which an employee can safely perform work functions. [Source: TxDOT Flexible Work Strategy Division and District SOP Guidance]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-46; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-17, AC-18, CP-07

PE-18 Location of System Components

Baselines

High

Overlays

CJIS; FedRAMP High

Requirements

Position system components within the facility to minimize potential damage from physical and environmental hazards as identified in the facility risk assessment (to include water, HAZMAT, exhaust hoods and fans, and fuel storage areas) and to minimize the opportunity for unauthorized access.

Implementation Standards

Std.01 — The organization considers the risks associated with physical and environmental hazards when planning new control system facilities or reviewing existing facilities. Risk mitigation strategies are documented in the control system security plan. [Source: Catalog of Control Systems Security: Recommendations for Standards Developers]

Std.02 — Document the physical location of system components in accordance with CM-08.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement 5.20.1.1.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an electromagnetic pulse,

electrical interference, and other forms of incoming electromagnetic radiation. Organizations consider the location of entry points where unauthorized individuals, while not being granted access, might nonetheless be near systems. Such proximity can increase the risk of unauthorized access to organizational communications using wireless packet sniffers or microphones, or unauthorized disclosure of information.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

CM-08, CP-02, PE-05, RA-03

PL — Planning

PL-01 Policy and Procedures

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level planning policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;

b. Designate a senior management official as defined in the planning policy to manage the development, documentation, and dissemination of the planning policy and procedures; and

c. Review and update the current planning:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — The TxDOT CISO reports annually on the TxDOT information security program in compliance with 1 TAC 202.23(a). [Source: DIR Control Standards Catalog PL-1]

Std.02 — The TxDOT Executive Director or their designated representative(s) shall ensure that senior agency officials and information-owners, in collaboration with the Information Resources Manager and Information Security Officer, support the provision of information security for the information systems that support the operations and assets under their direct or indirect (e.g., cloud computing or outsourced) control. [Source: 1 TAC 202.20(b)(3)]

Std.03 — The Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.04 CJIS — Review and update the current planning policy and procedures following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. [Source: CJIS PL-01]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Planning policy and procedures for the controls in the PL family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to planning policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-12, 800-18, 800-30, 800-39, 800-100; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

PM-09, PS-08, SI-12

PL-02 System Security and Privacy Plans

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop security and privacy plans for the system that:

1. Are consistent with the organization's enterprise architecture;

2. Explicitly define the constituent system components;

3. Describe the operational context of the system in terms of mission and business processes;

4. Identify the individuals that fulfill system roles and responsibilities;

5. Identify the information types processed, stored, and transmitted by the system;

6. Provide the security categorization of the system, including supporting rationale;

7. Describe any specific threats to the system that are of concern to the organization;

8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;

9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;

10. Provide an overview of the security and privacy requirements for the system;

11. Identify any relevant control baselines or overlays, if applicable;

12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;

13. Include risk determinations for security and privacy architecture and design decisions;

14. Include security- and privacy-related activities affecting the system that require planning and coordination with individuals or groups as identified in organization plans (including system security plans (SSPs), contingency plans, and incident response plans); and

15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

b. Distribute copies of the plans and communicate subsequent changes to the plans to personnel or roles as identified in the SSP;

c. Review the plans at least annually or when required due to system modifications or changes to the environment of operation (including new legislative requirements and newly discovered vulnerabilities);

d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and

e. Protect the plans from unauthorized disclosure and modification.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Develop a System Security Plan (SSP) template consistent with the TxDOT Information Security and Privacy Catalog Baselines.

Std.03 — Require that systems complete the SSP as part of the authorization process; and update to the approved SSP template prior to system authorization or re-authorization.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.04 CJIS —

a. Include security- and privacy-related activities affecting the system that require planning and coordination with individuals or groups as identified in organization plans (including system security plans (SSPs), contingency plans, and incident response plans); and

b. Review the system security and privacy plans at least annually or when required due to system changes or modifications.

[Source: CJIS PL-02]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

System security and privacy plans are scoped to the system and system components within the defined authorization boundary and contain an overview of the security and privacy requirements for the system and the controls selected to satisfy the requirements. The plans describe the intended application of each selected control in the context of the system with a sufficient level of detail to correctly implement the control and to subsequently assess the effectiveness of the control. The control documentation describes how system-specific and hybrid controls are implemented and the plans and expectations regarding the functionality of the system. System security and privacy plans can also be used in the design and development of systems in support of life cycle-based security and privacy engineering processes. System security and privacy plans are living documents that are updated and adapted throughout the system development life cycle (e.g., during capability determination, analysis of alternatives, requests for proposal, and design reviews). Section 2.1 describes the different types of requirements that are relevant to organizations during the system development life cycle and the relationship between requirements and controls.

Organizations may develop a single, integrated security and privacy plan or maintain separate plans. Security and privacy plans relate security and privacy requirements to a set of controls and control enhancements. The plans describe how the controls and control enhancements meet the security and privacy requirements but do not provide detailed, technical descriptions of the design or implementation of the controls and control enhancements. Security and privacy plans contain sufficient information (including specifications of control parameter values for selection and assignment operations explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented.

Security and privacy plans need not be single documents. The plans can be a collection of various documents, including documents that already exist. Effective security and privacy plans make extensive use of references to policies, procedures, and additional documents, including design and implementation specifications where more detailed information can be obtained. The use of references helps reduce the documentation associated with security and privacy programs and maintains the security- and privacy-related information in other established management and operational areas, including enterprise architecture, system development life cycle, systems engineering, and acquisition. Security and privacy plans need not contain detailed contingency plan or incident response plan information but can instead provide—explicitly or by reference—sufficient information to define what needs to be accomplished by those plans.

Security- and privacy-related activities that may require coordination and planning with other individuals or groups within the organization include assessments, audits, inspections, hardware and software maintenance, acquisition and supply chain risk management, patch management, and contingency plan testing. Planning and coordination include emergency and nonemergency (i.e., planned or non-urgent unplanned) situations. The process defined by organizations to plan and coordinate security- and privacy-related activities can also be included in other documents, as appropriate.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-18, 800-37, 800-160-1, 800-160-2; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-02, AC-06, AC-14, AC-17, AC-20, CA-02, CA-03, CA-07, CM-09, CP-02, CP-04, IR-04, IR-08, MA-04, MA-05, MP-04, MP-05, PL-08, PL-10, PL-11, PM-01, PM-07, PM-08, PM-09, PM-10, PM-11, RA-03, RA-08, RA-09, SA-05, SA-17, SA-22, SI-12, SR-02, SR-04

PL-04 Rules of Behavior

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;

b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;

c. Review and update the rules of behavior annually; and

d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge annually.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The user of an information resource has the responsibility to:

a. Use the resource only for the purpose specified by the agency or information-owner;

b. Comply with information security controls and agency policies to prevent unauthorized or accidental disclosure, modification, or destruction of information and information resources; and

c. Formally acknowledge that they will comply with the security policies and procedures in a method determined by the TxDOT Executive Director or his or her designated representative. [Source: 1 TAC 202.22(a)(3)]

Std.03 — Agency information resources designated for use by the public shall be configured to enforce security policies and procedures without requiring user participation or intervention. Information resources must require the acceptance of a banner or notice prior to use. [Source: 1 TAC 202.22(a)(4)]

Std.04 — TxDOT must develop a data use agreement for use by the agency that meets the particular needs of the agency and is consistent with rules adopted by the Texas Department of Information Resources that relate to information security standards for state agencies. [Source: TGC 2054.135(a)]

Std.05 — TxDOT must update the data use agreement at least biennially but may update the agreement at any time as necessary to accommodate best practices in data management. [Source: TGC 2054.135(b)]

Std.06 — TxDOT must distribute the data use agreement and each update to that agreement, to employees of the agency who handle sensitive information, including financial, medical, personnel, or student data. The employee shall sign the data use agreement distributed and each update to the agreement. [Source: TGC 2054.135(c)]

Std.07 — To the extent possible, TxDOT must provide employees described in TGC 2054.135(c) with cybersecurity awareness training to coincide with the distribution of:

a. The data use agreement required under TGC 2054.135(b); and

b. Each biennial update to that agreement. [Source: TGC 2054.135(d)]

Std.08 — Users of an information resource must meet the standards established under "Sensitive Information" within the Human Resources Policy Manual. [Source: TxDOT Human Resources Policy Manual]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 12.6.3.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.10 PCI — Acceptable use policies for end-user technologies are documented and implemented, including:

a. Explicit approval by authorized parties.

b. Acceptable uses of the technology.

c. List of products approved by the company for employee use, including hardware and software.

[Source: PCI DSS 12.2.1]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.11 CJIS — Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge annually, or when the rules are revised or updated. [Source: CJIS PL-04]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.09 FedRAMP — Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge at least annually and when the rules are revised or changed. [Source: FedRAMP Security Controls Baseline PL-4]

Discussion

Rules of behavior represent a type of access agreement for organizational users. Other types of access agreements include nondisclosure agreements, conflict-of-interest agreements, and acceptable use agreements (see PS-06).

Organizations consider rules of behavior based on individual user roles and responsibilities and differentiate between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users, including individuals who receive information from federal systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for organizational and non-organizational users can also be established in AC-08. The related controls section provides a list of controls that are relevant to organizational rules of behavior. PL-04b, the documented acknowledgment portion of the control, may be satisfied by the literacy training and awareness and role-based training programs conducted by organizations if such training includes rules of behavior. Documented acknowledgements for rules of behavior include electronic or physical signatures and electronic agreement check boxes or radio buttons.

TxDOT Discussion

None.

TxDOT References

Human Resources Policy Manual; Information Security and Privacy Policy

State References

1 TAC 202; TGC 2054; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-18; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-02, AC-06, AC-08, AC-17, AC-18, AC-19, AC-20, AT-02, AT-03, CM-11, IA-02, IA-04, IA-05, MP-07, PS-06, PS-08, SA-05, SI-12

PL-04(01) Social Media and External Site/Application Usage Restrictions

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Include in the rules of behavior, restrictions on:

a. Use of social media, social networking sites, and external sites/applications;

b. Posting organizational information on public websites; and

c. Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PL-04(01).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Social media, social networking, and external site/application usage restrictions address rules of behavior related to the use of social media, social networking, and external sites when organizational personnel are using such sites for official duties or in the conduct of official business, when organizational information is involved in social media and social networking transactions, and when personnel access social media and networking sites from organizational systems. Organizations also address specific rules that prevent unauthorized entities from obtaining non-public organizational information from social media and networking sites either directly or through

inference. Non-public information includes personally identifiable information and system account information.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-18; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-22

PL-08 Security and Privacy Architectures

Baselines

Moderate, High

Overlays

CJIS; Privacy; Sensitive; TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop security and privacy architectures for the system that:

1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;

2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;

3. Describe how the architectures are integrated into and support the enterprise architecture; and

4. Describe any assumptions about, and dependencies on, external systems and services;

b. Review and update the architectures annually or when changes to the information system or its environment warrant to reflect changes in the enterprise architecture; and

c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PL-08.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

The security and privacy architectures at the system level are consistent with the organization-wide security and privacy architectures described in PM-07, which are integral to and developed as part of the enterprise architecture. The architectures include an architectural description, the allocation of security and privacy functionality (including controls), security- and privacy-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. The architectures can also include other information, such as user roles and the access privileges assigned to each role; security and privacy requirements; types of information processed, stored, and transmitted by the system; supply chain risk management requirements; restoration priorities of information and system services; and other protection needs.

SP 800-160-1 provides guidance on the use of security architectures as part of the system development life cycle process. OMB M-19-03 requires the use of the systems security engineering concepts described in SP 800-160-1 for high value assets. Security and privacy architectures are reviewed and updated throughout the system development life cycle, from analysis of alternatives through review of the proposed architecture in the RFP responses to the design reviews before and during implementation (e.g., during preliminary design reviews and critical design reviews).

In today's modern computing architectures, it is becoming less common for organizations to control all information resources. There may be key dependencies on external information services and service providers. Describing such dependencies in the security and privacy architectures is necessary for developing a comprehensive mission and business protection strategy. Establishing, developing, documenting, and maintaining under configuration control a baseline configuration for organizational systems is critical to implementing and maintaining effective architectures. The development of the architectures is coordinated with the senior agency information security officer and the senior agency official for privacy to ensure that the controls needed to support security and privacy requirements are identified and effectively implemented. In many circumstances, there may be no distinction between the security and privacy architecture for a system. In other circumstances, security objectives may be adequately satisfied, but privacy objectives may only be partially satisfied by the security requirements. In these cases, consideration of the privacy requirements needed to achieve satisfaction will result in a distinct privacy architecture. The documentation, however, may simply reflect the combined architectures.

PL-08 is primarily directed at organizations to ensure that architectures are developed for the system and, moreover, that the architectures are integrated with or tightly coupled to the enterprise architecture. In contrast, SA-17 is primarily directed at the external information technology product and system developers and integrators. SA-17, which is complementary to PL-08, is selected when organizations outsource the development of systems or components to external entities and when there is a need to demonstrate consistency with the organization's enterprise architecture and security and privacy architectures.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-160-1, 800-160-2; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CM-02, CM-06, PL-02, PL-09, PM-05, PM-07, RA-09, SA-03, SA-05, SA-08, SA-17, SC-07

PL-09 Central Management

Baselines

N/A

Overlays

Privacy

Requirements

Centrally manage organization-wide privacy common controls as designated by the agency and related processes.

Implementation Standards

Std.01 — Document organization-wide privacy common controls in Information Security Program Plan.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Central management refers to organization-wide management and implementation of selected controls and processes. This includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed controls and processes. As the central management of controls is generally associated with the concept of common (inherited) controls, such management promotes and facilitates standardization of control implementations and management and the judicious use of organizational resources. Centrally managed controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate and as part of organizational continuous monitoring.

Automated tools (e.g., security information and event management tools or enterprise security monitoring and management tools) can improve the accuracy, consistency, and availability of information associated with centrally managed controls and processes. Automation can also provide data aggregation and data correlation capabilities; alerting mechanisms; and dashboards to support risk-based decision-making within the organization.

As part of the control selection processes, organizations determine the controls that may be suitable for central management based on resources and capabilities. It is not always possible to centrally manage every aspect of a control. In such cases, the control can be treated as a hybrid control with the control managed and implemented centrally or at the system level. The controls and control enhancements that are candidates for full or partial central management include but are not limited to: AC-02(01), AC-02(02), AC-02(03), AC-02(04), AC-04 (all), AC-17(01), AC-17(02), AC-17(03), AC-17(09), AC-18(01), AC-18(03), AC-18(04), AC-18(05), AC-19(04), AC-22, AC-23, AT-02(01), AT-02(02), AT-03(01), AT-03(02), AT-03(03), AT-04, AU-03, AU-06(01), AU-06(03), AU-06(05), AU-06(06), AU-06(09), AU-07(01), AU-07(02), AU-11, AU-13, AU-16, CA-02(01), CA-02(02), CA-02(03), CA-03(01), CA-03(02), CA-03(03), CA-07(01), CA-09, CM-02(02), CM-03(01), CM-03(04), CM-04, CM-06, CM-06(01), CM-07(02), CM-07(04), CM-07(05), CM-08(all), CM-09(01), CM-10, CM-11, CP-07(all), CP-08(all), SC-43, SI-02, SI-03, SI-04(all), SI-07, SI-08.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; NIST SP 800-37

Related Controls

PL-08, PM-09

PL-10 Baseline Selection

Baselines

Low, Moderate, High

Overlays

CJIS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Select a control baseline for the system.

Implementation Standards

Std.01 — Systems must be categorized and information classified in accordance with TxDOT's Risk Management Framework, and a control baseline assigned that aligns with or exceeds the baselines in the TxDOT Information Security and Privacy Controls Standards Catalog.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PL-10.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.02 FedRAMP — Select the appropriate FedRAMP Baseline. [Source: FedRAMP Security Controls Baseline PL-10]

Discussion

Control baselines are predefined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Controls are chosen for baselines to either satisfy mandates imposed by laws, executive orders, directives, regulations, policies, standards, and guidelines or address threats common to all users of the baseline under the assumptions specific to the baseline. Baselines represent a starting point for the protection of individuals' privacy, information, and information systems with subsequent tailoring actions to manage risk in accordance with mission, business, or other constraints (see PL-11). Federal control baselines are provided in SP 800-53B. The selection of a control baseline is determined by the needs of stakeholders. Stakeholder needs consider mission and business requirements as well as mandates imposed by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. For example, the control baselines in SP 800-53B are based on the requirements from FISMA and PRIVACT. The requirements, along with the NIST standards and guidelines implementing the legislation, direct organizations to select one of the control baselines after the reviewing the information types and the information that is processed, stored, and transmitted on the system; analyzing the potential adverse impact of the loss or compromise of the information or system on the organization's operations and assets, individuals, other organizations, or the Nation; and considering the results from system and organizational risk assessments. CNSSI 1253 provides guidance on control baselines for national security systems.

TxDOT Discussion

The TxDOT Information Security and Privacy Controls Standards Catalog provides the minimum required baselines for all systems processing TxDOT data. Additional requirements derived from partnership agreements, federal standards, or other sources may apply to some systems, but cannot be considered as replacements for the TxDOT baseline; baseline tailoring (see PL-11) cannot result in a baseline lower than that provided in the TxDOT Information Security and Privacy Controls Standards Catalog for a system at the assessed categorization level.

State Implementation Details

The default baseline for an information system shall be the controls contained in the Security Controls Catalog.

The agency head may employ standards for the cost-effective information security of information, information resources, and applications within or under the supervision of that state agency that are more stringent than the standards the department prescribes under this section if the more stringent standards:

(1) contain at least the applicable standards issued by the department; and/or

(2) are consistent with applicable federal law, policies, and guidelines issued under state rule, industry standards, best practices, or deemed necessary to adequately protect the information held by the state agency.

[Source: DIR Control Standards Catalog PL-10]

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

FIPS 199, 200; NIST SP 800-30, 800-37, 800-39, 800-53B, 800-60-1, 800-60-2, 800-160-1; CNSSI 1253; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

PL-02, PL-11, RA-02, RA-03, SA-08

PL-11 Baseline Tailoring

Baselines

Low, Moderate, High

Overlays

CJIS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Tailor the selected control baseline by applying specified tailoring actions.

Implementation Standards

Std.01 — Document tailored baselines in the System Security Plan (SSP), including rationale for tailoring and any security-relevant sources.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PL-11.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

The concept of tailoring allows organizations to specialize or customize a set of baseline controls by applying a defined set of tailoring actions. Tailoring actions facilitate such specialization and customization by allowing organizations to develop security and privacy plans that reflect their specific mission and business functions, the environments where their systems operate, the threats and vulnerabilities that can affect their systems, and any other conditions or situations that can impact their mission or business success. Tailoring guidance is provided in SP 800-53B. Tailoring a control baseline is accomplished by identifying and designating common controls, applying scoping considerations, selecting compensating controls, assigning values to control parameters, supplementing the control baseline with additional controls as needed, and providing information for control implementation. The general tailoring actions in SP 800-53B can be supplemented with additional actions based on the needs of organizations. Tailoring actions can be applied to the baselines in SP 800-53B in accordance with the security and privacy requirements from FISMA, PRIVACT, and OMB A-130. Alternatively, other communities of interest adopting different control baselines can apply the tailoring actions in SP 800-53B to specialize or customize the controls that represent the specific needs and concerns of those entities.

TxDOT Discussion

Potential inputs for baseline tailoring include, but are not limited to, risk assessment results, system and component inventories, system criticality, business and privacy impact analysis, risk management strategy, and partnership agreements. Tailored baselines for a system may not be less stringent than the TxDOT Information Security and Privacy Controls Standard Baseline for the assessed categorization level.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

FIPS 199, 200; NIST SP 800-30, 800-37, 800-39, 800-53B, 800-60-1, 800-60-2, 800-160-1; CNSSI 1253; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

PL-10, RA-02, RA-03, RA-09, SA-08

PM — Program Management

PM-01 Information Security Program Plan

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS

Requirements

a. Develop and disseminate an organization-wide information security program plan that:

1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;

2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

3. Reflects the coordination among organizational entities responsible for information security; and

4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;

b. Review and update the organization-wide information security program plan annually and following major changes to legislation or security requirements; and

c. Protect the information security program plan from unauthorized disclosure and modification.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The TxDOT Executive Director or their designated representative(s) shall ensure that senior agency officials support the state agency Information Security Officer in developing, at least annually, a report on the state agency information security program, as specified in 1 TAC 202.21(b)(11) and 202.23(a). [Source: 1 TAC 202.20(b)(5)]

Std.03 — Agency Program.

a. TxDOT shall develop, document, and implement an agency-wide information security program, approved by the agency head under 1 TAC 202.20, that includes protections based on risk for all information and information resources owned, leased, or under the custodianship of any department, operating unit, or employee of the agency including outsourced resources to another agency, contractor, or other source (e.g., cloud computing). The program shall include:

1. Periodic assessments in alignment with minimum legal reporting requirements of the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information, information systems, and applications that support the operations and assets of the agency;

2. Policies, controls, standards, and procedures that:

(a) Are based on the risk assessments required by 1 TAC 202.25;

(b) Cost-effectively reduce information security risks to a level acceptable to the agency head;

(c) Ensure that information security is addressed throughout the lifecycle of agency information resources; and

(d) Ensure compliance with:

(i) The requirements of 1 TAC 202.24;

(ii) Minimally acceptable system configuration requirements as determined by the state agency; and

(iii) The control catalog published by DIR;

3. Strategies to address risk to high impact information resources;

4. Plans for providing information security for networks, facilities, and systems or groups of information systems and applications based on risk;

5. A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency; and

6. A process to justify, grant, and document any exceptions to specific program requirements in accordance with requirements and processes defined in 1 TAC 202. [Source: 1 TAC 202.24(a)]; and

b. Information Security Plan.

1. Each state agency shall develop, and periodically update, an information security plan for protecting the security of the agency's information.

2. In developing the plan, the state agency shall:

(a) Consider any vulnerability report prepared under Section 2054.077 (Vulnerability Reports) for the agency;

(b) Incorporate the network security services provided by the department to the agency under Chapter 2059 (Texas Computer Network Security System);

(c) Identify and define the responsibilities of agency staff who produce, access, use, or serve as custodians of the agency's information;

(d) Identify risk management and other measures taken to protect the agency's information from unauthorized access, disclosure, modification, or destruction;

(e) Include:

(i) The best practices for information security developed by the department; or

(ii) A written explanation of why the best practices are not sufficient for the agency's security; and

(f) Omit from any written copies of the plan information that could expose vulnerabilities in the agency's network or online systems.

3. Not later than June 1 of each even-numbered year, each state agency shall submit a copy of the agency's information security plan to the department. Subject to available resources, the department may select a portion of the submitted security plans to be assessed by the department in accordance with department rules.

4. Each state agency's information security plan is confidential and exempt from disclosure under Chapter 552.

5. Each state agency shall include in the agency's information security plan a written document that is signed by the head of the agency, the chief financial officer, and each executive manager designated by the state agency and states that those persons have been made aware of the risks revealed during the preparation of the agency's information security plan. [Source: TGC 2054.133]

Std.04 —

a. At least once every two years, TxDOT shall conduct an information security assessment of the agency's:

1. Information resources systems, network systems, digital data storage systems, digital data security measures, and information resources vulnerabilities; and

2. Data governance program with participation from the agency's data management officer, if applicable, and in accordance with requirements established by department rule.

[Source: TGC 2054.515]

b. The agency's Biennial Information Security Plan may be considered to satisfy the information security assessment requirements of Texas Government Code 2054.515(a)(1) if the agency's Biennial Information Security Plan assesses the vulnerabilities of the agency's information resources, including an evaluation determining how well the organization's security policies protect its data and information systems.

[Source: TAC 202.3(c)(1)(c)]

Std.05 — The TxDOT Executive Director or their designated representative(s) shall review and approve at least annually the agency information security program required under 1 TAC 202.24. [Source: 1 TAC 202.20(b)(7)]

Std.06 — The Information Security Officer shall be responsible for developing and maintaining an agency-wide information security plan as required by Texas Government Code Sec. 2054.133. [Source: 1 TAC 202.21(b)(1)]

Std.07 — The Information Security Officer shall be responsible for reporting, at least annually, directly to the TxDOT Executive Director the status and

effectiveness of the security program and its controls. [Source: 1 TAC 202.21(b)(11)]

Std.08 — The Information Security Officer shall be responsible for informing any relevant parties in the event of noncompliance with 1 TAC 202 and/or with the state agency's information security policies. [Source: 1 TAC 202.21(b)(12)]

Std.09 — TxDOT shall submit to the Department of Information Resources a Biennial Information Security Plan in accordance with Texas Government Code Sec. 2054.133 . [Source: 1 TAC 202.23(b)(3)]

Std.10 — A review of TxDOT's information security program for compliance with the standards in the Security Control Standards Catalog will be performed at least biennially, based on business risk management decisions, by individual(s) independent of the information security program and designated by the TxDOT Executive Director or his or her designated representative(s). [Source: 1 TAC 202.26(c)]

Std.11 — TxDOT's Chief Information Security Officer shall prepare or have prepared a report, including an executive summary of the findings of the biennial report, not later than June 01 of each even-numbered year, assessing the extent to which a computer, a computer program, a computer network, a computer system, a printer, an interface to a computer system, including mobile and peripheral devices, computer software, or data processing of the agency or of a contractor of the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use. [Source: TGC 2054.077(b)]

Std.12 — Separate from the executive summary described by TGC 2057.077(b), TxDOT shall prepare a summary of the agency's vulnerability report that does not contain any information the release of which might compromise the security of the agency's or agency contractor's computers, computer programs, computer networks, computer systems, printers, interfaces to computer systems, including mobile and peripheral devices, computer software, data processing, or electronically stored information. The summary is available to the public on request. [Source: TGC 2054.077(e)]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 12.1.1, 12.1.2, and 12.1.3.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.13 PCI — Ensure that the following is included in contracts or SLAs for service providers: Responsibility is established by executive management for the protection of cardholder data and a PCI DSS compliance program to include:

a. Overall accountability for maintaining PCI DSS compliance.

b. Defining a charter for a PCI DSS compliance program and communication to executive management.

[Source: PCI DSS 12.4.1]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement 1.3.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

An information security program plan is a formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements. An information security program plan can be represented in a single document or compilations of documents. Privacy program plans and supply chain risk management plans are addressed separately in PM-18 and SR-02, respectively.

An information security program plan documents implementation details about program management and common controls. The plan provides sufficient information about the controls (including specification of parameters for assignment and selection operations, explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended. Updates to information security program plans include organizational changes and problems identified during plan implementation or control assessments.

Program management controls may be implemented at the organization level or the mission or business process level, and are essential for

managing the organization's information security program. Program management controls are distinct from common, system-specific, and hybrid controls because program management controls are independent of any particular system. Together, the individual system security plans and the organization-wide information security program plan provide complete coverage for the security controls employed within the organization.

Common controls available for inheritance by organizational systems are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for a system. The organization-wide information security program plan indicates which separate security plans contain descriptions of common controls.

Events that may precipitate an update to the information security program plan include, but are not limited to, organization-wide assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines.

TxDOT Discussion

If the Department of Information Resources (DIR) provides network security services for TxDOT, DIR is responsible for network security from external threats for the agency. Network security management for TxDOT regarding internal threats remains the responsibility of the agency. [Source: TGC 2059.056]

The information security program plan should provide sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended. [Source: Catalog of Control Systems Security: Recommendations for Standards Developers]

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; TGC 2054; DIR Security Control Standards Catalog

Federal References

FISMA; OMB A-130; NIST SP 800-37, 800-39; PCI DSS; CJIS Security Policy

Related Controls

PL-02, PM-18, PM-30, RA-09, SA-09, SI-12, SR-02

PM-02 Information Security Program Leadership Role

Baselines

Low, Moderate, High

Overlays

PCI DSS

Requirements

Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The TxDOT Executive Director or their designated representative(s) shall designate an Information Security Officer who has the explicit authority and the duty to administer the information security requirements of 1 TAC 202 agency wide. [Source: 1 TAC 202.20(b)(1)]

Std.03 — TxDOT's Information Security Officer shall report to executive level management, has explicit authority for information security for the entire state agency, and complies with all other requirements of Texas Government Code Sec. 2054.136. [Source: 1 TAC 202.21(a)]

Std.04 — The Information Security Officer shall be responsible for:

a. Developing and maintaining information security policies and procedures that address the requirements of 1 TAC 202 and the agency's information security risks;

b. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of this chapter and the agency's information security risks; and

c. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202. [Source: 1 TAC 202.21(b)(2, 3, 5)]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 12.1.4.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

The senior agency information security officer is an organizational official. For federal agencies (as defined by applicable laws, executive orders, regulations, directives, policies, and standards), this official is the senior agency information security officer. Organizations may also refer to this official as the senior information security officer or chief information security officer.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog

Federal References

OMB M-17-25; NIST SP 800-37, 800-39, 800-181; PCI DSS

Related Controls

None.

PM-03 Information Security and Privacy Resources

Baselines

Low, Moderate, High

Overlays

Privacy

Requirements

a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;

b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and

c. Make available for expenditure, the planned information security and privacy resources.

Implementation Standards

Std.01 — The TxDOT Executive Director or their designated representative(s) shall allocate resources for ongoing information security remediation, implementation, and compliance activities that reduce risk to a level acceptable to the TxDOT Executive Director. [Source: 1 TAC 202.20(b)(2)]

Std.02 — The Information Security Officer shall directly report to the TxDOT Executive Director, at least annually, on the adequacy and effectiveness of information security policies, procedures, practices, compliance with the requirements of 1 TAC 202, and state agency information security requirements and requests. [Source: 1 TAC 202.23(a)(3)]

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Organizations consider establishing champions for information security and privacy and, as part of including the necessary resources, assign specialized expertise and resources as needed. Organizations may designate and empower an Investment Review Board or similar group to manage and provide oversight for the information security and privacy aspects of the capital planning and investment control process.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog

Federal References

OMB A-130

Related Controls

PM-04, SA-02

PM-04 Plan of Action and Milestones Process

Baselines

Low, Moderate, High

Overlays

Privacy

Requirements

a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:

1. Are developed and maintained;

2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and

3. Are reported in accordance with established reporting requirements.

b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — An agency-wide information security program must be approved by the agency head and include a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency. [Source: 1 TAC 202.24(a)(5)]

Std.03 — Reporting requirements must comply with CA-05.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

The plan of action and milestones is a key organizational document and is subject to reporting requirements established by the Office of Management and Budget. Organizations develop plans of action and milestones with an organization-wide perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. Plan of action and milestones updates are based on findings from control assessments and continuous monitoring activities. There can be multiple plans of action and milestones corresponding to the information system level, mission/business process level, and organizational/governance level. While plans of action and milestones are required for federal organizations, other types of organizations can help reduce risk by documenting and tracking planned remediations. Specific guidance on plans of action and milestones at the system level is provided in CA-05.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog

Federal References

Privacy Act; OMB A-130; NIST SP 800-37

Related Controls

CA-05, CA-07, PM-03, RA-07, SI-12

PM-05 System Inventory

Baselines

Low, Moderate, High

Overlays

N/A

Requirements

Develop and update at least annually an inventory of organizational systems.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The Information Security Officer shall be responsible for reviewing the agency's inventory of information systems and related ownership and responsibilities. [Source: 1 TAC 202.21(b)(7)]

Std.03 — Information Resources Deployment Review

a. Not later than March 31 of each even-numbered year, a state agency shall complete a review of the operational aspects of the agency's information resources deployment following instructions developed by the Department of Information Resources (DIR).

b. Except as otherwise modified by rules adopted by DIR, the review must include:

1. An inventory of the agency's major information systems, as defined by Section 2054.008 (Contract Notification), and other operational or logistical components related to deployment of information resources as prescribed by DIR;

2. An inventory of the agency's major databases and applications;

3. A description of the agency's existing and planned telecommunications network configuration;

4. An analysis of how information systems, components, databases, applications, and other information resources have been deployed by the agency in support of:

(A) Applicable achievement goals established under Section 2056.006 (Goals) and the state strategic plan adopted under Section 2056.009 (State Plan);

(B) The state strategic plan for information resources; and

(C) The agency's business objectives, mission, and goals;

5. Agency information necessary to support the state goals for interoperability and reuse; and

6. Confirmation by the agency of compliance with state statutes, rules, and standards relating to information resources.

[Source: TGC 2054.0965]

Std.04 — All TxDOT information systems must be registered when the proposed system is funded. The system inventory must identify the information owner, information custodian, and any requirements outlined in RA-02.

Std.05 — The Information Owner must annually review and validate the accuracy of information systems information for which they are the owner.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

OMB A-130 provides guidance on developing systems inventories and associated reporting requirements. System inventory refers to an organization-wide inventory of systems, not system components as described in CM-08.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; TGC 2054; DIR Security Control Standards Catalog

Federal References

NIST IR 8062; OMB A-130

Related Controls

None.

PM-05(01) Inventory of Personally Identifiable Information

Baselines

Low, Moderate, High

Overlays

Privacy

Requirements

Establish, maintain, and update at least annually an inventory of all systems, applications, and projects that process personally identifiable information.

Implementation Standards

Std.01 — Classify all TxDOT data in accordance with the TxDOT Data Classification Policy.

Std.02 — Document, in inventories and System Security Plans (SSPs), which elements of personally identifiable information (PII) the system processes.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

An inventory of systems, applications, and projects that process personally identifiable information supports the mapping of data actions, providing individuals with privacy notices, maintaining accurate personally identifiable information, and limiting the processing of personally identifiable information when such information is not needed for operational purposes. Organizations may use this inventory to ensure that systems only process the personally identifiable information for authorized purposes and that this processing is still relevant and necessary for the purpose specified therein.

TxDOT Discussion

None.

TxDOT References

Data Classification Policy; Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST IR 8062

Related Controls

AC-03, CM-08, CM-12, PL-08, PM-22, PT-03, PT-05, SI-12

PM-06 Measures of Performance

Baselines

Low, Moderate, High

Overlays

Privacy

Requirements

Develop, monitor, and report on the results of information security and privacy measures of performance.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The Information Security Officer shall be responsible for reporting, at least annually, directly to the TxDOT Executive Director the status and effectiveness of the security program and its controls. [Source: 1 TAC 202.21(b)(11)]

Std.03 — The Information Security Officer shall directly report to the TxDOT Executive Director, at least annually, on the adequacy and effectiveness of information security policies, procedures, practices, compliance with the requirements of 1 TAC 202, and the effectiveness of current information security program and status of key initiatives. [Source: 1 TAC 202.23(a)]

Std.04 — Rescinded in V3.0.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security and privacy programs and the controls employed in support of the program. To facilitate security and privacy risk management, organizations consider aligning measures of performance with the organizational risk tolerance as defined in the risk management strategy.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog

Federal References

OMB A-130; NIST SP 800-37, 800-39, 800-55, 800-137

Related Controls

CA-07, PM-09

PM-07 Enterprise Architecture

Baselines

Low, Moderate, High

Overlays

Privacy

Requirements

Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.

Implementation Standards

Std.01 — The agency's enterprise information security architecture must be aligned with Federal, State, Local and agency data security and privacy requirements. [Source: Texas Cybersecurity Framework]

Std.02 — The Information Security Program must, using a roadmap and emerging technology process, stay abreast of the continued evolution of security solutions, processes, and technology to identify continuous, ongoing ways to deliver technology and information securely. [Source: Texas Cybersecurity Framework]

Std.03 — Ensure the enterprise architecture includes models and transition plans, and aligns with the agency Information Security Plan.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

The integration of security and privacy requirements and controls into the enterprise architecture helps to ensure that security and privacy considerations are addressed throughout the system development life cycle and are explicitly related to the organization's mission and business processes. The process of security and privacy requirements integration also embeds into the enterprise architecture and the organization's security and privacy architectures consistent with the organizational risk management strategy. For PM-07, security and privacy architectures are developed at a system-of-systems level, representing all organizational systems. For PL-08, the security and privacy architectures are developed at a level that represents an individual system. The system-level architectures are consistent with the security and privacy architectures defined for the organization. Security and privacy requirements and control integration are most effectively accomplished through the rigorous application of the Risk Management Framework SP 800-37 and supporting security standards and guidelines.

TxDOT Discussion

The principles of The Open Group Architecture Framework (TOGAF), TxDOT's preferred enterprise architecture framework and methodology, must be adopted and applied across enterprise architecture planning, development, execution and enforcement. [Source: RFP Outsourced Managed Information Technology Services]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; NIST SP 800-37, 800-39, 800-160-1, 800-160-2

Related Controls

AU-06, PL-02, PL-08, PM-11, RA-02, SA-03, SA-08, SA-17

PM-08 Critical Infrastructure Plan

Baselines

Low, Moderate, High

Overlays

Privacy

Requirements

Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Implementation Standards

Std.01 — Identify all agency assets, business processes, and resources that meet the definition of critical infrastructure and document that status in applicable System Security Plans (SSPs) and COOPs.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Protection strategies are based on the prioritization of critical assets and resources. The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

EO 13636; OMB A-130; HSPD 7; DHS National Infrastructure Protection Plan

Related Controls

CP-02, CP-04, PE-18, PL-02, PM-09, PM-11, PM-18, RA-03, SI-12

PM-09 Risk Management Strategy

Baselines

Low, Moderate, High

Overlays

Privacy

Requirements

a. Develop a comprehensive strategy to manage:

1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and

2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information;

b. Implement the risk management strategy consistently across the organization; and

c. Review and update the risk management strategy annually or as required, to address organizational changes.

Implementation Standards

Std.01 — The TxDOT risk management strategy must align with NIST's Risk Management Framework and includes the TxDOT Information Security and Privacy Controls Standards Catalog.

Std.02 — Information Security Plan:

a. Each state agency shall develop, and periodically update, an information security plan for protecting the security of the agency's information. [Source: TGC 2054.133(a)]

1. Within this plan, TxDOT shall identify risk management and other measures taken to protect the agency's information from unauthorized access, disclosure, modification, or destruction. [Source: TGC 2054.133(b)(4)]

b. Not later than June 1 of each even-numbered year, TxDOT shall submit a copy of the agency's information security plan to the Department of Information Resources. [Source: TGC 2054.133(c)]

c. TxDOT's information security plan is confidential and exempt from disclosure under Chapter 552. [Source: TGC 2054.133(d)]

d. TxDOT shall include in the agency's information security plan a written document that is signed by the Executive Director, the chief financial officer, and each executive manager designated by the agency and states that those persons have been made aware of the risks revealed during the preparation of the agency's information security plan. [Source: TGC 2054.133(e)]

1. Omit from any written copies of the plan information that could expose vulnerabilities in the agency's network or online systems. [Source: TGC 2054.133(b)(6)]

Std.03 — TxDOT Information Security Risk Management Reporting:

a. TxDOT's Chief Information Security Officer shall report, at least annually, directly to the TxDOT Executive Director the status and effectiveness of the security program and its controls. [Source: 1 TAC 202.21(b)(11)]

b. The Chief Information Security Officer shall directly report to the Executive Director, at least annually, on residual risks identified by the state agency risk management process. [Source: 1 TAC 202.23(a)(2)]

c. Approval of the security risk acceptance, transference, or mitigation decision shall be the responsibility of the TxDOT Executive Director for all systems identified with a High residual risk. [Source: 1 TAC 202.25(4)(B)]

Std.04 — Vulnerability Reports:

a. TxDOT's Chief Information Security Officer shall prepare or have prepared a report, including an executive summary of the findings of the biennial report, not later than June 1 of each even-numbered year, assessing the extent to which a computer, a computer program, a computer network, a computer system, a printer, an interface to a computer system, including mobile and peripheral devices, computer software, or data processing of the agency or of a contractor of the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use. [Source: TGC 2054.077(b)]

b. Except as provided by TGC 2054.077, a vulnerability report and any information or communication prepared or maintained for use in the preparation of a vulnerability report is confidential and is not subject to disclosure under Chapter 552. [Source: TGC 2054.077(c)]

c. Separate from the executive summary described by TGC 2057.077(b), TxDOT shall prepare a summary of the agency's vulnerability report that does not contain any information the release of which might compromise the security of the agency's or agency contractor's computers, computer programs, computer networks, computer systems, printers, interfaces to computer systems, including mobile and peripheral devices, computer software, data processing, or electronically stored information. The summary is available to the public on request. [Source: TGC 2054.077(e)]

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

An organization-wide risk management strategy includes an expression of the security and privacy risk tolerance for the organization, security and privacy risk mitigation strategies, acceptable risk assessment methodologies, a process for evaluating security and privacy risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The senior accountable official for risk management (agency head or designated official) aligns information security management processes with strategic, operational, and budgetary planning processes. The risk executive function, led by the senior accountable official for risk management, can facilitate consistent application of the risk management strategy organization-wide. The risk management strategy can be informed by security and privacy risk-related inputs from other sources, both internal and external to the organization, to ensure that the strategy is broad-based and comprehensive. The supply chain risk management strategy described in PM-30 can also provide useful inputs to the organization-wide risk management strategy.

TxDOT Discussion

Elements of the risk management program include:

1. The creation of a risk management policy for information systems and paper records that is formally approved by management and includes:

a. Objectives of the risk management process;

b. Management's clearly stated level of acceptable risk, informed by its role in the critical infrastructure and business-specific risk analysis;

c. The connection between the risk management policy and the organization's strategic planning processes; and

d. Documented risk assessment processes and procedures.

2. Regular performance of risk assessments;

3. Mitigation of risks identified from risk assessments and threat monitoring procedures;

4. Risk tolerance thresholds are defined for each category of risk;

5. The plan for managing operational risk communicated to stakeholders;

6. Reassessment of the risk management policy to ensure management's stated level of acceptable risk is still accurate, previously decided upon

security controls are still applicable and effective, and to evaluate the possible risk-level changes in the environment;

7. Updating the risk management policy if any of these elements have changed; and

8. Repeating the risk management process prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually. [Source: Hitrust CSF 03.a Risk Management Program Development]

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; TGC 2054; DIR Security Control Standards Catalog

Federal References

OMB A-130; NIST SP 800-30, 800-37, 800-39, 800-161; NIST IR 8023

Related Controls

AC-01, AT-01, AU-01, CA-01, CA-02, CA-05, CA-06, CA-07, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PL-02, PM-02, PM-08, PM-18, PM-28, PM-30, PS-01, PT-01, PT-02, PT-03, RA-01, RA-03, RA-09, SA-01, SA-04, SC-01, SI-01, SI-12, SR-01, SR-02

PM-10 Authorization Process

Baselines

Low, Moderate, High

Overlays

Privacy

Requirements

a. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes;

b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and

c. Integrate the authorization processes into an organization-wide risk management program.

Implementation Standards

Std.01 — The Authorizing Official (AO) formally assumes responsibility for operating an information system at an acceptable level of risk. No system shall be deployed to an operational state in a production environment without an Authorization to Operate approved by an AO.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Authorization processes for organizational systems and environments of operation require the implementation of an organization-wide risk management process and associated security and privacy standards and guidelines. Specific roles for risk management processes include a risk executive (function) and designated authorizing officials for each organizational system and common control provider. The authorization processes for the organization are integrated with continuous monitoring processes to facilitate ongoing understanding and acceptance of security and privacy risks to organizational operations, organizational assets, individuals, other organizations, and the Nation.

TxDOT Discussion

The Authorizing Official should ensure:

1. New information processing assets (internal to the organization or via a service provided by a third party) have appropriate user management authorization of their purpose and use, and authorization is also obtained from the manager responsible for maintaining the local information system security environment to ensure that all relevant security policies and requirements are met;

2. Information assets have appropriate security measures commensurate with the type of information they will store, process or transmit;

3. The assets comply with all applicable laws, regulations, standards, policies and other applicable frameworks including the Texas Cybersecurity Risk Framework;

4. Hardware and software are checked to ensure that they are compatible with other system components; and

5. Necessary controls for the use of personal or privately-owned information processing equipment (e.g., laptops, home-computers or hand-held devices) for processing business information, which may introduce new vulnerabilities, are identified and implemented. [Source: Hitrust CSF 05.d Authorization Process for Information Assets and Facilities]

TxDOT References

Information Security and Privacy Policy

State References

Texas Cybersecurity Framework; DIR Security Control Standards Catalog

Federal References

NIST SP 800-37, 800-39, 800-181

Related Controls

CA-06, CA-07, PL-02

PM-11 Mission and Business Process Definition

Baselines

Low, Moderate, High

Overlays

Privacy

Requirements

a. Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational

operations, organizational assets, individuals, other organizations, and the Nation; and

b. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and

c. Review and revise the mission and business processes at least annually and whenever changes to the environment of operation (including threats, infrastructures, and legislation) warrant.

Implementation Standards

Std.01 — Priorities for organizational mission, objectives, and activities are established and communicated [Source: Cybersecurity Framework ID.BE-3]

Std.02 — Document mission and business process priorities in applicable System Security Plans (SSPs) and COOPs, either as Cybersecurity Framework Profiles or in another approved format.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Protection needs are technology-independent capabilities that are required to counter threats to organizations, individuals, systems, and the Nation through the compromise of information (i.e., loss of confidentiality, integrity, availability, or privacy). Information protection and personally identifiable information processing needs are derived from the mission and business needs defined by organizational stakeholders, the mission and business processes designed to meet those needs, and the organizational risk management strategy. Information protection and personally identifiable information processing needs determine the required controls for the organization and the systems. Inherent to defining protection and personally

identifiable information processing needs is an understanding of the adverse impact that could result if a compromise or breach of information occurs. The categorization process is used to make such potential impact determinations. Privacy risks to individuals can arise from the compromise of personally identifiable information, but they can also arise as unintended consequences or a byproduct of the processing of personally identifiable information at any stage of the information life cycle. Privacy risk assessments are used to prioritize the risks that are created for individuals from system processing of personally identifiable information. These risk assessments enable the selection of the required privacy controls for the organization and systems. Mission and business process definitions and the associated protection requirements are documented in accordance with organizational policies and procedures.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; FIPS 199; NIST SP 800-39, 800-60-1, 800-60-2, 800-160-1; NITP12

Related Controls

CP-02, PL-02, PM-07, PM-08, RA-02, RA-03, RA-09, SA-02

PM-12 Insider Threat Program

Baselines

Low, Moderate, High

Overlays

N/A

Requirements

Implement an insider threat program that includes a cross-discipline insider threat incident handling team.

Implementation Standards

Std.01 — Include insider threat in the incident response plan established in accordance with IR-08, including mitigation of risk, monitoring, response, and training.

Std.02 —

a. Information security events shall be reported through appropriate communications channels as quickly as possible. All employees, contractors and third-party users shall be made aware of their responsibility to report any information security events as quickly as possible. [Source: Hitrust 11.a Reporting Information Security Events]

b. Information Security Training for employees and contractors must include content on insider threat including instructions on reporting.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Organizations that handle classified information are required, under Executive Order 13587 and the National Insider Threat Policy, to establish insider threat programs. The same standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of controlled unclassified and other information in non-national security systems. Insider threat programs include controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and nontechnical information to identify potential insider threat concerns. A senior official is

designated by the department or agency head as the responsible individual to implement and provide oversight for the program. In addition to the centralized integration and analysis capability, insider threat programs require organizations to prepare department or agency insider threat policies and implementation plans, conduct host-based user monitoring of individual employee activities on government-owned classified computers, provide insider threat awareness training to employees, receive access to information from offices in the department or agency for insider threat analysis, and conduct self-assessments of department or agency insider threat posture.

Insider threat programs can leverage the existence of incident handling teams that organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace, including ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues. These precursors can guide organizational officials in more focused, targeted monitoring efforts. However, the use of human resource records could raise significant concerns for privacy. The participation of a legal team, including consultation with the senior agency official for privacy, ensures that monitoring activities are performed in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

EO 13587; ODNI National Insider Threat Policy

Related Controls

AC-06, AT-02, AU-06, AU-07, AU-10, AU-12, CA-07, IA-04, IR-04, IR-08, MP-07, PE-02, PM-14, PM-16, PS-03, PS-04, PS-05, PS-07, PS-08, SC-07, SI-04

PM-13 Security and Privacy Workforce

Baselines

Low, Moderate, High

Overlays

Privacy

Requirements

Establish a security and privacy workforce development and improvement program.

Implementation Standards

Std.01 — The TxDOT Executive Director or their designated representative(s) shall ensure that the state agency has trained personnel to assist the agency in complying with the requirements of 1 TAC 202 and related policies. [Source: 1 TAC 202.20(b)(4)]

Std.02 — Information Security, with assistance from Human Resources and other internal and external partners, shall:

a. Ensure organizational information security workforce personnel obtain and continue to meet individual qualification standards, certification, and ongoing training for their assigned organization information security roles;

b. Annually re-evaluate the organization's workforce's knowledge and skill requirements based upon current risks and threats, and organization environment changes; and

c. Prioritize requirements for the development of training content to address the organization's information security workforce gaps and deficiencies.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Security and privacy workforce development and improvement programs include defining the knowledge, skills, and abilities needed to perform security and privacy duties and tasks; developing role-based training programs for individuals assigned security and privacy roles and responsibilities; and providing standards and guidelines for measuring and building individual qualifications for incumbents and applicants for security- and privacy-related positions. Such workforce development and improvement programs can also include security and privacy career paths to encourage security and privacy professionals to advance in the field and fill positions with greater responsibility. The programs encourage organizations to fill security- and privacy-related positions with qualified personnel. Security and privacy workforce development and improvement programs are complementary to organizational security awareness and training programs and focus on developing and institutionalizing the core security and privacy capabilities of personnel needed to protect organizational operations, assets, and individuals.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog

Federal References

OMB A-130; NIST SP 800-181

Related Controls

AT-02, AT-03

PM-14 Testing, Training, and Monitoring

Baselines

Low, Moderate, High

Overlays

Privacy

Requirements

a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:

1. Are developed and maintained; and

2. Continue to be executed; and

b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

A process for organization-wide security and privacy testing, training, and monitoring helps ensure that organizations provide oversight for testing, training, and monitoring activities and that those activities are coordinated. With the growing importance of continuous monitoring programs, the implementation of information security and privacy across the three levels of the risk management hierarchy and the widespread use of common controls, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing assessments supporting a variety of controls. Security and privacy training activities, while focused on individual systems and specific roles, require coordination

across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; NIST SP 800-37, 800-39, 800-53A, 800-115, 800-137

Related Controls

AT-02, AT-03, CA-07, CP-04, IR-03, PM-12, SI-04

PM-15 Security and Privacy Groups and Associations

Baselines

Low, Moderate, High

Overlays

N/A

Requirements

Establish and institutionalize contact with selected groups and associations within the security and privacy communities:

a. To facilitate ongoing security and privacy education and training for organizational personnel;

b. To maintain currency with recommended security and privacy practices, techniques, and technologies; and

c. To share current security and privacy information, including threats, vulnerabilities, and incidents.

Implementation Standards

Std.01 — Establish a process to receive, analyze and respond to reports of software vulnerabilities, including providing a means for external entities to contact the agency's security group. [Source: CIS 16.2 and CSF RS.AN-5]

Std.02 — Establish and maintain contact information for parties that need to be informed of security incidents, such as law enforcement, relevant government departments, vendors, and Information Sharing and Analysis Center (ISAC) partners. [Source: CIS 17.2]

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Ongoing contact with security and privacy groups and associations is important in an environment of rapidly changing technologies and threats. Groups and associations include special interest groups, professional associations, forums, news groups, users' groups, and peer groups of security and privacy professionals in similar organizations. Organizations select security and privacy groups and associations based on mission and business functions. Organizations share threat, vulnerability, and incident information as well as contextual insights, compliance techniques, and privacy problems consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

TxDOT Discussion

Membership in organization-defined special interest groups or forums/services is considered as a means to:

1. Improve knowledge about best practices and staying up to date with relevant security information;

2. Ensure the understanding of the information security environment is current and complete (e.g., threat monitoring/intelligence services);

3. Receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities;

4. Gain access to specialist information security advice;

5. Share and exchange information about new technologies, products, threats, or vulnerabilities;

6. Provide suitable liaison points when dealing with information security incidents. [Source: Hitrust CSF 05.g Contact with Special Interest Groups]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130

Related Controls

SA-11, SI-05

PM-16 Threat Awareness Program

Baselines

Low, Moderate, High

Overlays

N/A

Requirements

Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.

Implementation Standards

Std.01 — Review environment of operation for indicators of compromise identified in threat intelligence alerts and advisories, and take appropriate actions per incident response plan (see IR-04).

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it may be more likely that adversaries can successfully breach or compromise organizational systems. One of the best techniques to address this concern is for organizations to share threat information, including threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, and threat intelligence (i.e., indications and warnings about threats). Threat information sharing may be bilateral or multilateral. Bilateral threat sharing includes government-to-commercial and government-to-government cooperatives. Multilateral threat sharing includes organizations taking part in threat-sharing consortia. Threat information may require special agreements and protection, or it may be freely shared.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

None.

Related Controls

IR-04, PM-12

PM-16(01) Automated Means for Sharing Threat Intelligence

Baselines

Low, Moderate, High

Overlays

N/A

Requirements

Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

To maximize the effectiveness of monitoring, it is important to know what threat observables and indicators the sensors need to be searching for. By using well-established frameworks, services, and automated tools,

organizations improve their ability to rapidly share and feed the relevant threat detection signatures into monitoring tools.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

None.

Related Controls

None.

PM-18 Privacy Program Plan

Baselines

Low, Moderate, High

Overlays

Privacy

Requirements

a. Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency's privacy program, and:

1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program;

2. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements;

3. Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities;

4. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program;

5. Reflects coordination among organizational entities responsible for the different aspects of privacy; and

6. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and

b. Update the plan biennially and to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

A privacy program plan is a formal document that provides an overview of an organization's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the senior agency official for privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks. Privacy program plans can be represented in single documents or compilations of documents.

The senior agency official for privacy is responsible for designating which privacy controls the organization will treat as program management,

common, system-specific, and hybrid controls. Privacy program plans provide sufficient information about the privacy program management and common controls (including the specification of parameters and assignment and selection operations explicitly or by reference) to enable control implementations that are unambiguously compliant with the intent of the plans and a determination of the risk incurred if the plans are implemented as intended.

Program management controls are generally implemented at the organization level and are essential for managing the organization's privacy program. Program management controls are distinct from common, system-specific, and hybrid controls because program management controls are independent of any particular information system. Together, the privacy plans for individual systems and the organization-wide privacy program plan provide complete coverage for the privacy controls employed within the organization.

Common controls are documented in an appendix to the organization's privacy program plan unless the controls are included in a separate privacy plan for a system. The organization-wide privacy program plan indicates which separate privacy plans contain descriptions of privacy controls.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

Privacy Act; OMB A-130

Related Controls

PM-08, PM-09, PM-19

PM-19 Privacy Program Leadership Role

Baselines

Low, Moderate, High

Overlays

Privacy

Requirements

Appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.

Implementation Standards

Std.01 — The TxDOT Executive Director or his or her designated representative(s) shall designate a privacy officer to administer the state organization privacy program.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

The privacy officer is an organizational official. For federal agencies—as defined by applicable laws, executive orders, directives, regulations, policies, standards, and guidelines—this official is designated as the senior agency official for privacy. Organizations may also refer to this official as the chief privacy officer. The senior agency official for privacy also has roles on the data management board (see PM-23) and the data integrity board (see PM-24).

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

OMB A-130

Related Controls

PM-18, PM-20, PM-27

PM-20 Dissemination of Privacy Program Information

Baselines

Low, Moderate, High

Overlays

Privacy

Requirements

Maintain a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that:

a. Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy;

b. Ensures that organizational privacy practices and reports are publicly available; and

c. Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

Implementation Standards

Std.01 — Include contact information and a link to the Privacy Notice or Privacy Policy on all public-facing agency websites.

Std.02 — Post the agency Privacy Notice to a publicly accessible website.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

For federal agencies, the webpage is located at www.[agency].gov/privacy. Federal agencies include public privacy impact assessments, system of records notices, computer matching notices and agreements, PRIVACT exemption and implementation rules, privacy reports, privacy policies, instructions for individuals making an access or amendment request, email addresses for questions/complaints, blogs, and periodic publications.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

Privacy Act; OMB A-130, M-17-06

Related Controls

AC-03, PM-19, PT-05, PT-07, RA-08

PM-20(01) Privacy Policies on Websites, Applications, and Digital Services

Baselines

N/A

Overlays

Privacy

Requirements

Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that:

a. Are written in plain language and organized in a way that is easy to understand and navigate;

b. Provide information needed by the public to make an informed decision about whether and how to interact with the organization; and

c. Are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.

Implementation Standards

Std.01 — TxDOT shall prominently post a link to the policy statement on a generally accessible Internet site maintained by or for the agency. [Source: TGC 2054.126(b)]

Std.02 — TxDOT's posted privacy policy shall include statements:

a. Generally allowing the use and reproduction of information on a state agency's Internet site without the state agency's permission, subject to specified conditions;

b. Generally allowing linking from a web page to a page on a state agency's Internet site without the state agency's permission, subject to specified conditions;

c. Prohibiting a state agency from charging a fee to access, use, reproduce information on, or link to its Internet site except to the extent the state agency is specifically authorized to do so by the legislature;

d. Requiring that the state agency's Internet site be credited as the source of information reproduced from the site and requiring that the date that the material was reproduced from the site be clearly stated;

e. Prohibiting a state agency from selling or releasing an e-mail address of a member of the public unless the member of the public affirmatively consents to the sale or release of the e-mail address; and

f. Specifying other policies necessary to protect from public disclosure personal information submitted by a member of the public to a state agency's Internet site to the extent the information is:

1. Confidential;

2. Excepted from the requirements of Section 552.021; or

3. Protected by other law intended to protect a person's privacy interests. [Source: TGC 2054.126(c)]

Std.03 — Ensure that links to applicable privacy policies are included on all publicly accessible agency websites.

Std.04 — Review and formally approve applicable privacy policies at least once every three years.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Organizations post privacy policies on all external-facing websites, mobile applications, and other digital services. Organizations post a link to the relevant privacy policy on any known, major entry points to the website, application, or digital service. In addition, organizations provide a link to the privacy policy on any webpage that collects personally identifiable

information. Organizations may be subject to applicable laws, executive orders, directives, regulations, or policies that require the provision of specific information to the public. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

TGC 2054

Federal References

Privacy Act; OMB A-130, M-17-06

Related Controls

None.

PM-21 Accounting of Disclosures

Baselines

Low, Moderate, High

Overlays

Privacy

Requirements

a. Develop and maintain an accurate accounting of disclosures of personally identifiable information, including:

1. Date, nature, and purpose of each disclosure; and

2. Name and address, or other contact information of the individual or organization to which the disclosure was made;

b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and

c. Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

The purpose of accounting of disclosures is to allow individuals to learn to whom their personally identifiable information has been disclosed, to provide a basis for subsequently advising recipients of any corrected or disputed personally identifiable information, and to provide an audit trail for subsequent reviews of organizational compliance with conditions for disclosures. For federal agencies, keeping an accounting of disclosures is required by the PRIVACT; agencies should consult with their senior agency official for privacy and legal counsel on this requirement and be aware of the statutory exceptions and OMB guidance relating to the provision.

Organizations can use any system for keeping notations of disclosures, if it can construct from such a system, a document listing of all disclosures along with the required information. Automated mechanisms can be used by organizations to determine when personally identifiable information is disclosed, including commercial services that provide notifications and alerts. Accounting of disclosures may also be used to help organizations verify compliance with applicable privacy statutes and policies governing the disclosure or dissemination of information and dissemination restrictions.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

Privacy Act; OMB A-130

Related Controls

AC-03, AU-02, PT-02

PM-22 Personally Identifiable Information Quality Management

Baselines

N/A

Overlays

Privacy

Requirements

Develop and document organization-wide policies and procedures for:

a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle;

b. Correcting or deleting inaccurate or outdated personally identifiable information;

c. Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; and

d. Appeals of adverse decisions on correction or deletion requests.

Implementation Standards

Std.01 — At the point of collection, to the degree feasible:

a. Collect SPI directly from the individual;

b. Confirm accuracy and completeness of data; and

c. Provide individual a privacy notice and point of contact in case of later concerns.

Std.02 — Ensure that SPI is addressed in the SDLC.

Std.03 — Review SPI for accuracy, relevance, timeliness, and completeness at least annually and before any release of SPI, and correct or delete as appropriate.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Personally identifiable information quality management includes steps that organizations take to confirm the accuracy and relevance of personally identifiable information throughout the information life cycle. The information life cycle includes the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition of personally identifiable information. Organizational policies and procedures for personally identifiable information quality management are important because inaccurate or outdated personally identifiable information maintained by organizations may cause problems for individuals. Organizations consider the quality of personally identifiable information involved in business functions where inaccurate information may result in adverse decisions or the denial of benefits and services, or the disclosure of the information may cause stigmatization. Correct information, in certain circumstances, can cause problems for individuals that outweigh the benefits of organizations maintaining the information. Organizations consider creating policies and procedures for the removal of such information.

The senior agency official for privacy ensures that practical means and mechanisms exist and are accessible for individuals or their authorized representatives to seek the correction or deletion of personally identifiable information. Processes for correcting or deleting data are clearly defined and

publicly available. Organizations use discretion in determining whether data is to be deleted or corrected based on the scope of requests, the changes sought, and the impact of the changes. Additionally, processes include the provision of responses to individuals of decisions to deny requests for correction or deletion. The responses include the reasons for the decisions, a means to record individual objections to the decisions, and a means of requesting reviews of the initial determinations.

Organizations notify individuals or their designated representatives when their personally identifiable information is corrected or deleted to provide transparency and confirm the completed action. Due to the complexity of data flows and storage, other entities may need to be informed of the correction or deletion. Notice supports the consistent correction and deletion of personally identifiable information across the data ecosystem.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

OMB A-130, M-19-15; NIST SP 800-188

Related Controls

None.

PM-23 Data Governance Body

Baselines

Low, Moderate, High

Overlays

N/A

Requirements

Establish a Data Governance Body consisting of roles defined in Std.01 with responsibilities described in Std.01.

Implementation Standards

Std.01 — Designated Data Management Officer

a. Each state agency with more than 150 full-time employees shall designate a full-time employee of the agency to serve as a data management officer.

b. The data management officer for a state agency shall:

1. Coordinate with the chief data officer to ensure the agency performs the duties assigned under Section 2054.0286 (Chief Data Officer);

2. In accordance with department guidelines, establish an agency data governance program to identify the agency's data assets, exercise authority and management over the agency's data assets, and establish related processes and procedures to oversee the agency's data assets; and

3. Coordinate with the agency's information security officer, the agency's records management officer, and the Texas State Library and Archives Commission to:

(A) Implement best practices for managing and securing data in accordance with state privacy laws and data privacy classifications;

(B) Ensure the agency's records management programs apply to all types of data storage media;

(C) Increase awareness of and outreach for the agency's records management programs within the agency; and

(D) Conduct a data maturity assessment of the agency's data governance program in accordance with the requirements established by department rule.

c. In accordance with department guidelines, the data management officer for a state agency shall post on the Texas Open Data Portal established by the department under Section 2054.070 (Central Repository for Publicly Accessible Electronic Data) at least three high-value data sets as defined by Section 2054.1265 (Posting High-value Data Sets on Internet). The high-value data sets may not include information that is confidential or protected from disclosure under state or federal law.

d. The data management officer for a state agency may delegate in writing to another agency employee the duty to:

1. Implement a specific requirement of Subsection (b) or (c); or

2. Participate in the advisory committee established under Section 2054.0332 (Data Management Advisory Committee).

[Source: TGC 2054.137]

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

A Data Governance Body can help ensure that the organization has coherent policies and the ability to balance the utility of data with security and privacy requirements. The Data Governance Body establishes policies, procedures, and standards that facilitate data governance so that data, including personally identifiable information, is effectively managed and maintained in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidance. Responsibilities can include developing and implementing guidelines that support data modeling, quality, integrity, and the de-identification needs of personally identifiable information across the information life cycle as well as reviewing and approving applications to release data outside of the organization, archiving the applications and the released data, and performing post-release monitoring to ensure that the assumptions made as part of the data release continue to be valid. Members include the chief information officer, senior agency information security officer, and senior agency official for privacy. Federal agencies are required to establish a Data Governance Body with specific roles and responsibilities in accordance with the EVIDACT and policies set forth under OMB M-19-23.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

TGC 2054

Federal References

Evidence Act; OMB A-130, OMB M-19-23; SP 800-188

Related Controls

AT-02, AT-03, PM-19, PM-22, PT-07, SI-04, SI-19

PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research

Baselines

Low, Moderate, High

Overlays

Privacy

Requirements

a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;

b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;

c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and

d. Review and update policies and procedures at the frequencies specified in Std.02.

Implementation Standards

Std.01 — Ensure that test plan documentation includes rationale for use of sensitive personal information (SPI), risk minimization techniques, and removal of SPI at the conclusion of tests.

Std.02 — Review, and update as required:

a. Policies every three years; and

b. Procedures annually.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

The use of personally identifiable information in testing, research, and training increases the risk of unauthorized disclosure or misuse of such information. Organizations consult with the senior agency official for privacy and/or legal counsel to ensure that the use of personally identifiable information in testing, training, and research is compatible with the original purpose for which it was collected. When possible, organizations use placeholder data to avoid exposure of personally identifiable information when conducting testing, training, and research.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

OMB A-130

Related Controls

PT-03, SA-03, SA-08, SI-12

PM-26 Complaint Management

Baselines

N/A

Overlays

Privacy

Requirements

Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes:

a. Mechanisms that are easy to use and readily accessible by the public;

b. All information necessary for successfully filing complaints;

c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within 60 days;

d. Acknowledgement of receipt of complaints, concerns, or questions from individuals within a time period not to exceed five business days; and

e. Response to complaints, concerns, or questions from individuals within a time period not to exceed 10 days.

Implementation Standards

Std.01 — Designate one mailing address and one e-mail address for receiving complaints, concerns, and questions from individuals about privacy practices. Ensure that information is posted on public websites and physical signs to be placed in areas of facilities open to the public.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Complaints, concerns, and questions from individuals can serve as valuable sources of input to organizations and ultimately improve operational models, uses of technology, data collection practices, and controls. Mechanisms that can be used by the public include telephone hotline, email, or web-based forms. The information necessary for successfully filing complaints includes contact information for the senior agency official for privacy or other official designated to receive complaints. Privacy complaints may also include personally identifiable information which is handled in accordance with relevant policies and processes.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

OMB A-130

Related Controls

IR-07, PM-22

PM-27 Privacy Reporting

Baselines

Low, Moderate, High

Overlays

Privacy

Requirements

a. Develop privacy reports as defined in state legislation and the privacy policy and disseminate to:

1. Oversight bodies as specified in state legislation and the privacy policy to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and

2. Officials as defined in the privacy policy and other personnel with responsibility for monitoring privacy program compliance; and

b. Review and update privacy reports at least biennially.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Through internal and external reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting can also help organizations to determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, discover vulnerabilities, identify gaps in policy and implementation, and identify models for success. For federal agencies, privacy reports include annual senior agency official for privacy reports to OMB, reports to Congress required by Implementing Regulations of the 9/11 Commission Act, and other public reports required by law, regulation, or policy, including internal policies of organizations. The senior

agency official for privacy consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

FISMA; OMB A-108, A-130

Related Controls

PM-19

PM-28 Risk Framing

Baselines

Low, Moderate, High

Overlays

Privacy

Requirements

a. Identify and document:

1. Assumptions affecting risk assessments, risk responses, and risk monitoring;

2. Constraints affecting risk assessments, risk responses, and risk monitoring;

3. Priorities and trade-offs considered by the organization for managing risk; and

4. Organizational risk tolerance;

b. Distribute the results of risk framing activities to personnel as identified in the Information Security and Privacy policy; and

c. Review and update risk framing considerations annually.

Implementation Standards

Std.01 — Require that senior leaders/executives, in consultation and collaboration with the risk executive (function), define the organizational risk frame including the types of risk decisions (e.g., risk responses) supported, how and under what conditions risk is assessed to support those risk decisions, and how risk is monitored (e.g., to what level of detail, in what form, and with what frequency). [Source: SP 800-39]

Std.02 — Document the results of risk framing exercises in the TxDOT Risk Management Framework.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Risk framing is most effective when conducted at the organization level and in consultation with stakeholders throughout the organization including mission, business, and system owners. The assumptions, constraints, risk tolerance, priorities, and trade-offs identified as part of the risk framing process inform the risk management strategy, which in turn informs the conduct of risk assessment, risk response, and risk monitoring activities. Risk framing results are shared with organizational personnel, including mission and business owners, information owners or stewards, system owners, authorizing officials, senior agency information security officer, senior agency official for privacy, and senior accountable official for risk management.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

OMB A-130; NIST SP 800-39

Related Controls

CA-07, PM-09, RA-03, RA-07

PM-30 Supply Chain Risk Management Strategy

Baselines

Low, Moderate, High

Overlays

N/A

Requirements

a. Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;

b. Implement the supply chain risk management strategy consistently across the organization; and

c. Review and update the supply chain risk management strategy on an annual basis or as required, to address organizational changes.

Implementation Standards

Std.01 — The TxDOT supply chain risk management strategy must align with NIST's Risk Management Framework, and includes the TxDOT Information Security and Privacy Controls Standards Catalog.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

An organization-wide supply chain risk management strategy includes an unambiguous expression of the supply chain risk appetite and tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the supply chain risk management strategy, and the associated roles and responsibilities. Supply chain risk management includes considerations of the security and privacy risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services. The supply chain risk management strategy can be incorporated into the organization's overarching risk management strategy and can guide and inform supply chain policies and system-level supply chain risk management plans. In addition, the use of a risk executive function can facilitate a consistent, organization-wide application of the supply chain risk management strategy. The supply chain risk management strategy is implemented at the organization and mission/business levels, whereas the supply chain risk management plan (see SR-02) is implemented at the system level.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

Privacy Act; Secure Technology Act; 41 CFR 201; EO 13873; OMB A-130, M-17-06; ISO 27036, I20243; NIST SP 800-161; NIST IR 8272; CNSSD 505

Related Controls

CM-10, PM-09, SR-01, SR-02, SR-03, SR-04, SR-05, SR-06, SR-08, SR-09, SR-11

PM-30(01) Suppliers of Critical or Mission-Essential Items

Baselines

Low, Moderate, High

Overlays

N/A

Requirements

Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

The identification and prioritization of suppliers of critical or mission-essential technologies, products, and services is paramount to the

mission/business success of organizations. The assessment of suppliers is conducted using supplier reviews (see SR-06) and supply chain risk assessment processes (see RA-03(01)). An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

Privacy Act; Secure Technology Act; 41 CFR 201; EO 13873; OMB A-130, M-17-06; ISO 27036, 20243; NIST SP 800-161; NIST IR 8272

Related Controls

RA-03, SR-06

PM-31 Continuous Monitoring Strategy

Baselines

Low, Moderate, High

Overlays

Privacy

Requirements

Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include:

a. Establishing the following organization-wide metrics to be monitored: metrics defined in the Continuous Monitoring Program;

b. Establishing frequencies as specified in the Continuous Monitoring Program for monitoring and frequencies as specified in the program's requirement documents for assessment of control effectiveness;

c. Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy;

d. Correlation and analysis of information generated by control assessments and monitoring;

e. Response actions to address results of the analysis of control assessment and monitoring information; and

f. Reporting the security and privacy status of organizational systems to personnel or roles as defined in Stds.02 & 03 at the frequency defined in Stds.02 & 03.

Implementation Standards

Std.01 — The TxDOT Continuous Monitoring Program must align with NIST's Risk Management Framework, and includes the TxDOT Information Security and Privacy Controls Catalog.

Std.02 — The Information Security Officer shall be responsible for reporting, at least annually, directly to the TxDOT Executive Director the status and effectiveness of the security program and its controls. [Source: 1 TAC 202.21(b)(11)]

Std.03 — The Information Security Officer shall report, at least annually, to the TxDOT Executive Director on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of 1 TAC 202 and the effectiveness of current information security program and status of key initiatives. [Source: 1 TAC 202.23(a), (a)(1)]

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Continuous monitoring at the organization level facilitates ongoing awareness of the security and privacy posture across the organization to support organizational risk management decisions. The terms "continuous" and "ongoing" imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. The results of continuous monitoring guide and inform risk response actions by organizations. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security- and privacy-related information on a continuing basis through reports and dashboards gives organizational officials the capability to make effective, timely, and informed risk management decisions, including ongoing authorization decisions. To further facilitate security and privacy risk management, organizations consider aligning organization-defined monitoring metrics with organizational risk tolerance as defined in the risk management strategy. Monitoring requirements, including the need for monitoring, may be referenced in other controls and control enhancements such as, AC-02g, AC-02(07), AC-02(12)(a), AC-02(07)(b), AC-02(07)(c), AC-17(01), AT-04a, AU-13, AU-13(01), AU-13(02), CA-07, CM-03f, CM-06d, CM-11c, IR-05, MA-02b, MA-03a, MA-04a, PE-03d, PE-06, PE-14b, PE-16, PE-20, PM-06, PM-23, PS-07e, SA-09c, SC-05(03)(b), SC-07a, SC-07(24)(b), SC-18b, SC-43b, SI-04.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202

Federal References

NIST SP 800-37, 800-39, 800-137, 800-137A

Related Controls

AC-02, AC-06, AC-17, AT-04, AU-06, CA-02, CA-05, CA-06, CA-07, CM-03, CM-04, CM-06, CM-11, IA-05, IR-05, MA-02, MA-03, MA-04, PE-03, PE-06, PE-14, PE-16, PL-02, PM-04, PM-06, PM-09, PM-10, PM-12, PM-14, PM-28,

PS-07, PT-07, RA-03, RA-05, RA-07, SA-09, SA-11, SC-05, SC-07, SC-18, SI-03, SI-04, SI-12, SR-02, SR-04

PM-32 Purposing

Baselines

Low, Moderate, High

Overlays

N/A

Requirements

Analyze all systems or system components under configuration management supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose.

Implementation Standards

Std.01 — Review system security plans (SSPs) to ensure that all systems and system components have sufficient capacity and are appropriately protected based on risk.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Systems are designed to support a specific mission or business function. However, over time, systems and system components may be used to support services and functions that are outside of the scope of the intended mission or business functions. This can result in exposing information resources to unintended environments and uses that can significantly increase threat exposure. In doing so, the systems are more vulnerable to

compromise, which can ultimately impact the services and functions for which they were intended. This is especially impactful for mission-essential services and functions. By analyzing resource use, organizations can identify such potential exposures.

TxDOT Discussion

Initial authorization to operate is based on evidence available at one point in time, but systems and environments of operation change. Ongoing assessment of security control effectiveness supports a system's security authorization over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Through Information Security Continuous Monitoring (ISCM), new threat or vulnerability information is evaluated as it becomes available, permitting organizations to make adjustments to security requirements or individual controls as needed to maintain authorization decisions. [Source: SP 800-137 2.2 Ongoing System Authorizations]

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

NIST SP 800-160-1, 800-160-2

Related Controls

CA-07, PL-02, RA-03, RA-09

PS — Personnel Security

PS-01 Policy and Procedures

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level personnel security policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;

b. Designate a senior management official as defined in the personnel security policy to manage the development, documentation, and dissemination of the personnel security policy and procedures; and

c. Review and update the current personnel security:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Review and update the current personnel security policy and procedures following assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. [Source: CJIS PS-01]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Personnel security policy and procedures for the controls in the PS family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may

obviate the need for mission level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to personnel security policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-12, 800-30, 800-39, 800-100; FedRAMP Security Controls Baseline

Related Controls

PM-09, PS-08, SI-12

PS-02 Position Risk Designation

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Assign a risk designation to all organizational positions;

b. Establish screening criteria for individuals filling those positions; and

c. Review and update position risk designations annually, when the position is updated, and when the position is vacated.

Implementation Standards

Std.01 — Rescinded in V2.4.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PS-02.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Position risk designations reflect Office of Personnel Management (OPM) policy and guidance. Proper position designation is the foundation of an effective and consistent suitability and personnel security program. The Position Designation System (PDS) assesses the duties and responsibilities of a position to determine the degree of potential damage to the efficiency or integrity of the service due to misconduct of an incumbent of a position and establishes the risk level of that position. The PDS assessment also determines if the duties and responsibilities of the position present the potential for position incumbents to bring about a material adverse effect on national security and the degree of that potential effect, which establishes the sensitivity level of a position. The results of the assessment determine what level of investigation is conducted for a position. Risk designations can guide and inform the types of authorizations that individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements. Parts 1400 and 731 of Title 5, Code of Federal Regulations,

establish the requirements for organizations to evaluate relevant covered positions for a position sensitivity and position risk designation commensurate with the duties and responsibilities of those positions.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

5 CFR 731; NIST SP 800-181; FedRAMP Security Controls Baseline

Related Controls

AC-05, AT-03, PE-02, PE-03, PL-02, PS-03, PS-06, SA-05, SI-12

PS-03 Personnel Screening

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Screen individuals prior to authorizing access to the system; and

b. Rescreen individuals in accordance with rescreening conditions defined in Human Resources policies and procedures, and, where rescreening is indicated, before access is granted for any new or changed role.

Implementation Standards

Std.01 — Rescinded in V2.2.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 12.7.1.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.02 CJIS —

a. To properly screen, state of residency and national fingerprint-based record checks shall be conducted. National fingerprint-based record checks must be conducted pursuant to an FBI approved authority such as a federal statute or a state statute approved pursuant to Public Law 92-544. If the person resides in a different state than that of the assigned agency, the agency shall also conduct state (of the agency) record checks. When appropriate, the screening shall be consistent with:

1. 5 CFR 731.106; and/or

2. Office of Personnel Management policy, regulations, and guidance; and/or

3. agency policy, regulations, and guidance.

Agencies authorized to bypass state repositories in compliance with federal law must only conduct a national fingerprint-based record check.

Agencies without approved statutory authority authorizing or requiring civil fingerprint-based record checks on personnel with access to CHRI are exempt from this requirement until such time as appropriate statutory authority is obtained to conduct such record checks.

b. All requests for access shall be made as specified by the CSO, Authorized Recipient Official, or IA Official. The CSO/designee, Authorized Recipient Official/designee, or IA Official is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency. All Authorized Recipient designees shall be employed by the Authorized Recipient Agency.

c. If a criminal history record of any kind exists, access to CJI shall not be granted until the CSO/designee, Authorized Recipient Official/designee, or IA Official reviews the matter to determine if access is appropriate.

1. If a felony conviction of any kind exists, the agency shall deny access to CJI. However, the requesting agency may ask for a review by the CSO/designee, Authorized Recipient Official/designee, or IA Official in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

2. Applicants with a record of misdemeanor offense(s) may be granted access if the CSO/designee, Authorized Recipient Official/designee, or IA Official, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The requesting agency may request the CSO/designee, Authorized Recipient Official/designee, or IA Official review a denial of access determination.

3. If a criminal history record of any kind is found on a contractor, the CA shall be formally notified of continuing fitness determination and system access shall be delayed pending review of the criminal history record information. The CA shall in turn notify the contractor's security officer.

d. If the person appears to be a fugitive or has an arrest history without conviction, the CSO/designee, Authorized Recipient Official/designee, or IA Official shall review the matter to determine if access to CJI is appropriate.

e. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO/designee, Authorized Recipient Official/designee, or IA Official. This does not implicitly grant hiring/firing authority with the CSA, Authorized Recipient, or IA Official only the authority to grant access to CJI. For offenses other than felonies, the CSO/designee, Authorized Recipient Official/designee, or IA Official has the latitude to delegate continued access determinations.

f. If the CSO/designee, Authorized Recipient Official/designee, or IA Official determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.

g. The criminal and non-criminal justice agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the CSO/designee, Authorized Recipient Official/designee, or IA Official. [Source: CJIS PS-03]

Std.04 CJIS —Recommend rescreening individuals in accordance with PS-3(a)(1) above. The authority authorized for the national fingerprint-based background check must also authorize the rescreening. [Source: CJIS PS-03]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.03 FedRAMP — Rescreen individuals in accordance with the following:

a. For national security clearances; a reinvestigation is required during the fifth (5th) year for top secret security clearance, the tenth (10th) year for secret security clearance, and fifteenth (15th) year for confidential security clearance.

b. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the fifth (5th) year.

c. There is no reinvestigation for other moderate risk positions or any low risk positions.

[Source: FedRAMP Security Controls Baseline PS-3]

Discussion

Personnel screening and rescreening activities reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and specific criteria established for the risk designations of assigned positions. Examples of personnel screening include background investigations and agency checks. Organizations may define different rescreening conditions and frequencies for personnel accessing systems based on types of information processed, stored, or transmitted by the systems.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

EO 13526, 13587; FIPS 199, 201; NIST SP 800-60-1, 800-60-2, 800-73-4, 800-76-2, 800-78-4; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-02, IA-04, MA-05, PE-02, PM-12, PS-02, PS-06, PS-07

PS-03(03) Information Requiring Special Protective Measures

Baselines

N/A

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

Verify that individuals accessing a system processing, storing, or transmitting information requiring special protection:

a. Have valid access authorizations that are demonstrated by assigned official government duties; and

b. Satisfy personnel screening criteria – as required by specific information.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organizational information that requires special protection includes controlled unclassified information. Personnel security criteria include position sensitivity background screening requirements.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

PS-04 Personnel Termination

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Upon termination of individual employment:

a. Disable system access within one working day for voluntary terminations, and as soon as possible, but no later than four hours of any involuntary termination;

b. Terminate or revoke any authenticators and credentials associated with the individual;

c. Conduct exit interviews that include a discussion of all security constraints and continued obligations under non-disclosure, confidentiality, user access agreements, and applicable regulations;

d. Retrieve all security-related organizational system-related property; and

e. Retain access to organizational information and systems formerly controlled by the terminated individual.

Implementation Standards

Std.01 — TxDOT, upon termination of individual employment, must terminate information system access, retrieve all organizational information system-related property, and provide appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 8.2.5.

CJIS Correspondence

Std.02 CJIS —Rescinded in V4.0.

For systems processing CJIS data, PS-04a is superseded by the corresponding CJIS requirement:

Std.05 CJIS — Disable system access within twenty-four (24) hours.. [Source: CJIS PS-04]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low or Moderate baselines, the following standard applies:

Std.03 FedRAMP — Disable system access within four (4) hours. [Source: FedRAMP Security Controls Baseline PS-4]

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.04 FedRAMP — Disable system access within one (1) hour. [Source: FedRAMP Security Controls Baseline PS-4]

Discussion

System property includes hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. Security topics at exit interviews include reminding individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not always be possible for some individuals, including in cases related to the unavailability of supervisors, illnesses, or job abandonment. Exit interviews are important for individuals with security clearances. The timely execution of termination actions is essential for individuals who have been terminated for cause. In certain situations, organizations consider disabling the system accounts of individuals who are being terminated prior to the individuals being notified.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-02, IA-04, PE-02, PM-12, PS-06, PS-07

PS-04(02) Automated Actions

Baselines

High

Overlays

FedRAMP High

Requirements

Use automated mechanisms as identified in applicable System Security Plans (SSPs) to notify personnel or roles identified in the SSP of individual termination actions.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Std.01 CJIS — Rescinded in v4.0.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

In organizations with many employees, not all personnel who need to know about termination actions receive the appropriate notifications, or if such notifications are received, they may not occur in a timely manner. Automated mechanisms can be used to send automatic alerts or notifications to organizational personnel or roles when individuals are terminated. Such automatic alerts or notifications can be conveyed in a variety of ways, including via telephone, electronic mail, text message, or websites. Automated mechanisms can also be employed to quickly and thoroughly disable access to system resources after an employee is terminated.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

None.

PS-05 Personnel Transfer

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;

b. Initiate reassignment actions to ensure all system access no longer required is removed or disabled within 24 hours following the formal transfer action;

c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. Notify personnel identified in System Security Plans (SSPs) within 24 hours if not otherwise defined in policy.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Require re-authorization for privileged access, to ensure such access is only granted where appropriate for the new role and responsibilities.

Std.03 — Ensure facility access codes, if used, are modified to prevent misuse by personnel no longer require access.

Std.04 — Collect system-related property no longer required for personnel in new positions.

Std.05 — User access authorization shall be appropriately modified or removed when the user's employment or job responsibilities within the state agency change. [Source: DIR Control Standards Catalog PS-5]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PS-05.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Personnel transfer applies when reassignments or transfers of individuals are permanent or of such extended duration as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include returning old and issuing new keys, identification cards, and building passes; closing system accounts and establishing new accounts; changing system access authorizations (i.e., privileges); and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-02, IA-04, PE-02, PM-12, PS-04, PS-07

PS-06 Access Agreements

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop and document access agreements for organizational systems;

b. Review and update the access agreements annually; and

c. Verify that individuals requiring access to organizational information and systems:

1. Sign appropriate access agreements prior to being granted access; and

2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or at least annually.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Develop a data use agreement (DUA)/Acceptable Use Agreement for use by the agency that meets the particular needs of the agency and is consistent with rules adopted by the Department of Information Resources that relate to information security standards for state agencies.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Verify that individuals requiring access to organizational information and systems re-sign access agreements when signatories change.[Source: CJIS PS-06]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline

Related Controls

AC-17, PE-02, PL-04, PS-02, PS-03, PS-07, PS-08, SI-12

PS-07 External Personnel Security

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Establish personnel security requirements, including security roles and responsibilities for external providers;

b. Require external providers to comply with personnel security policies and procedures established by the organization;

c. Document personnel security requirements;

d. Require external providers to notify personnel as identified in contracts or System Security Plans (SSPs) of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within 24 hours; and

e. Monitor provider compliance with personnel security requirements.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Ensure that contractors receive appropriate security and privacy awareness training and agree to comply with organizational policies (see AT-02).

Std.03 — Include personnel security requirements, including screening, training, and compliance, in contract language.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PS-07.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low or Moderate baselines, the following standard applies:

Std.04 FedRAMP — Require external providers to notify including access control personnel responsible for the system and/or facilities, as appropriate of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within twenty-four (24) hours. [Source: FedRAMP Security Controls Baseline PS-7]

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.05 FedRAMP — Require external providers to notify including access control personnel responsible for the system and/or facilities, as appropriate of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within the following time periods:

a. Terminations: immediately;

b. Transfers: within twenty-four (24) hours.

[Source: FedRAMP Security Controls Baseline PS-7]

Discussion

External provider refers to organizations other than the organization operating or acquiring the system. External providers include service bureaus, contractors, and other organizations that provide system development, information technology services, testing or assessment services, outsourced applications, and network/security management. Organizations explicitly include personnel security requirements in acquisition-related documents. External providers may have personnel working at organizational facilities with credentials, badges, or system privileges issued by organizations. Notifications of external personnel changes ensure the appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include functions, roles, and the nature

of credentials or privileges associated with transferred or terminated individuals.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-35, 800-63-3; FedRAMP Security Controls Baseline

Related Controls

AT-02, AT-03, MA-05, PE-03, PS-02, PS-03, PS-04, PS-05, PS-06, SA-05, SA-09

PS-08 Personnel Sanctions

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and

b. Notify personnel or roles as defined in the personnel security policy within 24 hours when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Implementation Standards

Std.01 — Rescinded in V2.2.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PS-08.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Organizational sanctions reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Sanctions processes are described in access agreements and can be included as part of general personnel policies for organizations and/or specified in security and privacy policies. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PL-04, PM-01, PM-12, PS-01, PS-06, PT-01, RA-01, SA-01, SC-01, SI-01, SR-01

PS-09 Position Descriptions

Baselines

Low, Moderate, High

Overlays

CJIS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Incorporate security and privacy roles and responsibilities into organizational position descriptions.

Implementation Standards

Std.01 — Include in position descriptions security and privacy roles in accordance with the access control policy and account management procedures (see AC-02).

Std.02 — Ensure that position roles are tagged for appropriate role-based training (see AT-03).

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement PS-09.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Specification of security and privacy roles in individual organizational position descriptions facilitates clarity in understanding the security or privacy responsibilities associated with the roles and the role-based security and privacy training requirements for the roles.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

NIST SP 800-181; FedRAMP Security Controls Baseline

Related Controls

AC-02, AT-03

PT — Personally Identifiable Information Processing and Transparency

PT-01 Policy and Procedures

Baselines

N/A

Overlays

Privacy

Requirements

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level personally identifiable information processing and transparency policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;

b. Designate a senior management official as defined in the personally identifiable information processing and transparency policy to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; and

c. Review and update the current personally identifiable information processing and transparency:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — Security requirements shall be identified, documented, and addressed in all phases of personally identifiable information processing and transparency.

Std.02 — The Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Personally identifiable information processing and transparency policy and procedures address the controls in the PT family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that

security and privacy programs collaborate on the development of personally identifiable information processing and transparency policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to personally identifiable information processing and transparency policy and procedures include assessment or audit findings, breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202

Federal References

OMB A-130

Related Controls

None.

PT-02 Authority to Process Personally Identifiable Information

Baselines

N/A

Overlays

Privacy

Requirements

a. Determine and document the authority, as determined in the privacy impact assessments (PIAs), that permits the collection, use, maintenance, or transmission (either generally or in support of a specific program or information system need) of personally identifiable information; and

b. Restrict the collection, use, maintenance, or transmission of personally identifiable information to only that which is authorized.

Implementation Standards

Std.01 — TxDOT shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business. [Source: TBC 521.052(a)]

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

The processing of personally identifiable information is an operation or set of operations that the information system or organization performs with respect to personally identifiable information across the information life cycle. Processing includes but is not limited to creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal. Processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining.

Organizations may be subject to laws, executive orders, directives, regulations, or policies that establish the organization’s authority and

thereby limit certain types of processing of personally identifiable information or establish other requirements related to the processing. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such authority, particularly if the organization is subject to multiple jurisdictions or sources of authority. For organizations whose processing is not determined according to legal authorities, the organization's policies and determinations govern how they process personally identifiable information. While processing of personally identifiable information may be legally permissible, privacy risks may still arise. Privacy risk assessments can identify the privacy risks associated with the authorized processing of personally identifiable information and support solutions to manage such risks.

Organizations consider applicable requirements and organizational policies to determine how to document this authority. For federal agencies, the authority to process personally identifiable information is documented in privacy policies and notices, system of records notices, privacy impact assessments, PRIVACT statements, computer matching agreements and notices, contracts, information sharing agreements, memoranda of understanding, and other documentation.

Organizations take steps to ensure that personally identifiable information is only processed for authorized purposes, including training organizational personnel on the authorized processing of personally identifiable information and monitoring and auditing organizational use of personally identifiable information.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

TBC 521

Federal References

Privacy Act; OMB A-130; NIST IR 8112

Related Controls

AC-02, AC-03, PM-09, PT-01, PT-03, PT-05, RA-03, RA-08, SI-12

PT-03 Personally Identifiable Information Processing Purposes

Baselines

N/A

Overlays

Privacy

Requirements

a. Identify and document the purpose(s) as defined in PT-05 for processing personally identifiable information;

b. Describe the purpose(s) in the public privacy notices and policies of the organization;

c. Restrict the processing as defined in PT-02 of personally identifiable information to only that which is compatible with the identified purpose(s); and

d. Monitor changes in processing personally identifiable information and implement mechanisms as defined in System Security Plans (SSPs) to ensure that any changes are made in accordance with requirements as defined in the privacy policy.

Implementation Standards

Std.01 — Assess the privacy risk to individuals resulting from the collection of the sensitive personal information (SPI) to be collected for the processing purposes. Document this assessment in the privacy impact assessment (PIA) for each system or application.

Std.02 — Review and update PIAs as required as part of the authority to operate process (ATO).

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Identifying and documenting the purpose for processing provides organizations with a basis for understanding why personally identifiable information may be processed. The term "process" includes every step of the information life cycle, including creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal. Identifying and documenting the purpose of processing is a prerequisite to enabling owners and operators of the system and individuals whose information is processed by the system to understand how the information will be processed. This enables individuals to make informed decisions about their engagement with information systems and organizations and to manage their privacy interests. Once the specific processing purpose has been identified, the purpose is described in the organization’s privacy notices, policies, and any related privacy compliance documentation, including privacy impact assessments, system of records notices, PRIVACT statements, computer matching notices, and other applicable Federal Register notices.

Organizations take steps to help ensure that personally identifiable information is processed only for identified purposes, including training organizational personnel and monitoring and auditing organizational processing of personally identifiable information.

Organizations monitor for changes in personally identifiable information processing. Organizational personnel consult with the senior agency official for privacy and legal counsel to ensure that any new purposes that arise from changes in processing are compatible with the purpose for which the information was collected, or if the new purpose is not compatible, implement mechanisms in accordance with defined requirements to allow for the new processing, if appropriate. Mechanisms may include obtaining consent from individuals, revising privacy policies, or other measures to manage privacy risks that arise from changes in personally identifiable information processing purposes.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

Privacy Act; OMB A-130; NIST IR 8112

Related Controls

AC-02, AC-03, AT-03, PM-09, PM-25, PT-02, PT-05, PT-07, RA-08, SI-12

PT-04 Consent

Baselines

N/A

Overlays

Privacy

Requirements

Implement tools or mechanisms for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making.

Implementation Standards

Std.01 —

a. Except as provided by Subsection (b), a state agency may not:

1. Use global positioning system technology, individual contact tracing, or technology designed to obtain biometric identifiers to acquire information that alone or in conjunction with other information identifies an individual or the individual's location without the individual's written or electronic consent;

2. Retain information with respect to an individual described by Subdivision (1) without the individual's written or electronic consent; or

3. Disseminate to a person the information described by Subdivision (1) with respect to an individual unless the state agency first obtains the individual's written or electronic consent.

b. A state agency may acquire, retain, and disseminate information described by Subsection (a) with respect to an individual without the individual's written or electronic consent if the acquisition, retention, or dissemination is:

1. Required or permitted by a federal statute or by a state statute other than Chapter 552; or

2. Made by or to a law enforcement agency for a law enforcement purpose.

c. A state agency shall retain the written or electronic consent of an individual obtained as required under this section in the agency's records until the contract or agreement under which the information is acquired, retained, or disseminated expires. [Source: TGC 2062.002]

Std.02 — Ensure that consent is:

a. Explicit; and

b. Auditable.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Consent allows individuals to participate in making decisions about the processing of their information and transfers some of the risk that arises from the processing of personally identifiable information from the organization to an individual. Consent may be required by applicable laws, executive orders, directives, regulations, policies, standards, or guidelines.

Otherwise, when selecting consent as a control, organizations consider whether individuals can be reasonably expected to understand and accept the privacy risks that arise from their authorization. Organizations consider whether other controls may more effectively mitigate privacy risk either alone or in conjunction with consent. Organizations also consider any demographic or contextual factors that may influence the understanding or behavior of individuals with respect to the processing carried out by the system or organization. When soliciting consent from individuals, organizations consider the appropriate mechanism for obtaining consent, including the type of consent (e.g., opt-in, opt-out), how to properly authenticate and identity proof individuals and how to obtain consent through electronic means. In addition, organizations consider providing a mechanism for individuals to revoke consent once it has been provided, as appropriate. Finally, organizations consider usability factors to help individuals understand the risks being accepted when providing consent, including the use of plain language and avoiding technical jargon.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

TGC 2062; TGC 552

Federal References

Privacy Act; OMB A-130; NIST SP 800-63-3

Related Controls

PT-02, PT-05

PT-05 Privacy Notice

Baselines

N/A

Overlays

Privacy

Requirements

Provide notice to individuals about the processing of personally identifiable information that:

a. Is available to individuals upon first interacting with an organization, and subsequently at least annually and whenever an individual updates sensitive personal information (SPI);

b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language;

c. Identifies the authority that authorizes the processing of personally identifiable information;

d. Identifies the purposes for which personally identifiable information is to be processed; and

e. Includes information as defined in Std.01.

Implementation Standards

Std.01 — TxDOT's Privacy Notice must include, at a high level suitable for the public:

a. A description of agency activities that impact privacy including its collection, use, sharing, safeguarding, maintenance and disposal of SPI;

1. The SPI the agency collects;

2. The routine uses of SPI;

3. Whether the agency shares SPI externally, and if so, the purposes of that sharing; and

4. How the agency protects SPI.

b. Authority for collecting SPI;

c. The choices individuals may have regarding how the organization uses and shares SPI;

1. Whether individuals have the ability to consent to specific uses or sharing of SPI and, if so, how to exercise any such consent;

2. Whether individuals can rescind specific consent;

3. How to access and update SPI: and

4. How to request SPI be deleted.

d. The consequences of not supplying requested information; and

e. Contact information in case of questions, complaints, and concerns.

Std.02 — Revise the public Privacy Notice to reflect changes in practice or policy that affect SPI or changes in activities that impact privacy before or as soon as feasible after such changes.

Std.03 — Provide direct notice to individuals by means of Privacy Notices on the forms (electronic or hardcopy) used to collect SPI, or on separate forms that can be retained by the individuals.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Privacy notices help inform individuals about how their personally identifiable information is being processed by the system or organization. Organizations use privacy notices to inform individuals about how, under what authority, and for what purpose their personally identifiable information is processed, as well as other information such as choices individuals might have with respect to that processing and other parties with whom information is shared. Laws, executive orders, directives, regulations, or policies may require that privacy notices include specific elements or be provided in specific formats. Federal agency personnel consult with the senior agency official for privacy and legal counsel regarding when and where to provide privacy notices, as well as elements to include in privacy notices and required formats. In circumstances where laws or government-wide policies do not require privacy notices, organizational policies and determinations may require privacy notices and may serve as a source of the elements to include in privacy notices.

Privacy risk assessments identify the privacy risks associated with the processing of personally identifiable information and may help organizations determine appropriate elements to include in a privacy notice to manage such risks. To help individuals understand how their information is being processed, organizations write materials in plain language and avoid technical jargon.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

Privacy Act; OMB A-108, A-130

Related Controls

PM-20, PM-22, PT-02, PT-03, PT-04, PT-07, RA-03

PT-07 Specific Categories of Personally Identifiable Information

Baselines

N/A

Overlays

Privacy

Requirements

Apply processing conditions in accordance with the TxDOT Data Classification Policy for specific categories of personally identifiable information.

Implementation Standards

Std.01 — Establish, maintain, and update at least annually an inventory containing a listing of all programs and information systems identified as

collecting, using, maintaining, or sharing sensitive personal information (SPI).

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Organizations apply any conditions or protections that may be necessary for specific categories of personally identifiable information. These conditions may be required by laws, executive orders, directives, regulations, policies, standards, or guidelines. The requirements may also come from the results of privacy risk assessments that factor in contextual changes that may result in an organizational determination that a particular category of personally identifiable information is particularly sensitive or raises particular privacy risks. Organizations consult with the senior agency official for privacy and legal counsel regarding any protections that may be necessary.

TxDOT Discussion

None.

TxDOT References

Data Classification Policy; Information Security and Privacy Policy

State References

None.

Federal References

Privacy Act; OMB A-108, A-130; NARA CUI

Related Controls

PT-02, PT-03, RA-03

PT-07(01) Social Security Numbers

Baselines

N/A

Overlays

Privacy

Requirements

When a system processes Social Security numbers:

a. Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier;

b. Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; and

c. Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

Implementation Standards

Std.01 — Provide TxDOT's Privacy Notice before requesting personally identifiable information (PII) including Social Security Numbers.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Federal law and policy establish specific requirements for organizations' processing of Social Security numbers. Organizations take steps to eliminate unnecessary uses of Social Security numbers and other sensitive information and observe any particular requirements that apply.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

Privacy Act; OMB A-108, A-130

Related Controls

IA-04

RA — Risk Assessment

RA-01 Policy and Procedures

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level risk assessment policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;

b. Designate a senior management official as defined in the risk assessment policy to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and

c. Review and update the current risk assessment:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The owner or their designated representative(s) are responsible for:

a. Classifying information under their authority or responsibility, with the concurrence of the agency head or their designated representative(s), in accordance with the state agency's established information classification categories;

b. Approving access to information resources and periodically reviewing access lists based on documented risk management decisions;

c. Formally assigning custody of information or an information resource;

d. Coordinating data security control requirements with the Information Security Officer;

e. Conveying data security control requirements to custodians;

f. Providing authority to custodians to implement security controls and procedures;

g. Justifying, documenting, and being accountable for exceptions to security controls issued by the Information Security Officer for the information for which the Information Owner is responsible;

h. Coordinating and obtaining approval for exceptions to security controls with the state agency Information Security Officer; and

i. Performing risk assessments as provided under 1 TAC 202.25.

j. Information owners, in coordination with the information custodian, shall ensure that information resources provide a clear and conspicuous prohibition against unauthorized access or use as detailed by Texas Penal Code Sec. 33.02(b-1). [Source: 1 TAC 202.22(a)(1)]

Std.03 — Custodians of information resources, including third party entities providing outsourced information resources services to state agencies shall:

a. Implement controls required to protect information and information resources required by 1 TAC 202 based on the classification and risks specified by the information owner(s) or as specified by the policies, procedures, and standards defined by the state agency information security program;

b. Provide owners with information to evaluate the cost-effectiveness of controls and monitoring;

c. Adhere to monitoring techniques and procedures, approved by the Information Security Officer, for detecting, reporting, and investigating incidents;

d. Supply any information and/or documents necessary to provide appropriate information security training to employees; and

e. Ensure information is recoverable in accordance with risk management decisions. [Source: 1 TAC 202.22(a)(2)]

Std.04 — The user of an information resource has the responsibility to use the resource only for the purpose specified by the agency or information-owner; comply with information security controls and agency policies to prevent unauthorized or accidental disclosure, modification, or destruction of information and information resources; and formally acknowledge that they will comply with the security policies and procedures in a method determined by the agency head or his or her designated representative. [Source: 1 TAC 202.22(a)(3)]

Std.05 — Agency information resources designated for use by the public shall be configured to enforce security policies and procedures without requiring user participation or intervention. Information resources must require the acceptance of a banner or notice prior to use. [Source: 1 TAC 202.22(a)(4)]

Std.06 — The Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

Std.07 —

a. Information owners, custodians, and users of information resources shall, in consultation with TxDOT's Information Resources Manager and Information Security Officer, be identified by TxDOT; and

b. The responsibilities of information owners, custodians, and users of information resources shall be defined and documented by TxDOT. [Source: 1 TAC 202.22(a)]

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.08 CJIS — Review and update the current risk assessment policy and procedures following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. [Source: CJIS RA-01]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Risk assessment policy and procedures address the controls in the RA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of risk assessment policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system

security and privacy plans or in one or more separate documents. Events that may precipitate an update to risk assessment policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-12, 800-30, 800-39, 800-100; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

PM-09, PS-08, SI-12

RA-02 Security Categorization

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Categorize the system and information it processes, stores, and transmits;

b. Document the security categorization results, including supporting rationale, in the security plan for the system; and

c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

Implementation Standards

Std.01 — TxDOT is responsible for defining all information classification categories except the Confidential or Regulated Information category, which is defined in Subchapter A of 1 TAC 202, and establishing the controls for each. [Source: 1 TAC 202.24(b)(1)]

Std.02 — The Information Owner or their designated representative(s) are responsible for classifying information under their authority, with the concurrence of the TxDOT Executive Director or their designated representative(s), in accordance with the state agency's established information classification categories. [Source: 1 TAC 202.22(a)(1)(A)]

Std.03 — On initiation of an information resources technology project, including an application development project and any information resources projects described in this subchapter, a state agency shall classify the data produced from or used in the project and determine appropriate data security and applicable retention requirements under Section 441.185 for each classification. [Source: TGC 2054.161]

Std.04 — Involve the Senior Official for Privacy, or their designee, when conducting the security categorization process for information systems containing personally identifiable information (PII) or sensitive personal information (SPI).

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement RA-02.

Std.05 CJIS — Rescinded in V4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Security categories describe the potential adverse impacts or negative consequences to organizational operations, organizational assets, and individuals if organizational information and systems are compromised through a loss of confidentiality, integrity, or availability. Security categorization is also a type of asset loss characterization in systems security engineering processes that is carried out throughout the system development life cycle. Organizations can use privacy risk assessments or privacy impact assessments to better understand the potential adverse effects on individuals. CNSSI 1253 provides additional guidance on categorization for national security systems.

Organizations conduct the security categorization process as an organization-wide activity with the direct involvement of chief information officers, senior agency information security officers, senior agency officials for privacy, system owners, mission and business owners, and information owners or stewards. Organizations consider the potential adverse impacts to other organizations and, in accordance with USA Patriot Act and Homeland Security Presidential Directives, potential national-level adverse impacts.

Security categorization processes facilitate the development of inventories of information assets and, along with CM-08, mappings to specific system components where information is processed, stored, or transmitted. The security categorization process is revisited throughout the system development life cycle to ensure that the security categories remain accurate and relevant.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

TGC 2054; 1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 199, 200; NIST SP 800-30, 800-37, 800-39, 800-60-1, 800-60-2, 800-160-1; CNSSI 1253; NARA CUI; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

CM-08, MP-04, PL-02, PL-10, PL-11, PM-07, RA-03, RA-05, RA-07, RA-08, SA-08, SC-07, SI-12

RA-03 Risk Assessment

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Conduct a risk assessment, including:

1. Identifying threats to and vulnerabilities in the system;

2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and

3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

c. Document risk assessment results in organization approved assessment report format;

d. Review risk assessment results annually;

e. Disseminate risk assessment results to Information Owners, Information Custodians, Information Security Office; and

f. Update the risk assessment annually or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

Implementation Standards

Std.01 — TxDOT shall perform and document risk assessments and make and document risk management decisions in compliance with 1 TAC 202.25. TxDOT's security risk management plan may be excepted from disclosure under Texas Government Code Sec. 2054.077(c) or Sec. 552.139. [Source: DIR Control Standards Catalog RA-3]

Std.02 — The Information Security Officer shall be responsible for ensuring that risk assessments are performed by the information owners and supported by the information-custodians at least biennially for systems containing confidential data and periodically for systems containing agency sensitive or public data. [Source: 1 TAC 202.21(b)(6)]

Std.03 — An agency-wide information security program must be approved by the agency head and include periodic assessments of the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency. [Source: 1 TAC 202.24(a)(1)]

Std.04 — A risk assessment of TxDOT's information and information systems shall be performed and documented. Risks and impacts will be ranked, at a minimum, as either "High," "Moderate," or "Low." The schedule of future risk assessments will be documented. Risk assessment results, vulnerability reports, and similar information shall be documented and presented to the Information Security Officer or their designated representative(s). [Source: 1 TAC 202.25(1, 2, 3)]

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.06 PCI — Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes:

a. Identification of the assets being protected.

b. Identification of the threat(s) that the requirement is protecting against.

c. Identification of factors that contribute to the likelihood and/or impact of a threat being realized.

d. Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized.

e. Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed.

f. Performance of updated risk analyses when needed, as determined by the annual review.

[Source: PCI DSS 12.3.1]

Std.07 PCI — A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include:

a. Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis).

b. Approval of documented evidence by senior management.

c. Performance of the targeted analysis of risk at least once every 12 months.

[Source: PCI DSS 12.3.2]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.08 CJIS — Update the risk assessment at least quarterly or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system. [Source: CJIS RA-03]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.05 FedRAMP — Disseminate risk assessment results to all Authorizing Officials; for Joint Authorization Board (JAB) authorizations to include FedRAMP. [Source: FedRAMP Security Controls Baseline RA-3]

Discussion

Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation. Risk assessments also consider risk from external parties, including contractors who operate systems on behalf of the organization, individuals who access organizational systems, service providers, and outsourcing entities.

Organizations can conduct risk assessments at all three levels in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any stage in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including preparation, categorization, control selection, control implementation, control assessment, authorization, and control monitoring. Risk assessment is an ongoing activity carried out throughout the system development life cycle.

Risk assessments can also address information related to the system, including system design, the intended use of the system, testing results, and supply chain-related information or artifacts. Risk assessments can play an important role in control selection processes, particularly during the application of tailoring guidance and in the earliest phases of capability determination.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-30, 800-39, 800-161; NIST IR 8023, 8062, 8272; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CA-03, CA-06, CM-04, CP-06, CP-07, IA-08, MA-05, PE-03, PE-08, PE-18, PL-02, PL-10, PL-11, PM-08, PM-09, PM-28, PT-02, PT-07, RA-02, RA-05, RA-07, RA-09, SA-08, SA-09, SI-12

RA-03(01) Supply Chain Risk Assessment

Baselines

Low, Moderate, High

Overlays

FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Assess supply chain risks associated with all systems, system components, and system services under configuration management; and

b. Update the supply chain risk assessment at least annually, when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Supply chain-related events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion of malicious code. These events can have a significant impact on the confidentiality, integrity, or availability of a system and its information and, therefore, can also adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. The supply chain-related events may be unintentional or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; NIST SP 800-30, 800-39, 800-161; NIST IR 8023, 8062, 8272; FedRAMP Security Controls Baseline

Related Controls

PM-30, RA-02, RA-09, SR-02

RA-05 Vulnerability Monitoring and Scanning

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Monitor and scan for vulnerabilities in the system and hosted applications in accordance with Std.06 and when new vulnerabilities potentially affecting the system are identified and reported;

b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

1. Enumerating platforms, software flaws, and improper configurations;

2. Formatting checklists and test procedures; and

3. Measuring vulnerability impact;

c. Analyze vulnerability scan reports and results from vulnerability monitoring;

d. Remediate legitimate vulnerabilities per the timeline outlined in Std.07 in accordance with an organizational assessment of risk;

e. Share information obtained from the vulnerability monitoring process and control assessments with the Information Owner, and in accordance with Stds.02, 03, & 05 to help eliminate similar vulnerabilities in other systems; and

f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

Implementation Standards

Std.01 — TxDOT, when implementing an Internet website or mobile application that processes any sensitive personal or personally identifiable information or confidential information, must subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test. [Source: TGC 2054.516(a)(2)]

Std.02 — TxDOT's Chief Information Security Officer shall prepare or have prepared a report, including an executive summary of the findings of the biennial report, not later than October 15 of each even-numbered year, assessing the extent to which a computer, a computer program, a computer network, a computer system, a printer, an interface to a computer system, including mobile and peripheral devices, computer software, or data processing of the agency or of a contractor of the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or

contractor's electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use. [Source: TGC 2054.077(b)]

Std.03 — Except as provided by TGC 2054.077, a vulnerability report and any information or communication prepared or maintained for use in the preparation of a vulnerability report is confidential or regulated and is not subject to disclosure under Chapter 552. [Source: TGC 2054.077(c)]

Std.04 — TxDOT's Chief Information Security Officer shall provide an electronic copy of the vulnerability report on its completion to:

a. The Department of Information Resources;

b. The state auditor;

c. TxDOT's Executive Director;

d. The agency's designated information resources manager; and

e. Any other information technology security oversight group specifically authorized by the legislature to receive the report. [Source: TGC 2054.077(d)]

Std.05 — Separate from the executive summary described by Subsection (b), TxDOT shall prepare a summary of the agency's vulnerability report that does not contain any information the release of which might compromise the security of the state agency's or state agency contractor's computers, computer programs, computer networks, computer systems, printers, interfaces to computer systems, including mobile and peripheral devices, computer software, data processing, or electronically stored information. The summary is available to the public on request. [Source: TGC 2054.077(e)]

Std.06 — Rescinded in V4.0, specifics moved to ISS-01-218, TxDOT Vulnerability Scanning Standard.

Std.07 — Rescinded in V4.0, specifics moved to ISS-01-218, TxDOT Vulnerability Scanning Standard.

Std.08 — Utilize an up-to-date SCAP-compliant vulnerability scanning tool. [Source: CIS 7.5]

Std.09 — The network and host-based vulnerability scanner shall provide the following capabilities:

a. Identify active hosts on networks;

b. Identify active and vulnerable services (ports) on hosts;

c. Identify vulnerabilities associated with discovered operating systems and applications. [Source: FedRAMP Vulnerability Scanning Requirements]

Std.10 — Where possible, use tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities. [Source: FedRAMP Vulnerability Scanning Requirements]

Std.11 — TxDOT uses the latest Common Vulnerability Scoring System (CVSS) framework for ranking
vulnerability criticality. All vulnerability scanning tools must support this framework.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 6.3.1.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.12 PCI — Rescinded in V4.0.

Std.18 PCI —

All payment page scripts that are loaded and executed in the consumer's browser are managed as follows:

a. A method is implemented to confirm that each script is authorized.

b. A method is implemented to assure the integrity of each script.

c. An inventory of all scripts is maintained with written justification as to why each is necessary.

[Source: PCI DSS 6.4.3]

Std.13 PCI — Internal vulnerability scans are performed as follows:

a. At least once every three months.

b. High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved.

c. Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved.

d. Scan tool is kept up to date with latest vulnerability information.

e. Scans are performed by qualified personnel and organizational independence of the tester exists.

[Source: PCI DSS 11.3.1]

Std.14 PCI — Rescinded in V3.0.

Std.15 PCI — External vulnerability scans are performed as follows:

a. At least once every three months.

b. By a PCI SSC Approved Scanning Vendor (ASV).

c. Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met.

d. Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.

[Source: PCI DSS 11.3.2]

Std.16 PCI —

a. Internal vulnerability scans are performed after any significant change as follows:

1. High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved.

2. Rescans are conducted as needed.

3. Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).

[Source: PCI DSS 11.3.1.3]

b. External vulnerability scans are performed after any significant change as follows:

1. Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved.

2. Rescans are conducted as needed.

3. Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).

[Source: PCI DSS 11.3.2.1]

Std.19 PCI — All other applicable vulnerabilities (those not ranked as high-risk or critical per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows:

a. Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.

b. Rescans are conducted as needed.

[Source: PCI DSS 11.3.1.1]

Std.20 PCI — Internal vulnerability scans are performed via authenticated scanning as follows:

a. Systems that are unable to accept credentials for authenticated scanning are documented.

b. Sufficient privileges are used for those systems that accept credentials for scanning.

c. If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2.

[Source: PCI DSS 11.3.1.2]

For systems processing PCI DSS data, or that support PCI DSS processes, Std.07 is superseded by PCI DSS requirement 6.3.3:

Std.17 PCI — All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

a. Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.

b. All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).

[Source: PCI DSS 6.3.3]

c. Remediate legitimate vulnerabilities according to the Remediation Responses below, timeline beginning from the date vulnerability is published by the vendor:

1. External Uncredentialed Scan Vulnerability Response Time (Calendar Days)

A. Critical: 15

B. High: 30

C. Medium: 30

D. Low: 90

2. Internal Credentialed Vulnerability Response Time (Calendar Days)

A. Critical: 30

B. High: 30

C. Medium: 90

D. Low: 180

CJIS Correspondence

For systems processing CJIS data, RA-05 requirements a, d, and e are superseded by those requirements from the CJIS requirement RA-05:

Std.25 CJIS —

a. Monitor and scan for vulnerabilities in the system and hosted applications at least monthly and when new vulnerabilities potentially affecting the system are identified and reported;

b. Remediate legitimate vulnerabilities within the number of days listed:

- Critical–15 days
- High–30 days
- Medium–60 days
- Low–90 days; and

c. Share information obtained from the vulnerability monitoring process and control assessments with organizational personnel with risk assessment, control assessment, and vulnerability scanning responsibilities to help eliminate similar vulnerabilities in other systems.

[Source: CJIS RA-05]

TX-RAMP Correspondence

For systems subject to TX-RAMP Level 1 or Level 2 requirements, the following standard applies:

Std.21 TX-RAMP — Install security-relevant software and firmware updates within thirty days of the release of the updates. [Source: TX-RAMP Manual SI-2]

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standards apply:

Std.22 FedRAMP — An accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually. [Source: FedRAMP Security Controls Baseline RA-5]

Std.23 FedRAMP —

a. Remediate legitimate high-risk vulnerabilities within thirty days from date of discovery.

b. If a vulnerability is listed among the CISA Known Exploited Vulnerability (KEV) Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog) the KEV remediation date supersedes the FedRAMP parameter requirement.

[Source: FedRAMP Security Controls Baseline RA-5]

Std.24 FedRAMP — Share information obtained from the vulnerability monitoring process and control assessments with all Authorizing Officials, for Joint Authorization Board (JAB) authorizations to include FedRAMP, to help eliminate similar vulnerabilities in other systems. [Source: FedRAMP Security Controls Baseline RA-5]

Discussion

Security categorization of information and systems guides the frequency and comprehensiveness of vulnerability monitoring (including scans). Organizations determine the required vulnerability monitoring for system components, ensuring that the potential sources of vulnerabilities—such as infrastructure components (e.g., switches, routers, guards, sensors), networked printers, scanners, and copiers—are not overlooked. The capability to readily update vulnerability monitoring tools as new vulnerabilities are discovered and announced and as new scanning methods are developed helps to ensure that new vulnerabilities are not missed by employed vulnerability monitoring tools. The vulnerability monitoring tool update process helps to ensure that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability monitoring and analyses for custom software may require additional approaches, such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can use these analysis approaches in source code reviews and in a variety of tools, including web-based application scanners, static analysis tools, and binary analyzers.

Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly. Vulnerability monitoring may also include continuous vulnerability monitoring tools that use instrumentation to continuously analyze components. Instrumentation-based tools may improve accuracy and may be run throughout an organization without scanning. Vulnerability monitoring tools that facilitate interoperability include tools that are Security Content Automated Protocol (SCAP)-validated. Thus, organizations consider using scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that employ the Open Vulnerability Assessment Language (OVAL) to determine the presence of vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). Control assessments, such as red team exercises, provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).

Vulnerability monitoring includes a channel and process for receiving reports of security vulnerabilities from the public at-large. Vulnerability disclosure programs can be as simple as publishing a monitored email address or web form that can receive reports, including notification authorizing good-faith research and disclosure of security vulnerabilities. Organizations generally expect that such research is happening with or without their authorization and can use public vulnerability disclosure channels to increase the likelihood that discovered vulnerabilities are reported directly to the organization for remediation.

Organizations may also employ the use of financial incentives (also known as "bug bounties") to further encourage external security researchers to report discovered vulnerabilities. Bug bounty programs can be tailored to the organization's needs. Bounties can be operated indefinitely or over a defined period of time and can be offered to the general public or to a curated group. Organizations may run public and private bounties simultaneously and could choose to offer partially credentialed access to certain participants in order to evaluate security vulnerabilities from privileged vantage points.

TxDOT Discussion

False positives should be identified as such in the log. Where possible, scanners should be tuned to exclude a newly identified false positive, but no further remediation action is required.

For dynamic application security testing (DAST), see SA-11(08).

Note for systems subject to FedRAMP Requirements:

See the FedRAMP Documents page > Vulnerability Scanning Requirements

https://www.FedRAMP.gov/documents/

Informational findings from a scanner are detailed as a returned result that holds no vulnerability risk or severity and for FedRAMP does not require an entry onto the POA&M or entry onto the RET during any assessment phase.

Warning findings, on the other hand, are given a risk rating (low, moderate, high or critical) by the scanning solution and should be treated like any other finding with a risk or severity rating for tracking purposes onto either the POA&M or RET depending on when the findings originated (during assessments or during monthly continuous monitoring). If a warning is received during scanning, but further validation turns up no actual issue then this item should be categorized as a false positive. If this situation presents itself during an assessment phase (initial assessment, annual assessment or any SCR), follow guidance on how to report false positives in the Security Assessment Report (SAR). If this situation happens during monthly continuous monitoring, a deviation request will need to be submitted per the FedRAMP Vulnerability Deviation Request Form.

Warnings are commonly associated with scanning solutions that also perform compliance scans, and if the scanner reports a "warning" as part of the compliance scanning of a CSO, follow guidance surrounding the tracking of compliance findings during either the assessment phases (initial assessment, annual assessment or any SCR) or monthly continuous monitoring as it applies. Guidance on compliance scan findings can be found by searching on "Tracking of Compliance Scans" in FAQs.

[Source: FedRAMP Security Controls Baseline RA-5]

TxDOT References

Information Security and Privacy Policy

State References

TGC 2054; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

ISO 29147; NIST SP 800-40, 800-53A, 800-70, 800-115, 800-126; NIST IR 7788, 8011-4, 8023; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CA-02, CA-07, CA-08, CM-02, CM-04, CM-06, CM-08, RA-02, RA-03, SA-11, SA-15, SI-02, SI-03, SI-04, SI-07, SR-11

RA-05(02) Update Vulnerabilities to Be Scanned

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Update the system vulnerabilities to be scanned weekly, prior to a new scan, and when new vulnerabilities are identified and reported.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.03 CJIS — Update the system vulnerabilities to be scanned within 24 hours prior to running a new scan or when new vulnerabilities are identified and reported. [Source: CJIS RA-05(02)]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low baseline, the following standard applies:

Std.01 FedRAMP — Update the system vulnerabilities to be scanned prior to a new scan. [Source: FedRAMP Security Controls Baseline RA-5(2)]

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.02 FedRAMP — Update the system vulnerabilities to be scanned within 24 hours prior to running scans. [Source: FedRAMP Security Controls Baseline RA-5(2)]

Discussion

Due to the complexity of modern software, systems, and other factors, new vulnerabilities are discovered on a regular basis. It is important that newly discovered vulnerabilities are added to the list of vulnerabilities to be scanned to ensure that the organization can take steps to mitigate those vulnerabilities in a timely manner.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

ISO 29147; NIST SP 800-40, 800-53A, 800-70, 800-115, 800-126; NIST IR 7788, 8011-4, 8023; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

SI-05

RA-05(03) Breadth and Depth of Coverage

Baselines

N/A

Overlays

TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Define the breadth and depth of vulnerability scanning coverage.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

The breadth of vulnerability scanning coverage can be expressed as a percentage of components within the system, by the particular types of systems, by the criticality of systems, or by the number of vulnerabilities to be checked. Conversely, the depth of vulnerability scanning coverage can be expressed as the level of the system design that the organization intends to monitor (e.g., component, module, subsystem, element). Organizations can determine the sufficiency of vulnerability scanning coverage with regard to its risk tolerance and other factors. Scanning tools and how the tools are configured may affect the depth and coverage. Multiple scanning tools may be needed to achieve the desired depth and coverage. SP 800-53A provides additional information on the breadth and depth of coverage.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

RA-05(04) Discoverable Information

Baselines

High

Overlays

FedRAMP High

Requirements

Determine information about the system that is discoverable and take corrective actions as defined in Std.01.

Implementation Standards

Std.01 — Corrective actions depend on System Development Life Cycle (SDLC) phase:

a. For systems in development, require that developers make changes to system to mitigate risk; and

b. For systems in the operational & maintenance phase, implement corrective actions and document in the plan of action and milestones document (POAM).

Std.02 — Update System Security Plans (SSPs) following corrective actions.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.02 FedRAMP — Determine information about the system that is discoverable and take notify appropriate service provider personnel and follow procedures for organization and service provider-defined corrective actions. [Source: FedRAMP Security Controls Baseline RA-5(4)]

Discussion

Discoverable information includes information that adversaries could obtain without compromising or breaching the system, such as by collecting information that the system is exposing or by conducting extensive web searches. Corrective actions include notifying appropriate organizational personnel, removing designated information, or changing the system to make the designated information less relevant or attractive to adversaries. This enhancement excludes intentionally discoverable information that may be part of a decoy capability (e.g., honeypots, honeynets, or deception nets) deployed by the organization.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

ISO 29147; NIST SP 800-40, 800-53A, 800-70, 800-115, 800-126; NIST IR 7788, 8011-4, 8023; FedRAMP Security Controls Baseline

Related Controls

None.

RA-05(05) Privileged Access

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Implement privileged access authorization to Sensitive, Confidential, or Regulated components for vulnerability scanning activities.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.02 CJIS — Implement privileged access authorization to information system components containing or processing CJI for vulnerability scanning activities requiring privileged access. [Source: CJIS RA-05(05)]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.01 FedRAMP — Implement privileged access authorization to all components that support authentication for all scans.

[Source: FedRAMP Security Controls Baseline RA-5(5)]

Discussion

In certain situations, the nature of the vulnerability scanning may be more intrusive, or the system component that is the subject of the scanning may contain classified or controlled unclassified information, such as personally identifiable information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

ISO 29147; NIST SP 800-40, 800-53A, 800-70, 800-115, 800-126; NIST IR 7788, 8011-4, 8023; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

RA-05(08) Review Historic Audit Logs

Baselines

N/A

Overlays

FedRAMP High

Requirements

Review historic audit logs to determine if a vulnerability identified in a system under configuration control has been previously exploited within a time period in accordance with AU-06.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Reviewing historic audit logs to determine if a recently detected vulnerability in a system has been previously exploited by an adversary can provide important information for forensic analyses. Such analyses can help identify, for example, the extent of a previous intrusion, the trade craft employed during the attack, organizational information exfiltrated or modified, mission or business capabilities affected, and the duration of the attack.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

This control is required for all high (or critical) vulnerability scan findings. [Source: FedRAMP Security Controls Baseline RA-5(8)]

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

AU-06, AU-11

RA-05(11) Public Disclosure Program

Baselines

Low, Moderate, High

Overlays

CJIS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

Implementation Standards

Std.01 — Publish a vulnerability disclosure program policy statement to a publicly accessible agency website, including reporting contact details.

Std.02 — Configure reporting channels to notify appropriate personnel.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement RA-05(11).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

The reporting channel is publicly discoverable and contains clear language authorizing good-faith research and the disclosure of vulnerabilities to the organization. The organization does not condition its authorization on an expectation of indefinite non-disclosure to the public by the reporting entity

but may request a specific time period to properly remediate the vulnerability.

TxDOT Discussion

Liability Exemption. A person who in good faith discloses to a state agency or other governmental entity information regarding a potential security issue with respect to the agency's or entity's information resources technologies is not liable for any civil damages resulting from disclosing the information unless the person stole, retained, or sold any data obtained as a result of the security issue. [Source: TGC 2054.602]

TxDOT References

Information Security and Privacy Policy

State References

TGC 2054; DIR Security Control Standards Catalog

Federal References

ISO 29147; NIST SP 800-40, 800-53A, 800-70, 800-115, 800-126; NIST IR 7788, 8011-4, 8023; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

RA-07 Risk Response

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

Implementation Standards

Std.01 — Identify, prioritize, and implement responses to risks identified from assessments, monitoring, and audits. [Source: NIST Privacy Framework ID.RA-P5]

Std.02 — Document all responses to findings from internal assessments and monitoring in Plans of Action and Milestones (POAMs). Document all responses to findings from audits in management action plans (MAPs) and POAMs as appropriate.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement RA-07.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Organizations have many options for responding to risk including mitigating risk by implementing new controls or strengthening existing controls, accepting risk with appropriate justification or rationale, sharing or transferring risk, or avoiding risk. The risk tolerance of the organization influences risk response decisions and actions. Risk response addresses the need to determine an appropriate response to risk before generating a plan of action and milestones entry. For example, the response may be to accept risk or reject risk, or it may be possible to mitigate the risk immediately so that a plan of action and milestones entry is not needed. However, if the risk response is to mitigate the risk, and the mitigation cannot be completed immediately, a plan of action and milestones entry is generated.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

TX-RAMP Program Manual

Federal References

FIPS 199, 200; NIST SP 800-30, 800-37, 800-39, 800-160-1; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CA-05, PM-04, PM-28, RA-02, RA-03, SR-02

RA-08 Privacy Impact Assessments

Baselines

N/A

Overlays

Privacy

Requirements

Conduct privacy impact assessments for systems, programs, or other activities before:

a. Developing or procuring information technology that processes personally identifiable information; and

b. Initiating a new collection of personally identifiable information that:

1. Will be processed using information technology; and

2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.

Implementation Standards

Std.01 — Ensure that privacy impact assessments (PIAs) are conducted before processing of sensitive personal information (SPI).

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

A privacy impact assessment is an analysis of how personally identifiable information is handled to ensure that handling conforms to applicable privacy requirements, determine the privacy risks associated with an information system or activity, and evaluate ways to mitigate privacy risks. A privacy impact assessment is both an analysis and a formal document that details the process and the outcome of the analysis.

Organizations conduct and develop a privacy impact assessment with sufficient clarity and specificity to demonstrate that the organization fully considered privacy and incorporated appropriate privacy protections from the earliest stages of the organization's activity and throughout the information life cycle. In order to conduct a meaningful privacy impact assessment, the organization's senior agency official for privacy works closely with program managers, system owners, information technology experts, security officials, counsel, and other relevant organization personnel. Moreover, a privacy impact assessment is not a time-restricted activity that is limited to a particular milestone or stage of the information system or personally identifiable information life cycles. Rather, the privacy analysis continues throughout the system and personally identifiable information life cycles. Accordingly, a privacy impact assessment is a living document that organizations update whenever changes to the information technology, changes to the organization's practices, or other factors alter the privacy risks associated with the use of such information technology.

To conduct the privacy impact assessment, organizations can use security and privacy risk assessments. Organizations may also use other related processes that may have different names, including privacy threshold analyses. A privacy impact assessment can also serve as notice to the public regarding the organization's practices with respect to privacy. Although

conducting and publishing privacy impact assessments may be required by law, organizations may develop such policies in the absence of applicable laws. For federal agencies, privacy impact assessments may be required by EGOV; agencies should consult with their senior agency official for privacy and legal counsel on this requirement and be aware of the statutory exceptions and OMB guidance relating to the provision.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

E-Government Act; OMB A-130, M-03-22

Related Controls

CM-04, CM-09, PT-02, PT-03, PT-05, RA-01, RA-02, RA-03, RA-07

RA-09 Criticality Analysis

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Identify critical system components and functions by performing a criticality analysis for all systems, system components, or system services under configuration management at all decision points as defined in TxDOT's system development life cycle.

Implementation Standards

Std.01 — Define and document in the System Security Plan (SSP) all critical hardware and software systems, system components, and system services.

[Source: Catalog of Control Systems Security: Recommendations for Standards Developers]

Std.02 — For systems in the architectural design process step, perform component-level security categorization to support the system-level criticality analysis.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement RA-09.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Not all system components, functions, or services necessarily require significant protections. For example, criticality analysis is a key tenet of supply chain risk management and informs the prioritization of protection activities. The identification of critical system components and functions considers applicable laws, executive orders, regulations, directives, policies, standards, system functionality requirements, system and component interfaces, and system and component dependencies. Systems engineers conduct a functional decomposition of a system to identify mission-critical functions and components. The functional decomposition includes the identification of organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and external to the system.

The operational environment of a system or a system component may impact the criticality, including the connections to and dependencies on cyber-physical systems, devices, system-of-systems, and outsourced IT services. System components that allow unmediated access to critical system components or functions are considered critical due to the inherent vulnerabilities that such components create. Component and function criticality are assessed in terms of the impact of a component or function

failure on the organizational missions that are supported by the system that contains the components and functions.

Criticality analysis is performed when an architecture or design is being developed, modified, or upgraded. If such analysis is performed early in the system development life cycle, organizations may be able to modify the system design to reduce the critical nature of these components and functions, such as by adding redundancy or alternate paths into the system design. Criticality analysis can also influence the protection measures required by development contractors. In addition to criticality analysis for systems, system components, and system services, criticality analysis of information is an important consideration. Such analysis is conducted as part of security categorization in RA-02.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

NIST IR 8179; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CP-02, PL-02, PL-08, PL-11, PM-01, PM-11, RA-02, RA-03, SA-08, SA-15, SR-05

SA — System and Services Acquisition

SA-01 Policy and Procedures

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level system and services acquisition policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;

b. Designate a senior management official as defined in the system and services acquisition policy to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and

c. Review and update the current system and services acquisition:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 6.1.1 and 6.1.2.

Std.03 PCI — Rescinded in V3.0.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Review and update the current system and services acquisition policy and procedures following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI [Source: CJIS SA-01]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

System and services acquisition policy and procedures address the controls in the SA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and services acquisition policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and services acquisition policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-12, 800-30, 800-39, 800-100, 800-160-1; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

PM-09, PS-08, SA-08, SI-12

SA-02 Allocation of Resources

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;

b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and

c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

Implementation Standards

Std.01 — The TxDOT Executive Director or their designated representative(s) shall allocate resources for ongoing information security remediation, implementation, and compliance activities that reduce risk to a level acceptable to the TxDOT Executive Director. [Source: 1 TAC 202.20(b)(2)]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SA-02.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Resource allocation for information security and privacy includes funding for system and services acquisition, sustainment, and supply chain-related risks throughout the system development life cycle.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog

Federal References

OMB A-130; NIST SP 800-37, 800-160-1; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

PM-03, PM-11, SA-09, SR-03, SR-05

SA-03 System Development Life Cycle

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Acquire, develop, and manage the system using TxDOT's system development life cycle that incorporates information security and privacy considerations;

b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;

c. Identify individuals having information security and privacy roles and responsibilities; and

d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

Implementation Standards

Std.01 — TxDOT shall include information security, security testing, and audit controls in all phases of the system development lifecycle or acquisition process.

Std.02 — The TxDOT Executive Director or their designated representative(s) shall ensure that information security management processes are integrated with state agency strategic and operational planning processes. [Source: 1 TAC 202.20(b)(8)]

Std.03 — The Information Security Officer shall be responsible for working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks. [Source: 1 TAC 202.21(b)(3)]

Std.04 — The Information Security Officer shall be responsible for recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure. [Source: 1 TAC 202.21(b)(8)]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SA-03.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

A system development life cycle process provides the foundation for the successful development, implementation, and operation of organizational

systems. The integration of security and privacy considerations early in the system development life cycle is a foundational principle of systems security engineering and privacy engineering. To apply the required controls within the system development life cycle requires a basic understanding of information security and privacy, threats, vulnerabilities, adverse impacts, and risk to critical mission and business functions. The security engineering principles in SA-08 help individuals properly design, code, and test systems and system components. Organizations include qualified personnel (e.g., senior agency information security officers, senior agency officials for privacy, security and privacy architects, and security and privacy engineers) in system development life cycle processes to ensure that established security and privacy requirements are incorporated into organizational systems. Role-based security and privacy training programs can ensure that individuals with key security and privacy roles and responsibilities have the experience, skills, and expertise to conduct assigned system development life cycle activities.

The effective integration of security and privacy requirements into enterprise architecture also helps to ensure that important security and privacy considerations are addressed throughout the system life cycle and that those considerations are directly related to organizational mission and business processes. This process also facilitates the integration of the information security and privacy architectures into the enterprise architecture, consistent with the risk management strategy of the organization. Because the system development life cycle involves multiple organizations, (e.g., external suppliers, developers, integrators, service providers), acquisition and supply chain risk management functions and controls play significant roles in the effective management of the system during the life cycle.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-30, 800-37, 800-160-1, 800-171, 800-172; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AT-03, PL-08, PM-07, SA-04, SA-05, SA-08, SA-11, SA-15, SA-17, SA-22, SR-03, SR-04, SR-05, SR-09

SA-04 Acquisition Process

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Include the following requirements, descriptions, and criteria, explicitly or by reference, using standardized contract language provided by the Information Technology and Security Requirements Attachment in the acquisition contract for the system, system component, or system service:

a. Security and privacy functional requirements;

b. Strength of mechanism requirements;

c. Security and privacy assurance requirements;

d. Controls needed to satisfy the security and privacy requirements;

e. Security and privacy documentation requirements;

f. Requirements for protecting security and privacy documentation;

g. Description of the system development environment and environment in which the system is intended to operate;

h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and

i. Acceptance criteria.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — TxDOT shall require each vendor contracting with the agency to provide cloud computing services for the agency to comply with the requirements of the state risk and authorization management program (TX-RAMP). [Source: TGC 2054.0593(d)]

Std.03 — TxDOT, as a state agency contracting for cloud computing services that store, process, or transmit data of the state agency, shall:

a. Confirm that vendors contracting with the state agency to provide cloud computing services for the state agency are certified through TX-RAMP prior to entering or renewing a cloud computing services contract on or after January 1, 2022; and

b. Require a vendor contracting with the state agency to provide cloud computing services for the state agency that are subject to the state risk and authorization management program to maintain TX-RAMP compliance and certification throughout the term of the contract. [Source: 1 TAC 202.27]

Std.04 — The Information Security Officer shall be responsible for coordinating the review of security requirements and specifications, and verifying that security requirements are identified and risk mitigation plans are developed and contractually agreed and obligated prior to the acquisition of new information systems and/or related services and applications. [Source: 1 TAC 202.21(b)(9)]

Std.05 — The Information Security Officer shall be responsible for verifying that security requirements are identified and risk mitigation plans are developed and implemented prior to the deployment of internally-developed information systems and/or related applications or services. [Source: 1 TAC 202.21(b)(10)]

Std.06 — Where software development is outsourced, the following points are addressed either in a contract or security service level agreement (SLA):

a. Licensing arrangements, code ownership, and intellectual property rights;

b. Certification of the quality and accuracy of the work carried out;

c. Escrow arrangements in the event of failure of the third-party;

d. Rights of access for audit of the quality and accuracy of work done;

e. Contractual requirements for quality and security functionality of code; and

f. Testing before installation to detect malicious code. [Source: Hitrust 10.l Outsourced Software Development]

Std.07 — TxDOT, as a state agency entering into or renewing a contract with a vendor authorized to access, transmit, use, or store data for the agency, shall include a provision in the contract requiring the vendor to meet the security controls the agency determines are proportionate with the agency's risk under the contract based on the sensitivity of the agency's data. The vendor must periodically provide to the agency evidence that the vendor meets the security controls required under the contract. [Source: TGC 2054.138]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SA-04.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.08 FedRAMP — The service provider must comply with Federal Acquisition Regulation (FAR) Subpart 7.103, and Section 889 of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 (Pub. L. 115-232), and FAR Subpart 4.21, which implements Section 889 (as well as any added updates related to FISMA to address security concerns in the system acquisitions process). [Source: FedRAMP Security Controls Baseline SA-4]

Discussion

Security and privacy functional requirements are typically derived from the high-level security and privacy requirements described in SA-02. The derived requirements include security and privacy capabilities, functions, and mechanisms. Strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to tampering or bypass, and resistance to direct attack. Assurance requirements include development processes, procedures, and methodologies as well as the evidence from development and assessment

activities that provide grounds for confidence that the required functionality is implemented and possesses the required strength of mechanism. SP 800-160-1 describes the process of requirements engineering as part of the system development life cycle.

Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and for reflecting the security and privacy requirements of stakeholders. Controls are selected and implemented in order to satisfy system requirements and include developer and organizational responsibilities. Controls can include technical, administrative, and physical aspects. In some cases, the selection and implementation of a control may necessitate additional specification by the organization in the form of derived requirements or instantiated control parameter values. The derived requirements and control parameter values may be necessary to provide the appropriate level of implementation detail for controls within the system development life cycle.

Security and privacy documentation requirements address all stages of the system development life cycle. Documentation provides user and administrator guidance for the implementation and operation of controls. The level of detail required in such documentation is based on the security categorization or classification level of the system and the degree to which organizations depend on the capabilities, functions, or mechanisms to meet risk response expectations. Requirements can include mandated configuration settings that specify allowed functions, ports, protocols, and services. Acceptance criteria for systems, system components, and system services are defined in the same manner as the criteria for any organizational acquisition or procurement.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred.

See https://www.niap-ccevs.org/Product/index.cfm or https://www.commoncriteriaportal.org/products/. [Source: FedRAMP Security Controls Baseline SA-4]

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; TGC 2054; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

Privacy Act; OMB A-130; ISO 15408-1, 15408-2, 15408-3, 29148; FIPS 140, 201; NIST SP 800-35, 800-37, 800-70, 800-73-4, 800-137, 800-160-1, 800-161; NIST IR 7539, 7622, 7676, 7870, 8062; NIAP Common Criteria Evaluation and Validation Scheme; NSA CSFC; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CM-06, CM-08, PS-07, SA-03, SA-05, SA-08, SA-11, SA-15, SA-16, SA-17, SR-03, SR-05

SA-04(01) Functional Properties of Controls

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

Implementation Standards

Std.01 — Require the developer of the system, system component, or system service to meet or exceed the baseline by security categorization provided in the TxDOT Security and Privacy Controls Standard Baseline.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SA-04(01).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Functional properties of security and privacy controls describe the functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.

TxDOT Discussion

Specifications for the security control requirements include that security controls be incorporated in the information system, supplemented by manual controls as needed. These considerations are applied when evaluating software packages, developed or purchased. Security requirements and controls reflect the business value of the information assets involved, and the potential business damage that might result from a failure or absence of security. [Source: Hitrust CSF 10.a Security Requirements Analysis and Specification]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

Privacy Act; OMB A-130; ISO 15408-1, 15408-2, 15408-3; FIPS 140, 201; NIST SP 800-35, 800-37, 800-70, 800-73-4, 800-137, 800-160-1, 800-161; NIST IR 7539, 7622, 7676, 7870, 8062; NIAP Common Criteria Evaluation and Validation Scheme; NSA CSFC; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

SA-04(02) Design and Implementation Information for Controls

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; and design and implementation information as specified in contracts or service level agreements (SLAs) at a level of detail sufficient to allow independent analysis.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.01 CJIS — Require the developer of the system, system component, or system service to provide a project plan that addresses sufficient detail to permit analysis and testing of the controls. [Source: CJIS SA-04(02)]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organizations may require different levels of detail in the documentation for the design and implementation of controls in organizational systems, system components, or system services based on mission and business requirements, requirements for resiliency and trustworthiness, and requirements for analysis and testing. Systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules and the interfaces between modules providing security-relevant functionality. Design and implementation documentation can include manufacturer, version, serial number, verification hash signature, software libraries used, date of purchase or download, and the vendor or download source. Source code and hardware schematics are referred to as the implementation representation of the system.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

Privacy Act; OMB A-130; ISO 15408-1, 15408-2, 15408-3; FIPS 140, 201; NIST SP 800-35, 800-37, 800-70, 800-73-4, 800-137, 800-160-1, 800-161; NIST IR 7539, 7622, 7676, 7870, 8062; NIAP Common Criteria Evaluation and Validation Scheme; NSA CSFC; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

SA-04(05) System, Component, and Service Configurations

Baselines

N/A

Overlays

FedRAMP High

Requirements

Require the developer of the system, system component, or system service to:

a. Deliver the system, component, or service with security configurations as defined in Std.01 FedRAMP implemented; and

b. Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.01 FedRAMP — The service provider shall use the DoD STIGs to establish configuration settings; Center for Internet Security up to Level 2 (CIS Level 2) guidelines shall be used if STIGs are not available; Custom baselines shall be used if CIS is not available. [Source: FedRAMP Security Controls Baseline SA-4(5)]

Discussion

Examples of security configurations include the U.S. Government Configuration Baseline (USGCB), Security Technical Implementation Guides (STIGs), and any limitations on functions, ports, protocols, and services. Security characteristics can include requiring that default passwords have been changed.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

SA-04(09) Functions, Ports, Protocols, and Services in Use

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SA-04(09).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design stages) allows organizations to influence the design of the system, system component, or system service. This early involvement in the system development life cycle helps organizations avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services or requiring system service providers to do so. Early identification of functions, ports, protocols, and services avoids costly retrofitting of controls after the system, component, or system service has been implemented. SA-09 describes the requirements for external system services. Organizations identify which functions, ports, protocols, and services are provided from external sources.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

Privacy Act; OMB A-130; ISO 15408-1, 15408-2, 15408-3; FIPS 140, 201; NIST SP 800-35, 800-37, 800-70, 800-73-4, 800-137, 800-160-1, 800-161; NIST IR 7539, 7622, 7676, 7870, 8062; NIAP Common Criteria Evaluation

and Validation Scheme; NSA CSFC; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CM-07, SA-09

SA-04(10) Use of Approved PIV Products

Baselines

N/A

Overlays

CJIS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SA-04(10).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Products on the FIPS 201-approved products list meet NIST requirements for Personal Identity Verification (PIV) of Federal Employees and Contractors.

PIV cards are used for multi-factor authentication in systems and organizations.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

IA-02, IA-08, PM-09

SA-05 System Documentation

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Obtain or develop administrator documentation for the system, system component, or system service that describes:

1. Secure configuration, installation, and operation of the system, component, or service;

2. Effective use and maintenance of security and privacy functions and mechanisms; and

3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;

b. Obtain or develop user documentation for the system, system component, or system service that describes:

1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;

2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and

3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take actions defined in Std.02 in response; and

d. Distribute documentation to personnel identified in the System Security Plan (SSP).

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — When documentation cannot be obtained, record in the System Security Plan (SSP):

a. The missing documentation types and topics as defined in this control; and

b. Auditable information, such as e-mails, meeting minutes, or other artifacts, regarding attempts to obtain documentation.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Document steps to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent by contacting manufacturers, suppliers, or developers and conducting web-based searches in response. [Source: CJIS SA-05]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

System documentation helps personnel understand the implementation and operation of controls. Organizations consider establishing specific measures to determine the quality and completeness of the content provided. System documentation may be used to support the management of supply chain risk, incident response, and other functions. Personnel or roles that require documentation include system owners, system security officers, and system administrators. Attempts to obtain documentation include contacting manufacturers or suppliers and conducting web-based searches. The inability to obtain documentation may occur due to the age of the system or component or the lack of support from developers and contractors. When documentation cannot be obtained, organizations may need to recreate the documentation if it is essential to the implementation or operation of the controls. The protection provided for the documentation is commensurate with the security category or classification of the system. Documentation that addresses system vulnerabilities may require an increased level of protection. Secure operation of the system includes initially starting the system and resuming secure system operation after a lapse in system operation.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-160-1; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CM-04, CM-06, CM-07, CM-08, PL-02, PL-04, PL-08, PS-02, SA-03, SA-04, SA-08, SA-09, SA-10, SA-11, SA-15, SA-16, SA-17, SI-12, SR-03

SA-08 Security and Privacy Engineering Principles

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: systems security and privacy engineering principles in Std.01.

Implementation Standards

Std.01 — System security and privacy engineering principles that must be applied are those principles defined in the TxDOT SDLC, including at a minimum the following principles drafted according to the guidance in NIST SP 800-160-1:

a. Security Architecture and Design;

b. Security Capability and Intrinsic Behaviors; and

c. Life Cycle Security.

Std.02 — Provide role-specific training for all personnel in roles with responsibilities that contribute to secure development. Periodically review role-specific training and update it as needed. [Source: SP 800-218 PO.2.2]

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.03 PCI — Bespoke and custom software are developed securely, as follows:

a. Based on industry standards and/or best practices for secure development.

b. In accordance with PCI DSS (for example, secure authentication and logging).

c. Incorporating consideration of information security issues during each stage of the software development lifecycle.

[Source: PCI DSS 6.2.1]

Std.04 PCI —

a. Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

1. On software security relevant to their job function and development languages.

2. Including secure software design and secure coding techniques.

3. Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

[Source: PCI DSS 6.2.2]

b. Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following:

1. Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws.

2. Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data.

3. Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.

4. Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other

system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).

5. Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms.

6. Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

[Source: PCI DSS 6.2.4]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SA-08.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Systems security and privacy engineering principles are closely related to and implemented throughout the system development life cycle (see SA-03). Organizations can apply systems security and privacy engineering principles to new systems under development or to systems undergoing upgrades. For existing systems, organizations apply systems security and privacy engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems.

The application of systems security and privacy engineering principles helps organizations develop trustworthy, secure, and resilient systems and reduces the susceptibility to disruptions, hazards, threats, and the creation of privacy problems for individuals. Examples of system security engineering principles include: developing layered protections; establishing security and privacy policies, architecture, and controls as the foundation for design and development; incorporating security and privacy requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; tailoring controls to meet organizational needs; and performing threat modeling to identify use cases, threat agents, attack vectors and

patterns, design patterns, and compensating controls needed to mitigate risk.

Organizations that apply systems security and privacy engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risk to acceptable levels; and make informed risk management decisions. System security engineering principles can also be used to protect against certain supply chain risks, including incorporating tamper-resistant hardware into a design.

TxDOT Discussion

The following security engineering techniques help manage risks:

1. Anticipate the maximum possible ways that a product or service can be misused and abused in order to help identify how to protect the product or system from such uses. Address intended and unintended use scenarios in architecture and design;

2. Limit the number, size, and privilege levels of critical elements. Using criticality analysis will aid in determining which elements or functions are critical;

3. Use security mechanisms that help to reduce opportunities to exploit supply chain vulnerabilities, including, for example, encryption, access control, identity management, and malware or tampering discovery;

4. Design information system components and elements to be difficult to disable (e.g., tamper-proofing techniques) and, if disabled, trigger notification methods such as audit trails, tamper evidence, or alarms;

5. Design delivery mechanisms (e.g., downloads for software) to avoid unnecessary exposure or access to the supply chain infrastructure and the information systems/components traversing supply chain during delivery; and

6. Design relevant validation mechanisms to be used during implementation and operation. [Source: SP 800-161]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

Privacy Act; OMB A-130; FIPS 199, 200; NIST SP 800-37, 800-53A, 800-60-1, 800-60-2, 800-160-1, 800-218; NIST IR 8062; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

PL-08, PM-07, RA-02, RA-03, RA-09, SA-03, SA-04, SA-15, SA-17, SC-02, SC-03, SC-23, SC-39, SR-02, SR-03, SR-04, SR-05

SA-08(33) Minimization

Baselines

N/A

Overlays

CJIS; Privacy

Requirements

Implement the privacy principle of minimization using processes as defined in Std.01.

Implementation Standards

Std.01 —

a. Identify the minimum elements of personally identifiable information (PII) that are relevant and necessary to accomplish the legally authorized purpose of collection;

b. Limit the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and

c. Conduct an initial evaluation of PII holdings; and review those holdings at least biennially to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SA-08(33).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

The principle of minimization states that organizations should only process personally identifiable information that is directly relevant and necessary to accomplish an authorized purpose and should only maintain personally identifiable information for as long as is necessary to accomplish the purpose. Organizations have processes in place, consistent with applicable laws and policies, to implement the principle of minimization.

TxDOT Discussion

The minimum set of sensitive personal information (SPI) elements required to support a specific organization business process may be a subset of the SPI the organization is authorized to collect.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

Privacy Act; OMB A-130; FIPS 199, 200; NIST SP 800-37, 800-53A, 800-60-1, 800-60-2, 800-160-1; NIST IR 8062; CJIS Security Policy

Related Controls

PE-08, PM-25, SI-12

SA-09 External System Services

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: security and privacy controls as defined in TxDOT Information Security and Privacy Controls Standards Catalog and service level agreements (SLAs);

b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and

c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: processes, methods, and techniques as specified in contracts, SLAs, and the Continuous Monitoring Program (see CA-07).

Implementation Standards

Std.01 — Ensure that SLAs include:

a. Service definitions;

b. Delivery levels;

c. Security controls, including third-party personnel security, information classification, transmission, and authorization;

d. Aspects of service management, including monitoring, auditing, impacts to the organization's resilience, and change management; and

e. Issues of liability, reliability of services and response times for the provision of services. [Source: Hitrust 09.e Service Delivery]

Std.15 — Information resources assigned from or shared between one state agency to another or from or between a state agency to a contractor or other third party shall be protected in accordance with the conditions imposed by the providing state agency at a minimum. [Source: DIR Control Standards Catalog SA-9]

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.02 PCI — Rescinded in V3.0.

Std.03 PCI — Rescinded in V4.0.

Std.04 PCI —

a. Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems:

1. Network security controls.

2. IDS/IPS.

3. Change-detection mechanisms.

4. Anti-malware solutions.

5. Physical access controls.

6. Logical access controls.

7. Audit logging mechanisms.

8. Segmentation controls (if used).

9. Audit log review mechanisms.

10. Automated security testing tools (if used).

[Source: PCI DSS 10.7.2]

b. Failures of any critical security controls systems are responded to promptly, including but not limited to:

1. Restoring security functions.

2. Identifying and documenting the duration (date and time from start to end) of the security failure.

3. Identifying and documenting the cause(s) of failure and documenting required remediation.

4. Identifying and addressing any security issues that arose during the failure.

5. Determining whether further actions are required as a result of the security failure.

6. Implementing controls to prevent the cause of failure from reoccurring.

7. Resuming monitoring of security controls.

[Source: PCI DSS 10.7.3]

Std.05 PCI — A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided. [Source: PCI DSS 12.8.1]

Std.06 PCI — Written agreements with third-party service providers (TPSPs) are maintained as follows:

a. Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the Cardholder Data Environment (CDE).

b. Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.

[Source: PCI DSS 12.8.2]

Std.07 PCI — Information is maintained about which PCI DSS requirements are managed by each third-party service provider (TPSP), which are managed by the entity, and any that are shared between the TPSP and the entity. [Source: PCI DSS 12.8.5]

Std.08 PCI — Ensure that the following is included in contracts or SLAs for service providers: third-party service providers (TPSPs) acknowledge in writing to customers that they are responsible for the security of account data the TPSP possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's Cardholder Data Environment (CDE). [Source: PCI DSS 12.9.1]

Std.17 PCI — Additional requirement for issuers and companies that support issuing services and store sensitive authentication data:

Any storage of sensitive authentication data is:

a. Limited to that which is needed for a legitimate issuing business need and is secured.

b. Encrypted using strong cryptography.

[Source: PCI DSS 3.3.3]

Std.18 PCI — Ensure that the following is included in contracts or SLAs for service providers: Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and updating of such keys is documented and distributed to the service provider's customers. [Source: PCI DSS 3.7.9]

Std.19 PCI — Ensure that the following is included in contracts or SLAs for service providers: Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels. [Source: PCI DSS 11.5.1.1]

Std.20 PCI — Ensure that the following is included in contracts or SLAs for service providers: PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2. [Source: PCI DSS 12.5.2.1]

Std.21 PCI — Ensure that the following is included in contracts or SLAs for service providers: Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management. [Source: PCI DSS 12.5.3]

Std.22 PCI — Ensure that the following is included in contracts or SLAs for service providers: TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request:

a. PCI DSS compliance status information for any service the TPSP performs on behalf of customers (Requirement 12.8.4).

b. Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5).

[Source: PCI DSS 12.9.2]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.09 CJIS — The Contracting Government Agency (CGA) entering into an agreement with a contractor shall appoint an agency coordinator (AC). [Source: CJIS 3.2.6]

Std.10 CJIS — The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, and scheduling of initial training and testing. The AC shall:

a. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.

b. Participate in related meetings and provide input and comments for system improvement.

c. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.

d. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.

e. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).

f. Train or ensure the training of Contractor personnel.

g. Not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.

h. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.

i. Fulfill any other responsibility for the AC promulgated by the FBI. [Source: CJIS 3.2.7]

Std.11 CJIS —

Outsourcing Standards for Channelers: Channelers designated to request civil fingerprint-based background checks on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact Council Security and Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing. Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function and shall be subject to the same extent of audit review as are local user agencies. [Source: CJIS SA-09]

Std.12 CJIS —

Outsourcing Standards for Non-Channelers: Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function and shall be subject to the same extent of audit review as are local user agencies. [Source: CJIS SA-09]

Std.13 CJIS —

a. As specified in the interagency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed.

b. The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response.

c. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy. [Source: CJIS 5.1.2]

Std.14 CJIS —

a. Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI.

b. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change. [Source: CJIS 5.1.2.1]

Std.17 CJIS —

Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis:

a. All agencies having access to CJI shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations.

b. At a minimum, triennially audit all external service providers which have access to the information system in order to ensure compliance with applicable statutes, regulations, and policies.

c. Have the authority to conduct unannounced security inspections and scheduled audits of external service providers facilities. [Source: CJIS SA-09]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.16 FedRAMP —

a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: Appropriate FedRAMP Security Controls Baseline(s) if Federal information is processed or stored within the external system;

b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and

c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored.

[Source: FedRAMP Security Controls Baseline SA-9]

Discussion

External system services are provided by an external provider, and the organization has no direct control over the implementation of the required controls or the assessment of control effectiveness. Organizations establish relationships with external service providers in a variety of ways, including through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges. The responsibility for managing risks from the use of external system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a certain level of confidence that each provider in the consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust vary based on relationships between organizations and the external providers. Organizations document the basis for the trust relationships so that the relationships can be monitored. External system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define the expectations of performance for implemented controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-35, 800-160-1, 800-161, 800-171; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-20, CA-03, CA-07, CP-02, IR-04, IR-07, PL-10, PL-11, PS-07, SA-02, SA-04, SR-03, SR-05

SA-09(01) Risk Assessments and Organizational Approvals

Baselines

N/A

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

a. Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and

b. Verify that the acquisition or outsourcing of dedicated information security services is approved by personnel or roles as defined in the system and services acquisition policy.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Information security services include the operation of security devices, such as firewalls or key management services as well as incident monitoring, analysis, and response. Risks assessed can include system, mission or business, security, privacy, or supply chain risks.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

CA-06, RA-03, RA-08

SA-09(02) Identification of Functions, Ports, Protocols, and Services

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: all external systems and services that have a dedicated connection with TxDOT.

Implementation Standards

Std.01 — Ensure required functions, ports, protocols, and other services required for enabling the dedicated connection with TxDOT are:

a. Authorized in accordance with CA-03;

b. Documented in the System Security Plan (SSP); and

c. Appropriately whitelisted or blacklisted in accordance with configuration management policy and procedures.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: any system with a local, network, or remote connection to an agency information system. [Source: CJIS SA-09(02)]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.02 FedRAMP — Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: all external systems where Federal information is processed or stored. [Source: FedRAMP Security Controls Baseline SA-9(2)]

Discussion

Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be useful when the need arises to understand the trade-offs involved in restricting certain functions and services or blocking certain ports and protocols.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-35, 800-160-1, 800-161, 800-171; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CA-03, CM-06, CM-07

SA-09(05) Processing, Storage, and Service Location

Baselines

Moderate, High

Overlays

TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Restrict the location of information processing and data to facilities located within in the legal jurisdictional boundary of the United States based on data classification other than Public.

Implementation Standards

Std.04 — Information Owners and the Chief Information Officer must approve information other than public being processed or stored outside of the legal jurisdictional boundary of the United States.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

For systems subject to TX-RAMP Level 2 requirements, the following standard applies:

Std.03 TX-RAMP —

a. Require that third party service providers (TPSPs) disclose the location of information processing, information or data, and system services, including

whether or not located within in the legal jurisdictional boundary of the United States based on data classification other than Public.

b. Each instance of TxDOT information other than Public being processed or stored outside of the legal jurisdictional boundary of the United States must be approved by the relevant Information Owners and the TxDOT Chief Information Officer.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate baseline, the following standard applies:

Std.01 FedRAMP — Restrict the location of information processing, information or data, and system services to facilities located within in the legal jurisdictional boundary of the United States based on data classification other than Public. [Source: FedRAMP Security Controls Baseline SA-9(5)]

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.02 FedRAMP — Restrict the location of information processing, information or data, and system services to U.S./U.S. Territories or geographic locations where there is U.S. jurisdiction based on all High impact data, systems, or services. [Source: FedRAMP Security Controls Baseline SA-9(5)]

Discussion

The location of information processing, information and data storage, or system services can have a direct impact on the ability of organizations to successfully execute their mission and business functions. The impact occurs when external providers control the location of processing, storage, or services. The criteria that external providers use for the selection of processing, storage, or service locations may be different from the criteria that organizations use. For example, organizations may desire that data or information storage locations be restricted to certain locations to help facilitate incident response activities in case of information security incidents or breaches. Incident response activities, including forensic analyses and after-the-fact investigations, may be adversely affected by the governing laws, policies, or protocols in the locations where processing and storage occur and/or the locations from which system services emanate.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline

Related Controls

SA-05, SR-04

SA-10 Developer Configuration Management

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Require the developer of the system, system component, or system service to:

a. Perform configuration management during system, component, or service design, development, implementation, operation, and disposal;

b. Document, manage, and control the integrity of changes to all configuration items under configuration management;

c. Implement only organization-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and

e. Track security flaws and flaw resolution within the system, component, or service and report findings to personnel identified in the System Security Plan (SSP).

Implementation Standards

Std.01 — Rescinded in V2.4.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SA-10.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.02 FedRAMP — Track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel, to include FedRAMP. [Source: FedRAMP Security Controls Baseline SA-10]

Discussion

Organizations consider the quality and completeness of configuration management activities conducted by developers as direct evidence of applying effective security controls. Controls include protecting the master copies of material used to generate security-relevant portions of the system hardware, software, and firmware from unauthorized modification or destruction. Maintaining the integrity of changes to the system, system component, or system service requires strict configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.

The configuration items that are placed under configuration management include the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the current running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and source code with previous versions; and test fixtures and documentation. Depending on the mission and business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance stage of the system development life cycle.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 180, 202; NIST SP 800-128, 800-160-1; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CM-02, CM-03, CM-04, CM-07, CM-09, SA-04, SA-05, SA-08, SA-15, SI-02, SR-03, SR-04, SR-05, SR-06

SA-10(01) Software and Firmware Integrity Verification

Baselines

N/A

Overlays

TX-RAMP Level 2

Requirements

Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

None.

Discussion

Software and firmware integrity verification allows organizations to detect unauthorized changes to software and firmware components using developer-provided tools, techniques, and mechanisms. The integrity checking mechanisms can also address counterfeiting of software and firmware components. Organizations verify the integrity of software and firmware components, for example, through secure one-way hashes provided by developers. Delivered software and firmware components also include any updates to such components.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

None.

Related Controls

SI-07, SR-11

SA-11 Developer Testing and Evaluation

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; Privacy; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:

a. Develop and implement a plan for ongoing security and privacy control assessments;

b. Perform unit, integration, system, and regression testing/evaluation as specified in Std.01 at an organization-defined depth and coverage to include, at a minimum, the system components to be scanned and the vulnerabilities to be checked;

c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;

d. Implement a verifiable flaw remediation process; and

e. Correct flaws identified during testing and evaluation.

Implementation Standards

Std.01 — Perform testing at frequencies:

a. In accordance with the organization's defined System Development Life Cycle (SDLC);

b. Before being placed in the production environment; and

c. Whenever security-relevant modifications have been made to the information system subsequent to developer testing.

Std.02 — Include contractual language requiring developers of systems, components, or solutions to create and document security testing plans and test all required security controls.

Std.03 — Require developers to document and approve test plans that define responsibilities for parties involved and a comprehensive set of test transactions and test data that represents the various activities and conditions that will be encountered in processing.

Std.04 — For all moderate- or high-impact systems under development, ensure security test results are required elements in the acceptance criteria for the system.

Std.05 — For all moderate- or high-impact systems, ensure security test results are considered during the authorization to operate process (ATO).

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.06 PCI — Test data and test accounts are removed from system components before the system goes into production. [Source: PCI DSS 6.5.6]

Std.07 PCI — Rescinded in V3.0.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SA-11.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Developmental testing and evaluation confirms that the required controls are implemented correctly, operating as intended, enforcing the desired security and privacy policies, and meeting established security and privacy requirements. Security properties of systems and the privacy of individuals may be affected by the interconnection of system components or changes to those components. The interconnections or changes—including upgrading or replacing applications, operating systems, and firmware—may adversely affect previously implemented controls. Ongoing assessment during development allows for additional types of testing and evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as manual code review, security architecture review, and penetration testing, as well as and static analysis, dynamic analysis, binary analysis, or a hybrid of the three analysis approaches.

Developers can use the analysis approaches, along with security instrumentation and fuzzing, in a variety of tools and in source code reviews. The security and privacy assessment plans include the specific activities that developers plan to carry out, including the types of analyses, testing, evaluation, and reviews of software and firmware components; the degree of rigor to be applied; the frequency of the ongoing testing and evaluation; and the types of artifacts produced during those processes. The depth of testing

and evaluation refers to the rigor and level of detail associated with the assessment process. The coverage of testing and evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security and privacy assessment plans, flaw remediation processes, and the evidence that the plans and processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the system. Contracts may specify protection requirements for documentation.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

ISO 15408-3; NIST SP 800-30, 800-53A, 800-154, 800-160-1; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CA-02, CA-07, CM-04, SA-03, SA-04, SA-05, SA-08, SA-15, SA-17, SI-02, SR-05, SR-06

SA-11(01) Static Code Analysis

Baselines

Moderate, High

Overlays

PCI DSS; FedRAMP Moderate, FedRAMP High

Requirements

Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

Implementation Standards

Std.01 — Static code analysis must be a design requirement for all system, system component, or system service projects developed on behalf of the organization.

Std.02 — Require the developer to use only approved tools and libraries for static code analysis, and to address vulnerabilities discovered through use of those tools and libraries.

Std.03 — Require the developer to perform static code analysis in accordance with the organization's Software Development Life Cycle (SDLC).

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.04 PCI —

a. Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows:

1. Code reviews ensure code is developed according to secure coding guidelines.

2. Code reviews look for both existing and emerging software vulnerabilities.

3. Appropriate corrections are implemented prior to release.

[Source: PCI DSS 6.2.3]

b. If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:

1. Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices.

2. Reviewed and approved by management prior to release.

[Source: PCI DSS 6.2.3.1]

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.05 FedRAMP —

a. The service provider must document its methodology for reviewing newly developed code for the Service in its Continuous Monitoring Plan.

b. If Static code analysis cannot be performed (for example, when the source code is not available), then dynamic code analysis must be performed (see SA-11(8))

[Source: FedRAMP Security Controls Baseline SA-11(1)]

Discussion

Static code analysis provides a technology and methodology for security reviews and includes checking for weaknesses in the code as well as for the incorporation of libraries or other included code with known vulnerabilities or that are out-of-date and not supported. Static code analysis can be used to identify vulnerabilities and enforce secure coding practices. It is most effective when used early in the development process, when each code change can automatically be scanned for potential weaknesses. Static code analysis can provide clear remediation guidance and identify defects for developers to fix. Evidence of the correct implementation of static analysis can include aggregate defect density for critical defect types, evidence that defects were inspected by developers or security professionals, and evidence that defects were remediated. A high density of ignored findings, commonly referred to as false positives, indicates a potential problem with the analysis process or the analysis tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

ISO 15408-3; NIST SP 800-30, 800-53A, 800-154, 800-160-1; PCI DSS; FedRAMP Security Controls Baseline

Related Controls

None.

SA-11(02) Threat Modeling and Vulnerability Analyses

Baselines

Moderate, High

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that:

a. Uses the following contextual information: information from system categorization, risk assessment, vulnerability scans, risk register, and/or authority to operate (ATO);

b. Employs the following tools and methods: tools and methods equivalent to or more thorough than scans performed by the Department of Information Resources (DIR);

c. Conducts the modeling and analyses at the following level of rigor: at organization-defined depth and coverage to include, at a minimum, the system components to be scanned and the vulnerabilities checked; and

d. Produces evidence that meets the following acceptance criteria: requirements of controls including CA-02, and any applicable service level agreements (SLAs).

Implementation Standards

Std.01 — TxDOT, when implementing an Internet website or mobile application that processes any sensitive personal or personally identifiable information or confidential information must subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test. [Source: TGC 2054.516(a)(2)]

Std.02 — The developer of the system or system component must perform threat and vulnerabilities analyses and subsequent testing/evaluation of the as-built system, component or service.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Systems, system components, and system services may deviate significantly from the functional and design specifications created during the requirements and design stages of the system development life cycle. Therefore, updates to threat modeling and vulnerability analyses of those systems, system components, and system services during development and prior to delivery are critical to the effective operation of those systems, components, and services. Threat modeling and vulnerability analyses at this stage of the system development life cycle ensure that design and implementation changes have been accounted for and that vulnerabilities created because of those changes have been reviewed and mitigated.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

TGC 2054; DIR Security Control Standards Catalog

Federal References

ISO 15408-3; NIST SP 800-30, 800-53A, 800-154, 800-160-1; FedRAMP Security Controls Baseline

Related Controls

PM-15, RA-03, RA-05

SA-11(05) Penetration Testing

Baselines

Low, Moderate, High

Overlays

N/A

Requirements

Require the developer of the system, system component, or system service to perform penetration testing:

a. At the following level of rigor: organization-defined breadth and depth to include, at a minimum, the system components to be scanned and the vulnerabilities checked; and

b. Under the following constraints: constraints defined in Stds.01 & 02 below.

Implementation Standards

Std.01 — TxDOT, when implementing an Internet website or mobile application that processes any sensitive personal or personally identifiable information or confidential information must subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test. [Source: TGC 2054.516(a)(2)]

Std.02 — Require advanced coordination and formal authorization for all penetration testing on systems in the production environment. Authorization must include scope of test including, but not limited to, system components and planned actions.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Penetration testing is an assessment methodology in which assessors, using all available information technology product or system documentation and working under specific constraints, attempt to circumvent the implemented security and privacy features of information technology products and systems. Useful information for assessors who conduct penetration testing includes product and system design specifications, source code, and administrator and operator manuals. Penetration testing can include white-box, gray-box, or black-box testing with analyses performed by skilled professionals who simulate adversary actions. The objective of penetration testing is to discover vulnerabilities in systems, system components, and services that result from implementation errors, configuration faults, or other operational weaknesses or deficiencies. Penetration tests can be performed in conjunction with automated and manual code reviews to provide a greater level of analysis than would ordinarily be possible. When user session information and other personally identifiable information is captured or recorded during penetration testing, such information is handled appropriately to protect privacy.

TxDOT Discussion

Reporting on penetration testing should include the defined list of targets provided (IP addresses, protocols, services or applications, etc.); the specific commercial, public, and proprietary tools used; and, if applicable, evidence of successful exploitation or illustrations of exploitability where vulnerabilities exist.

TxDOT References

Information Security and Privacy Policy

State References

TGC 2054; DIR Security Control Standards Catalog

Federal References

ISO 15408-3; NIST SP 800-30, 800-53A, 800-154, 800-160-1

Related Controls

CA-08, PM-14, PM-25, PT-02, SA-03, SI-02, SI-06

SA-11(08) Dynamic Code Analysis

Baselines

Moderate, High

Overlays

PCI DSS

Requirements

Require the developer of the system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

Implementation Standards

Std.01 — TxDOT, when implementing an Internet website or mobile application that processes any sensitive personal or personally identifiable information or confidential information, must subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test. [Source: TGC 2054.516(a)(2)]

Std.02 — A security test and evaluation plan, including the use of dynamic code analysis at run-time, must be created and implemented for any information system developed on behalf of TxDOT.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.03 PCI — Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows:

a. Code reviews ensure code is developed according to secure coding guidelines.

b. Code reviews look for both existing and emerging software vulnerabilities.

c. Appropriate corrections are implemented prior to release.

[Source: PCI DSS 6.2.3]

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Dynamic code analysis provides runtime verification of software programs using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs runtime tools to ensure that security functionality performs in the way it was designed. A type of dynamic analysis, known as fuzz testing, induces program failures by deliberately introducing malformed or random data into software programs. Fuzz testing strategies are derived from the intended use of applications and the functional and design specifications for the applications. To understand the scope of dynamic code analysis and the assurance provided, organizations may also consider conducting code coverage analysis (i.e., checking the degree to which the code has been tested using metrics such as percent of subroutines tested or percent of program statements called during execution of the test suite) and/or concordance analysis (i.e., checking for words that are out of place in software code, such as non-English language words or derogatory terms).

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

TGC 2054; DIR Security Control Standards Catalog

Federal References

ISO 15408-3; NIST SP 800-30, 800-53A, 800-154, 800-160-1; PCI DSS

Related Controls

None.

SA-15 Development Process, Standards, and Tools

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Require the developer of the system, system component, or system service to follow a documented development process that:

1. Explicitly addresses security and privacy requirements;

2. Identifies the standards and tools used in the development process;

3. Documents the specific tool options and tool configurations used in the development process; and

4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Review the development process, standards, tools, tool options, and tool configurations at least annually to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: all applicable security and privacy requirements as identified in the System Security Plan (SSP).

Implementation Standards

Std.01 — Developers must follow processes identified in TxDOT's SDLC, which incorporates information security and privacy requirements.

Std.02 — SDLC processes must include provisions for documenting tool options and tool configurations.

Std.03 — Changes to tools and tool configurations in the TxDOT environment must be managed in accordance with CM-03.

Std.04 — Developers must self-assess and attest, or permit TxDOT to assess, the developer's process, standards, tools, and tool options/configurations as part of the source selection evaluation to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy all privacy and security requirements.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.07 CJIS — Review the development process, standards, tools, tool options, and tool configurations to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy security and privacy requirements during design, development, implementation, operation, and disposal. [Source: CJIS SA-15]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate baseline, the following standard applies:

Std.05 FedRAMP — Review the development process, standards, tools, tool options, and tool configurations at least annually to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: FedRAMP Security Authorization requirements. [Source: FedRAMP Security Controls Baseline SA-15]

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.06 FedRAMP — Review the development process, standards, tools, tool options, and tool configurations before first use and annually thereafter to

determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: FedRAMP Security Authorization requirements. [Source: FedRAMP Security Controls Baseline SA-15]

Discussion

Development tools include programming languages and computer-aided design systems. Reviews of development processes include the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes facilitates effective supply chain risk assessment and mitigation. Such integrity requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.

TxDOT Discussion

Specifications for the security control requirements include that security controls be incorporated in the information system, supplemented by manual controls as needed. These considerations are applied when evaluating software packages, developed or purchased. Security requirements and controls reflect the business value of the information assets involved, and the potential business damage that might result from a failure or absence of security. For purchased commercial products, a formal acquisition process is followed. Contracts with the supplier include the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement, then the risk introduced and associated controls are reconsidered prior to purchasing the product. Where additional functionality is supplied, and causes a security risk, this is disabled or mitigated through application of additional controls. The organization requires developers of information systems, components, and services to identify (document) early in the system development life cycle, the functions ports, protocols, and services intended for organizational use. [Source: Hitrust CSF 10.a Security Requirements Analysis and Specification]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-160-1; NIST IR 8179; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CM-03, MA-06, SA-03, SA-04, SA-08, SA-10, SA-11, SR-03, SR-04, SR-05, SR-06, SR-09

SA-15(03) Criticality Analysis

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Require the developer of the system, system component, or system service to perform a criticality analysis:

a. At the following decision points in the system development life cycle: at a minimum, prior to entering into a production environment and before issuing or renewing an ATO; and

b. At the following level of rigor: breadth and depth of criticality analysis specified in the SSDLC.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, SA-15(03)a is superseded by CJIS requirement SA-15(03)a:

Std.04 CJIS — Require the developer of the system, system component, or system service to perform a criticality analysis at the following decision points in the system development life cycle: design, development, implementation, and operational. [Source: CJIS SA-15(03)]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Criticality analysis performed by the developer provides input to the criticality analysis performed by organizations. Developer input is essential to organizational criticality analysis because organizations may not have access to detailed design documentation for system components that are developed as commercial off-the-shelf products. Such design documentation includes functional specifications, high-level designs, low-level designs, source code, and hardware schematics. Criticality analysis is important for organizational systems that are designated as high value assets. High value assets can be moderate- or high-impact systems due to heightened adversarial interest or potential adverse effects on the federal enterprise. Developer input is especially important when organizations conduct supply chain criticality analyses.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

RA-09

SA-16 Developer-provided Training

Baselines

High

Overlays

FedRAMP High

Requirements

Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: training defined in Std.01.

Implementation Standards

Std.01 — Require that training be provided as defined in Statements of Work (SOWs), to include, at a minimum, one of the following:

a. Role-based training for users, privileged users, admins, developers, security personnel, and others as specified (for example, trainers, support staff); or

b. Sufficient training materials for the organization to conduct in-house training or offer self-training to organizational personnel after initial system deployment.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Developer-provided training applies to external and internal (in-house) developers. Training personnel is essential to ensuring the effectiveness of the controls implemented within organizational systems. Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Organizations can also request training materials from developers to conduct in-house training or offer self-training to organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security and privacy functions, controls, and mechanisms.

TxDOT Discussion

Agencies may contract with external vendors to provide qualified instructors and necessary instruction material, as agreed, to train personnel (including contractors and partners as applicable) in the secure and cost-effective use of products or services. Training content must address all stages from installation through decommissioning and known inherent risks and mitigations as appropriate to audience.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FedRAMP Security Controls Baseline

Related Controls

AT-02, AT-03, PE-03, SA-04, SA-05

SA-17 Developer Security and Privacy Architecture and Design

Baselines

High

Overlays

FedRAMP High

Requirements

Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that:

a. Is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture;

b. Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; and

c. Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.

Implementation Standards

Std.01 — Ensure developers produce design specifications and security architectures consistent with the agency's security architecture as defined in PL-08 and enterprise architecture as defined in PM-07.

Std.02 — Statements of business requirements for new information systems (developed or purchased), or enhancements to existing information systems shall specify the requirements for security and privacy controls. [Source: Hitrust 10.a Security Requirements Analysis and Specification]

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Developer security and privacy architecture and design are directed at external developers, although they could also be applied to internal (in-house) development. In contrast, PL-08 is directed at internal developers to ensure that organizations develop a security and privacy architecture that is integrated with the enterprise architecture. The distinction between SA-17 and PL-08 is especially important when organizations outsource the development of systems, system components, or system services and when there is a requirement to demonstrate consistency with the enterprise architecture and security and privacy architecture of the organization. ISO 15408-2, ISO 15408-3, and SP 800-160-1 provide information on security architecture and design, including formal policy models, security-relevant components, formal and informal correspondence, conceptually simple design, and structuring for least privilege and testing.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

ISO 15408-2, 15408-3; NIST SP 800-160-1; FedRAMP Security Controls Baseline

Related Controls

PL-02, PL-08, PM-07, SA-03, SA-04, SA-08, SC-07

SA-21 Developer Screening

Baselines

N/A

Overlays

FedRAMP High

Requirements

Require that the developer of a system, system component, or system service intended to process data not classified as Public:

a. Has appropriate access authorizations as determined by assigned official government duties in Statements of Work or contracts; and

b. Satisfies the following additional personnel screening criteria: screening criteria as specified in contracts and SLAs.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Developer screening is directed at external developers. Internal developer screening is addressed by PS-03. Because the system, system component, or system service may be used in critical activities essential to the national or economic security interests of the United States, organizations have a strong interest in ensuring that developers are trustworthy. The degree of trust required of developers may need to be consistent with that of the individuals who access the systems, system components, or system services once deployed. Authorization and personnel screening criteria include clearances, background checks, citizenship, and nationality. Developer trustworthiness may also include a review and analysis of company ownership and relationships that the company has with entities that may potentially affect the quality and reliability of the systems, components, or services being developed. Satisfying the required access authorizations and personnel screening criteria includes providing a list of all individuals who are authorized to perform development activities on the selected system, system component, or system service so that organizations can validate that the developer has satisfied the authorization and screening requirements.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

PS-02, PS-03, PS-06, PS-07, SA-04, SR-06

SA-22 Unsupported System Components

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or

b. Provide the following options for alternative sources for continued support for unsupported components in-house support or support from external providers as specified in Statements of Work (SOWs).

Implementation Standards

Std.01 — Rescinded in V3.0.

Std.02 — The exception process must be followed for any unsupported components in the TxDOT environment of operations.

Std.03 — The support status of components must be documented in the System Security Plan (SSP) and system/component inventory.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, SA-22b is superseded by CJIS requirement SA-22b:

Std.04 CJIS — Provide the following options for alternative sources for continued support for unsupported components: original manufacturer support, or original contracted vendor support. [Source: CJIS SA-22]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in an opportunity for adversaries to exploit weaknesses in the installed components. Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.

Alternative sources for support address the need to provide continued support for system components that are no longer supported by the original manufacturers, developers, or vendors when such components remain essential to organizational mission and business functions. If necessary, organizations can establish in-house support by developing customized patches for critical software components or, alternatively, obtain the services of external providers who provide ongoing support for the designated unsupported components through contractual relationships. Such contractual relationships can include open-source software value-added vendors. The increased risk of using unsupported system components can be mitigated, for example, by prohibiting the connection of such components to public or uncontrolled networks, or implementing other forms of isolation.

TxDOT Discussion

Texas Government Code provides the following definition: a "legacy system" means a computer system or application program that is operated with obsolete or inefficient hardware or software technology. [Source: TGC 2054.571]

Legacy System Modernization Strategy

a. DIR shall, in collaboration with state agencies other than institutions of higher education, develop a legacy system modernization strategy to guide the state in legacy system modernization efforts.

b. The strategy must:

1. Plan for legacy system modernization statewide and at the agency level;

2. Establish a statewide application development framework;

3. Facilitate standardization and collaboration among state agencies; and

4. Promote the use of common technology solutions and collective purchasing by the state. [Source: TGC 2054.572a-b]

DIR's Legacy Modernization Guide provides information about legacy Application Portfolio Management (APM) and modernization strategies.

If systems or system components in production are no longer supported by the developer, vendor, or manufacturer, the organization must show evidence of a formal migration plan approved by management to replace the system or system component. [Source: Hitrust CSF 10.h Control of Operational Software] If replacement is not feasible, a mitigation plan must be developed.

TxDOT References

Information Security and Privacy Policy

State References

TGC 2054; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

CJIS Security Policy

Related Controls

PL-02, SA-03

SC — System and Communications Protection

SC-01 Policy and Procedures

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level system and communications protection policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;

b. Designate a senior management official as defined in the system and communications protection policy to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and

c. Review and update the current system and communications protection:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 1.1.1, 1.1.2, 4.1.1, and 4.1.2.

Std.03 PCI — Rescinded in V3.0.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.04 CJIS — Review and update the current system and communications protection policy and procedures following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. [Source: CJIS SC-01]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

System and communications protection policy and procedures address the controls in the SC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and communications protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and communications protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-12, 800-100; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

PM-09, PS-08, SA-08, SI-12

SC-02 Separation of System and User Functionality

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Separate user functionality, including user interface services, from system management functionality.

Implementation Standards

Std.01 — Design and configure systems to physically or logically separate user functionality from information storage and from management and administrative functionality, and to prevent users from performing any functions that are not explicitly authorized for their roles. Ensure that the functionality of one process or service given to one application does not enable the same functionality for another application.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SC-02.

Std.02 CJIS —Rescinded in V4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

System management functionality includes functions that are necessary to administer databases, network components, workstations, or servers. These

functions typically require privileged user access. The separation of user functions from system management functions is physical or logical. Organizations may separate system management functions from user functions by using different computers, instances of operating systems, central processing units, or network addresses; by employing virtualization techniques; or some combination of these or other methods. Separation of system management functions from user functions includes web administrative interfaces that employ separate authentication methods for users of any other system resources. Separation of system and user functions may include isolating administrative interfaces on different domains and with additional access controls. The separation of system and user functionality can be achieved by applying the systems security engineering design principles in SA-08, including SA-08(01), SA-08(03), SA-08(04), SA-08(10), SA-08(12), SA-08(13), SA-08(14), and SA-08(18).

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-06, SA-04, SA-08, SC-03, SC-07, SC-22, SC-39

SC-03 Security Function Isolation

Baselines

High

Overlays

FedRAMP High

Requirements

Isolate security functions from nonsecurity functions.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Security functions are isolated from nonsecurity functions by means of an isolation boundary implemented within a system via partitions and domains. The isolation boundary controls access to and protects the integrity of the hardware, software, and firmware that perform system security functions. Systems implement code separation in many ways, such as through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that protect the code on disk and address space protections that protect executing code. Systems can restrict access to security functions using access control mechanisms and by implementing least privilege capabilities. While the ideal is for all code within the defined security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include nonsecurity functions as an exception. The isolation of security functions from nonsecurity functions can be achieved by applying the systems security engineering design principles in SA-08, including SA-08(01), SA-08(03), SA-08(04), SA-08(10), SA-08(12), SA-08(13), SA-08(14), and SA-08(18).

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FedRAMP Security Controls Baseline

Related Controls

AC-03, AC-06, CM-02, CM-04, SA-04, SA-05, SA-08, SA-15, SA-17, SC-02, SC-07, SC-39, SI-16

SC-04 Information in Shared System Resources

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Prevent unauthorized and unintended information transfer via shared system resources.

Implementation Standards

Std.01 — Ensure that the information system does not share resources that are used to interface with systems operating at different security levels.

Std.02 — Ensure that system resources shared between two or more users are released back to the information system and are protected from accidental or purposeful disclosure.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SC-04.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Preventing unauthorized and unintended information transfer via shared system resources stops information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. Information in shared system resources also applies to encrypted representations of information. In other contexts, control of information in shared system resources is referred to as object reuse and residual information protection. Information in shared system resources does not address information remanence, which refers to the residual representation of data that has been nominally deleted; covert channels (including storage and timing channels), where shared system resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-03, AC-04, SA-08

SC-05 Denial-of-Service Protection

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Protect against or limit the effects of the following types of denial-of-service events: events as defined in Std.03; and

b. Employ the following controls to achieve the denial-of-service objective: controls as defined in Std.04.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The Department of Information Resources (DIR) will provide security information management services to include external network monitoring, scanning, and alerting for state organizations that utilize state information resources as specified in Chapters 2054 and 2059, Government Code. Perimeter security controls may include some or all of the following components: DMZ, firewall, intrusion detection or prevention system, or router. [Source: DIR Control Standards Catalog v1.3 SC-5]

Std.03 — Protect against denial-of-service events against which preventive or limiting measures must be taken, including:

a. Consumption of scarce, limited, or non-renewable resources;

b. Destruction or alteration of configuration information; and

c. Physical destruction or alteration of network components. [Source: SP 800-82]

Std.04 — Employ applicable compensating controls, including:

a. The use of tools and configuration settings at boundaries to prevent denial of service events, including:

1. IDS/IPS;

2. Packet filtering; and

3. Bandwidth limiting.

b. Monitoring;

c. Operating in "safe mode" upon loss of communication;

d. Alternate communications services;

e. Securing and separating configuration backups; and

f. Alternate processing sites and services.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SC-05.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.05 FedRAMP — Protect against the effects of the following types of denial-of-service events: at a minimum: ICMP (ping) flood, SYN flood, slowloris, buffer overflow attack, and volume attack. [Source: FedRAMP Security Controls Baseline SC-5]

Discussion

Denial-of-service events may occur due to a variety of internal and external causes, such as an attack by an adversary or a lack of planning to support organizational needs with respect to capacity and bandwidth. Such attacks can occur across a wide range of network protocols (e.g., IPv4, IPv6). A variety of technologies are available to limit or eliminate the origination and effects of denial-of-service events. For example, boundary protection devices can filter certain types of packets to protect system components on internal networks from being directly affected by or the source of denial-of-service attacks. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial-of-service events.

TxDOT Discussion

Specific details about event types can be found at us-cert.gov, https://nvd.nist.gov/home, or other sources of threat intelligence per PM-16.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-189; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CP-02, IR-04, PM-16, SC-07

SC-07 Boundary Protection

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;

b. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks; and

c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

Implementation Standards

Std.01 — System Security Plans (SSPs) must include:

a. A complete, up-to-date network diagram and/or inventory of the system's boundaries;

b. Logging frequency to review logs and security events for all servers and system components providing security functions (for example, firewalls,

intrusion-detection systems/intrusion prevention systems) to identify anomalies or suspicious activity; and

c. Methods to prevent the unauthorized release of information outside the information system boundary if an operational failure of the boundary protection mechanisms occurs.

Std.02 — Network communications must deny all by default and permit by exception for both inbound and outbound network communications traffic.

Std.03 — Separate subnetworks should be established as separate physical network interfaces for publicly-accessible system components.

Std.04 — Inbound traffic from untrusted networks to trusted networks is restricted to:

a. Communications with system components that are authorized to provide publicly accessible services, protocols, and ports.

b. Stateful responses to communications initiated by system components in a trusted network.

c. All other traffic is denied.

[Source: PCI DSS 1.4.2]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 1.2.3 and 1.4.2.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.05 PCI — Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network. [Source: PCI DSS 1.4.3]

Std.06 PCI — The disclosure of internal IP addresses and routing information is limited to only authorized parties. [Source: PCI DSS 1.4.5]

Std.07 PCI — For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following:

a. Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks.

b. Actively running and up to date as applicable.

c. Generating audit logs.

d. Configured to either block web-based attacks or generate an alert that is immediately investigated.

[Source: PCI DSS 6.4.2]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SC-07.

Std.07 CJIS —Rescinded in V4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture. Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational systems includes restricting external web traffic to designated web servers within managed interfaces, prohibiting external traffic that appears to be spoofing internal addresses, and prohibiting internal traffic that appears to be spoofing external addresses. SP 800-189 provides additional information on source address validation techniques to prevent ingress and egress of traffic with spoofed addresses. Commercial telecommunications services are provided by network components and consolidated management systems shared by customers. These services may also include third party-provided access lines and other service elements. Such services may represent sources of increased risk despite contract security provisions. Boundary protection may be implemented as a common control for all or part of an organizational network such that the boundary to be protected is greater than a system-specific boundary (i.e., an authorization boundary).

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

SC-7(b) should be met by subnet isolation. A subnetwork (subnet) is a physically or logically segmented section of a larger network defined at TCP/IP Layer 3, to both minimize traffic and, important for a FedRAMP Authorization, add a crucial layer of network isolation. Subnets are distinct from VLANs (Layer 2), security groups, and VPCs and are specifically required to satisfy SC-7 part b and other controls. See the FedRAMP Subnets White Paper (https://www.fedramp.gov/assets/resources/documents/FedRAMP_subnets_white_paper.pdf) for additional information. [Source: FedRAMP Security Controls Baseline SC-7]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-04, AC-17, AC-18, AC-19, AC-20, CA-03, CM-02, CM-04, CM-07, CM-10, CP-08, CP-10, IR-04, MA-04, PE-03, PL-08, PM-12, SA-08, SA-17, SC-05

SC-07(03) Access Points

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Limit the number of external network connections to the system.

Implementation Standards

Std.01 — Document, verify and control connections to and use of external systems. [Source: SP 800-171 3.1.21/ CSF ID.AM-4]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SC-07(03).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Limiting the number of external network connections facilitates monitoring of inbound and outbound communications traffic. The Trusted Internet Connection DHS TIC initiative is an example of a federal guideline that requires limits on the number of external network connections. Limiting the number of external network connections to the system is important during transition periods from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). Such transitions may require implementing the older and newer technologies simultaneously during the transition period and thus increase the number of access points to the system.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

SC-07(04) External Telecommunications Services

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Implement a managed interface for each external telecommunication service;

b. Establish a traffic flow policy for each managed interface;

c. Protect the confidentiality and integrity of the information being transmitted across each interface;

d. Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;

e. Review exceptions to the traffic flow policy at least once every 180 days and upon implementation of a major new system and remove exceptions that are no longer supported by an explicit mission or business need;

f. Prevent unauthorized exchange of control plane traffic with external networks;

g. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and

h. Filter unauthorized control plane traffic from external networks.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.03 CJIS — Review exceptions to the traffic flow policy after any incident. [Source: CJIS SC-07(04)]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate baseline, the following standard applies:

Std.01 FedRAMP — Review exceptions to the traffic flow policy at least every 180 days or whenever there is a change in the threat environment that warrants a review of the exceptions and remove exceptions that are no longer supported by an explicit mission or business need. [Source: FedRAMP Security Controls Baseline SC-7(4)]

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.02 FedRAMP — Review exceptions to the traffic flow policy at least every ninety (90) days or whenever there is a change in the threat environment that warrants a review of the exceptions and remove exceptions that are no longer supported by an explicit mission or business need. [Source: FedRAMP Security Controls Baseline SC-7(4)]

Discussion

External telecommunications services can provide data and/or voice communications services. Examples of control plane traffic include Border Gateway Protocol (BGP) routing, Domain Name System (DNS), and management protocols. See SP 800-189 for additional information on the use of the resource public key infrastructure (RPKI) to protect BGP routes and detect unauthorized BGP announcements.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-03, SC-08, SC-20, SC-21, SC-22

SC-07(05) Deny by Default — Allow by Exception

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Deny network communications traffic by default and allow network communications traffic by exception at managed interfaces.

Implementation Standards

Std.01 —

a. Inbound traffic to the Cardholder Data Environment (CDE) is restricted as follows:

1. To only traffic that is necessary.

2. All other traffic is specifically denied.

[Source: PCI DSS 1.3.1]

b. Outbound traffic from the Cardholder Data Environment (CDE) is restricted as follows:

1. To only traffic that is necessary.

2. All other traffic is specifically denied.

[Source: PCI DSS 1.3.2]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 1.3.1 and 1.3.2.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.02 PCI — Network Security Controls (NSCs) are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that:

a. All wireless traffic from wireless networks into the CDE is denied by default.

b. Only wireless traffic with an authorized business purpose is allowed into the CDE.

[Source: PCI DSS 1.3.3]

Std.03 PCI — Rescinded in V3.0.

Std.04 PCI — Rescinded in V3.0.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.06 CJIS — Deny network communications traffic by default and allow network communications traffic by exception at boundary devices for information systems used to process, store, or transmit CJI. [Source: CJIS SC-07(05)]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard supersedes TxDOT requirement SC-07(05):

Std.05 FedRAMP — Deny network communications traffic by default and allow network communications traffic by exception for any systems. [Source: FedRAMP Security Controls Baseline SC-7(5)]

Discussion

Denying by default and allowing by exception applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections that are essential and approved are allowed. Deny by default, allow by exception also applies to a system that is connected to an external system.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

For Joint Authorization Board (JAB) Authorization, Cloud Service Providers (CSPs) shall include details of this control in their Architecture Briefing. [Source: FedRAMP Security Controls Baseline SC-7(5)]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

SC-07(07) Split Tunneling for Remote Devices

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using the following organization-defined safeguards: split tunneling is not authorized.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SC-07(07).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Split tunneling is the process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices and simultaneously, access uncontrolled networks. Split tunneling might be desirable by remote users to communicate with local system resources, such as printers or file servers. However, split tunneling can facilitate unauthorized external connections, making the system vulnerable to attack and to exfiltration of organizational information. Split tunneling can be prevented by disabling configuration settings that allow such capability in remote devices and by preventing those configuration settings from being configurable by users. Prevention can also be achieved by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. A virtual private network (VPN) can be used to securely provision a split tunnel. A securely provisioned VPN includes locking connectivity to exclusive, managed, and named environments, or to a specific set of pre-approved addresses, without user control.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

SC-07(08) Route Traffic to Authenticated Proxy Servers

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; FedRAMP Moderate, FedRAMP High

Requirements

Route all internal communications traffic to any external networks through authenticated proxy servers at managed interfaces.

Implementation Standards

None.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.01 PCI — Network Security Controls (NSCs) are implemented between trusted and untrusted networks. [Source: PCI DSS 1.4.1]

CJIS Correspondence

For systems processing CJIS data, SC-07(08) is superseded by CJIS requirement SC-07(08):

Std.02 CJIS — Route all internal communications traffic that may be proxied, except traffic specifically exempted by organizational personnel with information security responsibilities, to all untrusted networks through

authenticated proxy servers at managed interfaces.[Source: CJIS SC-07(08)]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

External networks are networks outside of organizational control. A proxy server is a server (i.e., system or application) that acts as an intermediary for clients requesting system resources from non-organizational or other organizational servers. System resources that may be requested include files, connections, web pages, or services. Client requests established through a connection to a proxy server are assessed to manage complexity and provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers that provide access to the Internet. Proxy servers can support the logging of Transmission Control Protocol sessions and the blocking of specific Uniform Resource Locators, Internet Protocol addresses, and domain names. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites. Note that proxy servers may inhibit the use of virtual private networks (VPNs) and create the potential for "man-in-the-middle" attacks (depending on the implementation).

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-03

SC-07(10) Prevent Exfiltration

Baselines

N/A

Overlays

FedRAMP High

Requirements

a. Prevent the exfiltration of information; and

b. Conduct exfiltration tests at a minimum, once per year.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Prevention of exfiltration applies to both the intentional and unintentional exfiltration of information. Techniques used to prevent the exfiltration of information from systems may be implemented at internal endpoints, external boundaries, and across managed interfaces and include adherence to protocol formats, monitoring for beaconing activity from systems, disconnecting external network interfaces except when explicitly needed,

employing traffic profile analysis to detect deviations from the volume and types of traffic expected, call backs to command and control centers, conducting penetration testing, monitoring for steganography, disassembling and reassembling packet headers, and using data loss and data leakage prevention tools. Devices that enforce strict adherence to protocol formats include deep packet inspection firewalls and Extensible Markup Language (XML) gateways. The devices verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices that operate at the network or transport layers. The prevention of exfiltration is similar to data loss prevention or data leakage prevention and is closely associated with cross-domain solutions and system guards that enforce information flow requirements.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

AC-02, CA-08, SI-03

SC-07(12) Host-Based Protection

Baselines

N/A

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

Implement Host Intrusion Prevention System (HIPS), Host Intrusion Detection System (HIDS), or minimally a host-based firewall at external

managed interfaces to the system and at key internal managed interfaces within the system.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Host-based boundary protection mechanisms include host-based firewalls. System components that employ host-based boundary protection mechanisms include servers, workstations, notebook computers, and mobile devices.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

SC-07(18) Fail Secure

Baselines

High

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Fail secure is a condition achieved by employing mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces, systems do not enter into unsecure states where intended security properties no longer hold. Managed interfaces include routers, firewalls, and application gateways that reside on protected subnetworks (commonly referred to as demilitarized zones). Failures of boundary protection devices cannot lead to or cause information external to the devices to enter the devices nor can failures permit unauthorized information releases.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; FedRAMP Security Controls Baseline

Related Controls

CP-02, SC-24

SC-07(20) Dynamic Isolation and Segregation

Baselines

N/A

Overlays

FedRAMP High

Requirements

Provide the capability to dynamically isolate system components as defined in System Security Plans (SSPs) supporting all organizational missions or business functions from other system components.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

The capability to dynamically isolate certain internal system components is useful when it is necessary to partition or separate system components of questionable origin from components that possess greater trustworthiness. Component isolation reduces the attack surface of organizational systems. Isolating selected system components can also limit the damage from successful attacks when such attacks occur.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

SC-07(21) Isolation of System Components

Baselines

High

Overlays

PCI DSS; FedRAMP High

Requirements

Employ boundary protection mechanisms to isolate system components as defined in System Security Plans (SSPs) supporting all organizational missions or business functions.

Implementation Standards

None.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.01 PCI — System components that store cardholder data are not directly accessible from untrusted networks. [Source: PCI DSS 1.4.4]

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Organizations can isolate system components that perform different mission or business functions. Such isolation limits unauthorized information flows among system components and provides the opportunity to deploy greater levels of protection for selected system components. Isolating system components with boundary protection mechanisms provides the capability for increased protection of individual system components and to more effectively control information flows between those components. Isolating system components provides enhanced protection that limits the potential harm from hostile cyber-attacks and errors. The degree of isolation varies depending upon the mechanisms chosen. Boundary protection mechanisms include routers, gateways, and firewalls that separate system components into physically separate networks or subnetworks; cross-domain devices that separate subnetworks; virtualization techniques; and the encryption of information flows among system components using distinct encryption keys.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; PCI DSS; FedRAMP Security Controls Baseline

Related Controls

CA-09

SC-07(24) Personally Identifiable Information

Baselines

N/A

Overlays

CJIS; PCI DSS; Privacy

Requirements

For systems that process personally identifiable information:

a. Apply the following processing rules to data elements of personally identifiable information: processing rules in accordance with PT-02;

b. Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system;

c. Document each processing exception; and

d. Review and remove exceptions that are no longer supported.

Implementation Standards

Std.01 — Document processing rules in the System Security Plan (SSP).

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.02 PCI — An accurate data-flow diagram(s) is maintained that meets the following:

a. Shows all account data flows across systems and networks.

b. Updated as needed upon changes to the environment.

[Source: PCI DSS 1.2.4]

Std.03 PCI — Primary account number (PAN) is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the bank identification number (BIN) and last four digits of the PAN.
[Source: PCI DSS 3.4.1]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SC-07(24).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Managing the processing of personally identifiable information is an important aspect of protecting an individual's privacy. Applying, monitoring for, and documenting exceptions to processing rules ensure that personally identifiable information is processed only in accordance with established privacy requirements.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; FIPS 199; NIST SP 800-37, 800-41, 800-77, 800-189; PCI DSS; CJIS Security Policy

Related Controls

PT-02

SC-08 Transmission Confidentiality and Integrity

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Protect the confidentiality and integrity of transmitted information.

Implementation Standards

Std.01 — Moved to SC-08(01) Std.02 in V2.2.1 errata.

Std.02 — Moved to SC-08(01) Std.03 in V2.2.1 errata.

Std.03 — Rescinded in V2.2.1 errata.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.04 CJIS — Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other

commercial purposes by any cloud service provider or other associated entity. [Source: CJIS SC-08]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Protecting the confidentiality and integrity of transmitted information applies to internal and external networks as well as any system components that can transmit information, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of information can be accomplished by physical or logical means. Physical protection can be achieved by using protected distribution systems. A protected distribution system is a wireline or fiber-optics telecommunications system that includes terminals and adequate electromagnetic, acoustical, electrical, and physical controls to permit its use for the unencrypted transmission of classified information. Logical protection can be achieved by employing encryption techniques.

Organizations that rely on commercial providers who offer transmission services as commodity services rather than as fully dedicated services may find it difficult to obtain the necessary assurances regarding the implementation of needed controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality or integrity services are available in standard, commercial telecommunications service packages. If it is not feasible to obtain the necessary controls and assurances of control effectiveness through appropriate contracting vehicles, organizations can implement appropriate compensating controls.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

For each instance of data in transit, confidentiality AND integrity should be through cryptography as specified in SC-8(1), physical means as specified in SC-8(5), or in combination.

For clarity, this control applies to all data in transit. Examples include the following data flows:

a. Crossing the system boundary;

b. Between compute instances - including containers;

c. From a compute instance to storage;

d. Replication between availability zones;

e. Transmission of backups to storage;

f. From a load balancer to a compute instance;

g. Flows from management tools required for their work – e.g. log collection, scanning, etc.

[Source: FedRAMP Security Controls Baseline SC-8]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 197; NIST SP 800-52, 800-77, 800-81-2, 800-113, 800-177; NIST IR 8023; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-17, AC-18, AU-10, IA-03, IA-08, MA-04, PE-04, SA-04, SA-08, SC-07, SC-20, SC-23, SC-28

SC-08(01) Cryptographic Protection

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; Sensitive; TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission.

Implementation Standards

Std.01 — Rescinded in V2.2.1 errata.

Std.02 — Rescinded in V3.0.

Std.03 — Sensitive information that is transmitted over a public network (e.g., the Internet) must be encrypted.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.04 PCI — Strong cryptography and security protocols are implemented as follows to safeguard primary account number (PAN) during transmission over open, public networks:

a. Only trusted keys and certificates are accepted.

b. Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. This bullet is a best practice until its effective date; refer to applicability notes below for details.

c. The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations.

d. The encryption strength is appropriate for the encryption methodology in use.

[Source: PCI DSS 4.2.1]

Std.05 PCI — Primary account number (PAN) is secured with strong cryptography whenever it is sent via end-user messaging technologies. [Source: PCI DSS 4.2.2]

Std.08 PCI — An inventory of the entity's trusted keys and certificates used to protect primary account number (PAN) during transmission is maintained. [Source: PCI DSS 4.2.1.1]

Std.09 PCI — Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following:

a. An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used.

b. Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use.

c. A documented strategy to respond to anticipated changes in cryptographic vulnerabilities.

[Source: PCI DSS 12.3.3]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SC-08(01).

Std.06 CJIS — Rescinded in V4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.07 FedRAMP — Please ensure SSP Section 10.3 Cryptographic Modules Implemented for Data At Rest (DAR) and Data In Transit (DIT) is fully populated for reference in this control. [Source: FedRAMP Security Controls Baseline SC-8(1)]

Discussion

Encryption protects information from unauthorized disclosure and modification during transmission. Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and IPSec. Cryptographic mechanisms used to protect information integrity include cryptographic hash functions that have applications in digital signatures, checksums, and message authentication codes.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

See M-22-09, including "Agencies encrypt all DNS requests and HTTP traffic within their environment"

SC-8(1) applies when encryption has been selected as the method to protect confidentiality and integrity. Otherwise refer to SC-8(5). SC-8(1) is strongly encouraged.

Note that this enhancement requires the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13.)

When leveraging encryption from the underlying IaaS/PaaS: While some IaaS/PaaS services provide encryption by default, many require encryption to be configured, and enabled by the customer. The Cloud Service Provider (CSP) has the responsibility to verify encryption is properly configured.

[Source: FedRAMP Security Controls Baseline SC-8(1)]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 197; NIST SP 800-52, 800-77, 800-81-2, 800-113, 800-177; NIST IR 8023; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

SC-12, SC-13

SC-10 Network Disconnect

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Terminate the network connection associated with a communications session at the end of the session or after the period defined in Std.01 of inactivity.

Implementation Standards

Std.01 —

a. Configure network connections to disconnect according to the following guide:

1. For low baseline: 60 minutes of inactivity;

2. For moderate baseline: 30 minutes of inactivity;

3. For high baseline: 10 minutes of inactivity.

b. Require re-authentication before allowing access to the system after the network connection has been terminated due to inactivity.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SC-10.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate baseline, the following standard applies:

Std.02 FedRAMP — Terminate the network connection associated with a communications session at the end of the session or after no longer than ten (10) minutes for privileged sessions and no longer than fifteen (15) minutes for user sessions of inactivity. [Source: FedRAMP Security Controls Baseline SC-10]

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Network disconnect applies to internal and external networks. Terminating network connections associated with specific communications sessions includes de-allocating TCP/IP address or port pairs at the operating system level and de-allocating the networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. Periods of inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-17, SC-23

SC-12 Cryptographic Key Establishment and Management

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: SC-13 and applicable System Security Plans (SSPs).

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — For websites and mobile applications, only procure, or otherwise implement, certificates from PKI Service Providers that appear on the DIR "Approved List of PKI Service Providers." [Source: 1 TAC 203.25(b)]

Std.03 — Protect all cryptographic keys against modification, loss, and destruction; protect secret and private keys against unauthorized disclosure. Limit cryptographic keys to the fewest number of custodians necessary. Physically protect equipment used to generate, store, and archive keys, and store encryption keys separately from encrypted data. [Source: Hitrust 10.g Key Management]

Std.04 — For Web and mobile apps, the name on the certificate should match the fully qualified domain name (FQDN) of the website.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 3.6.1.3.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.05 PCI — Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include:

a. Access to keys is restricted to the fewest number of custodians necessary.

b. Key-encrypting keys are at least as strong as the data-encrypting keys they protect.

c. Key-encrypting keys are stored separately from data-encrypting keys.

d. Keys are stored securely in the fewest possible locations and forms.

[Source: PCI DSS 3.6.1]

Std.06 PCI — Secret and private keys used to encrypt/decrypt stored account data are stored in one (or more) of the following forms at all times:

a. Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key.

b. Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device.

c. As at least two full-length key components or key shares, in accordance with an industry-accepted method.

[Source: PCI DSS 3.6.1.2]

Std.07 PCI — Cryptographic keys are stored in the fewest possible locations. [Source: PCI DSS 3.6.1.4]

Std.08 PCI — Key-management policies and procedures are implemented to include:

a. Generation of strong cryptographic keys used to protect stored account data. [Source: PCI DSS 3.7.1]

b. Secure distribution of cryptographic keys used to protect stored account data. [Source: PCI DSS 3.7.2]

c. Secure storage of cryptographic keys used to protect stored account data. [Source: PCI DSS 3.7.3]

d. The retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when:

1. The key has reached the end of its defined cryptoperiod.

2. The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known.

3. The key is suspected of or known to be compromised.

e. Retired or replaced keys are not used for encryption operations.

[Source: PCI DSS 3.7.5]

f. Prevention of unauthorized substitution of cryptographic keys. [Source: PCI DSS 3.7.7]

g. Cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities. [Source: PCI DSS 3.7.8]

Std.10 PCI — Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their

cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following:

a. A defined cryptoperiod for each key type in use.

b. A process for key changes at the end of the defined cryptoperiod.

[Source: PCI DSS 3.7.4]

Std.11 PCI — Where manual cleartext cryptographic key-management operations are performed by personnel, key-management policies and procedures are implemented include managing these operations using split knowledge and dual control. [Source: PCI DSS 3.7.6]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.12 CJIS — Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: encryption key generation, distribution, storage, access, and destruction is controlled by the agency. [Source: CJIS SC-12]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.09 FedRAMP — Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: In accordance with Federal requirements. [Source: FedRAMP Security Controls Baseline SC-12]

Discussion

Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and specify appropriate options, parameters, and levels. Organizations manage trust stores to ensure that only approved trust anchors are part of such trust stores. This includes

certificates with visibility external to organizational systems and certificates related to the internal operations of systems. NIST CMVP and NIST CAVP provide additional information on validated cryptographic modules and algorithms that can be used in cryptographic key management and establishment.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

Must meet applicable Federal Cryptographic Requirements. See References Section of control.

Wildcard certificates may be used internally within the system, but are not permitted for external customer access to the system.

[Source: FedRAMP Security Controls Baseline SC-12]

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 203; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140; NIST SP 800-56A, 800-56B, 800-56C, 800-57-1, 800-57-2, 800-57-3, 800-63-3; NIST IR 7956, 7966; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-17, AU-09, AU-10, CM-03, IA-03, IA-07, SA-04, SA-08, SA-09, SC-08, SC-13, SC-17, SC-20, SI-03, SI-07

SC-12(01) Availability

Baselines

High

Overlays

FedRAMP High

Requirements

Maintain availability of information in the event of the loss of cryptographic keys by users.

Implementation Standards

Std.01 — Mechanisms must be employed to:

a. Prohibit the use of encryption keys that are not recoverable by authorized personnel;

b. Require approval by senior management (as defined in applicable System Security Plans (SSPs)) to authorize recovery of keys by other than the key owner; and

c. Comply with approved cryptography standards (see SC-13).

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Escrowing of encryption keys is a common practice for ensuring availability in the event of key loss. A forgotten passphrase is an example of losing a cryptographic key.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FIPS 140; NIST SP 800-56A, 800-56B, 800-56C, 800-57-1, 800-57-2, 800-57-3, 800-63-3; NIST IR 7956, 7966; FedRAMP Security Controls Baseline

Related Controls

SC-13

SC-13 Cryptographic Protection

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Determine the cryptographic uses in accordance with Stds.01-04; and

b. Implement the following types of cryptography required for each specified cryptographic use: TxDOT systems with Sensitive, Confidential or Regulated data must implement encryption in accordance with Std.05.

Implementation Standards

Std.01 — Encryption requirements for information storage devices and data transmissions, as well as specific requirements for portable devices, removable media, and encryption key standards and management, shall be based on documented TxDOT risk management decisions. [Source: DIR Control Standards Catalog SC-13]

Std.02 — Sensitive, Confidential or Regulated information that is transmitted over a public network (e.g., the Internet) must be encrypted. [Source: DIR Control Standards Catalog SC-13]

Std.03 — Sensitive, Confidential or Regulated information stored in a public location that is directly accessible without compensating controls in place (e.g., FTP without access control) must be encrypted. [Source: DIR Control Standards Catalog SC-13]

Std.04 — Confidential or regulated information must be encrypted if copied to, or stored on, a portable computing device, removable media, or a non-TxDOT owned computing device. [Source: DIR Control Standards Catalog SC-13]

Std.05 — TxDOT systems must implement encryption algorithms to the level recommend by the Commercial National Security Algorithm (CNSA) Suite: https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

Std.06 — Rescinded in V3.0.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.07 PCI — Ensure that the following is included in contracts or SLAs for service providers: A documented description of the cryptographic architecture is maintained that includes:

a. Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date.

b. Preventing the use of the same cryptographic keys in production and test environments.

c. Description of the key usage for each key.

d. Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in Requirement 12.3.4.

[Source: PCI DSS 3.6.1.1]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirements SC-13 and 5.20.1.1.

Std.08 CJIS — Rescinded in V3.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Cryptography can be employed to support a variety of security solutions, including the protection of classified information and controlled unclassified information, the provision and implementation of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances but lack the necessary formal access approvals. Cryptography can also be used to support random number and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. For example, organizations that need to protect classified information may specify the use of NSA-approved cryptography. Organizations that need to provision and implement digital signatures may specify the use of FIPS-validated cryptography. Cryptography is implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

TxDOT Discussion

Storing Sensitive, Confidential or Regulated information on portable devices is discouraged.

TxDOT may also choose to implement additional protections, which may include encryption, for other data classifications. [Source: DIR Control Standards Catalog SC-13]

Note for systems subject to FedRAMP Requirements:

This control applies to all use of cryptography. In addition to encryption, this includes functions such as hashing, random number generation, and key generation. Examples include the following:

a. Encryption of data;

b. Decryption of data;

c. Generation of one time passwords (OTPs) for MFA;

d. Protocols such as TLS, SSH, and HTTPS.

The requirement for FIPS 140 validation, as well as timelines for acceptance of FIPS 140-2, and 140-3 can be found at the NIST Cryptographic Module Validation Program (CMVP).

https://csrc.nist.gov/projects/cryptographic-module-validation-program

For NSA-approved cryptography, the National Information Assurance Partnership (NIAP) oversees a national program to evaluate Commercial IT Products for Use in National Security Systems. The NIAP Product Compliant List can be found at the following location:

https://www.niap-ccevs.org/Product/index.cfm

When leveraging encryption from underlying IaaS/PaaS: While some IaaS/PaaS provide encryption by default, many require encryption to be configured, and enabled by the customer. The CSP has the responsibility to verify encryption is properly configured.

Moving to non-FIPS CM or product is acceptable when:

a. FIPS validated version has a known vulnerability;

b. Feature with vulnerability is in use;

c. Non-FIPS version fixes the vulnerability;

d. Non-FIPS version is submitted to NIST for FIPS validation;

e. POA&M is added to track approval, and deployment when ready.

At a minimum, this control applies to cryptography in use for the following controls: AU-9(3), CP-9(8), IA-2(6), IA-5(1), MP-5, SC-8(1), and SC-28(1).

[Source: FedRAMP Security Controls Baseline SC-13]

Note for systems subject to CJIS requirements:

Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-3 compliancy can be used in the interim until certification is complete. FIPS 140-2 certificates will not be acceptable after September 21, 2026. [Source: CJIS SC-13]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-02, AC-03, AC-07, AC-17, AC-18, AC-19, AU-09, AU-10, CM-11, CP-09, IA-03, IA-05, IA-07, MA-04, MP-02, MP-04, MP-05, SA-04, SA-08, SA-09, SC-08, SC-12, SC-20, SC-23, SC-28, SI-03, SI-07

SC-15 Collaborative Computing Devices and Applications

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: centrally managed dedicated devices located in TxDOT-managed facilities for which remote activation is approved and documented in System Security Plans (SSPs); and

b. Provide an explicit indication of use to users physically present at the devices.

Implementation Standards

Std.01 — Collaborative computing devices must be disconnected by default and provide at least one explicit indicator of use when powered on and connected.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, SC-15s is superseded by CJIS requirement SC-15a:

Std.04 CJIS — Prohibit remote activation of collaborative computing devices and applications. [Source: CJIS SC-15]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standards apply:

Std.02 FedRAMP —

a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: no exceptions for computing devices; and

b. Provide an explicit indication of use to users physically present at the devices.

[Source: FedRAMP Security Controls Baseline SC-15]

Std.03 FedRAMP — The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use. [Source: FedRAMP Security Controls Baseline SC-15]

Discussion

Collaborative computing devices and applications include remote meeting devices and applications, networked white boards, cameras, and microphones. The explicit indication of use includes signals to users when collaborative computing devices and applications are activated.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-21

SC-17 Public Key Infrastructure Certificates

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Issue public key certificates under a TxDOT-approved certificate policy or obtain public key certificates from an approved service provider; and

b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

Implementation Standards

Std.01 — State agencies shall only procure, or otherwise implement, certificates from PKI Service Providers that appear on the Texas Department of Information Resources "Approved List of PKI Service Providers." [Source: 1 TAC 203.25(b)]

Std.02 — Public key certificates must be issued using a secure process that both verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party at the assurance level specified in TxDOT Identification and Authentication Standard.

Std.03 — Certificates for internal system operations (for example, application-specific time services, desktops, internal servers) must use Active Directory certificates or others approved by TxDOT and documented in the System Security Plan (SSP).

Std.04 — TxDOT must provide oversight in the creation of Public Key Infrastructure (PKI) framework and services that provide the generation, production, distribution, control, revocation, recovery, and tracking of PKI certificates and their corresponding private keys.

Std.05 — PKI certificates must be encrypted using an approved algorithm as defined in SC-13. (See SC-13 Std.05).

Std.06 — PKI certificates must be valid for a maximum of, as follows:

a. End entity (internet-facing) certificates: 397 days;

b. Subordinate (internal) entity certificates: two years.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SC-17.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Public key infrastructure (PKI) certificates are certificates with visibility external to organizational systems and certificates related to the internal operations of systems, such as application-specific time services. In cryptographic systems with a hierarchical structure, a trust anchor is an authoritative source (i.e., a certificate authority) for which trust is assumed and not derived. A root certificate for a PKI system is an example of a trust anchor. A trust store or certificate store maintains a list of trusted root certificates.

TxDOT Discussion

None.

TxDOT References

Identification and Authentication Standard; Information Security and Privacy Policy

State References

1 TAC 203; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST 800-57-1, 800-57-2, 800-57-3, 800-63-3; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AU-10, IA-05, SC-12

SC-18 Mobile Code

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Define acceptable and unacceptable mobile code and mobile code technologies; and

b. Authorize, monitor, and control the use of mobile code within the system.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SC-18.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. Decisions regarding the use of mobile code within organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include Java applets, JavaScript, HTML5, WebGL, and VBScript. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices, including notebook computers and smart phones. Mobile code policy and procedures address specific actions taken to prevent the development, acquisition, and introduction of unacceptable mobile code within organizational systems, including requiring mobile code to be digitally signed by a trusted source.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-28; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AU-02, AU-12, CM-02, CM-06, SI-03

SC-20 Secure Name/Address Resolution Service (Authoritative Source)

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Implementation Standards

Std.01 — Enable remote clients to obtain origin authentication and integrity verification assurances along with the authoritative data for the name/address resolution information obtained through the service consistent with the guidance in SP 800-81.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SC-20.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baseline, the following standards apply:

Std.02 FedRAMP — Control Description should include how DNSSEC is implemented on authoritative DNS servers to supply valid responses to external DNSSEC requests. [Source: FedRAMP Security Controls Baseline SC-20]

Std.03 FedRAMP — Authoritative DNS servers must be geolocated in accordance with SA-9(5). [Source: FedRAMP Security Controls Baseline SC-20]

Discussion

Providing authoritative source information enables external clients, including remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Systems that provide name and address resolution services include domain name system (DNS) servers. Additional artifacts include DNS Security Extensions (DNSSEC) digital signatures and cryptographic keys. Authoritative data includes DNS resource records. The means for indicating the security status of child zones include the use of delegation signer resource records in the DNS. Systems that use technologies other than the DNS to map between host and service names and network addresses provide other means to assure the authenticity and integrity of response data.

TxDOT Discussion

Mechanisms to ensure that name/address resolution service provides additional data origin, integrity artifacts, and authoritative data in response to queries should include all of the following:

1. Digital signatures;

2. Digital certificates;

3. Digital time stamping;

4. DNSSEC;

5. Approved encryption requirements and technology (see SC-13).

Additionally, means to indicate the security status of child subspaces may include delegation signer (DS) resource records in the DNS.

Note for systems subject to FedRAMP Requirements:

SC-20 applies to use of external authoritative DNS to access a Cloud Service Offering (CSO) from outside the boundary.

External authoritative DNS servers may be located outside an authorized environment. Positioning these servers inside an authorized boundary is encouraged.

Cloud Service Providers (CSPs) are recommended to self-check DNSSEC configuration through one of many available analyzers such as Sandia National Labs (https://dnsviz.net)

[Source: FedRAMP Security Controls Baseline SC-20]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FIPS 140, 186; NIST SP 800-81-2; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AU-10, SC-08, SC-12, SC-13, SC-21, SC-22

SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Implementation Standards

Std.01 — The information system that provides name/address resolution service for local clients must perform data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems following the guidance in NIST SP 800-81, Security Domain Name Deployment Guide. [Source: DIR Control Standards Catalog v1.3 SC-21]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SC-21.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baseline, the following standards apply:

Std.02 FedRAMP — Control description should include how DNSSEC is implemented on recursive DNS servers to make DNSSEC requests when resolving DNS requests from internal components to domains external to the Cloud Service Offering (CSO) boundary.

a. If the reply is signed, and fails DNSSEC, do not use the reply.

b. If the reply is unsigned, Cloud Service Provider (CSP) chooses the policy to apply. [Source: FedRAMP Security Controls Baseline SC-21]

Std.03 FedRAMP — Internal recursive DNS servers must be located inside an authorized environment. It is typically within the boundary, or leveraged from an underlying IaaS/PaaS. [Source: FedRAMP Security Controls Baseline SC-21]

Discussion

Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Systems that provide name and address resolution services for local clients include recursive resolving or caching domain name system (DNS) servers. DNS

client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Systems that use technologies other than the DNS to map between host and service names and network addresses provide some other means to enable clients to verify the authenticity and integrity of response data.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

Accepting an unsigned reply is acceptable.

SC-21 applies to use of internal recursive DNS to access a domain outside the boundary by a component inside the boundary.

DNSSEC resolution to access a component inside the boundary is excluded.

[Source: FedRAMP Security Controls Baseline SC-21]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-81-2; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

SC-20, SC-22

SC-22 Architecture and Provisioning for Name/Address Resolution Service

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SC-22.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Systems that provide name and address resolution services include domain name system (DNS) servers. To eliminate single points of failure in systems and enhance redundancy, organizations employ at least two authoritative domain name system servers—one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks, including the Internet). Organizations specify clients that can access authoritative DNS servers in certain roles (e.g., by address ranges and explicit lists).

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-81-2; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

SC-02, SC-20, SC-21, SC-24

SC-23 Session Authenticity

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Protect the authenticity of communications sessions.

Implementation Standards

Std.01 — Provide session-level protection using approved cryptographic modules in accordance with SC-13.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SC-23.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Protecting session authenticity addresses communications protection at the session level, not at the packet level. Such protection establishes grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and the validity of transmitted information. Authenticity protection includes protecting against "man-in-the-middle" attacks, session hijacking, and the insertion of false information into sessions.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-52, 800-77, 800-95, 800-113; CJIS Security Policy

Related Controls

AU-10, SC-08, SC-10, SC-13

SC-24 Fail in Known State

Baselines

High

Overlays

FedRAMP High

Requirements

Fail to a known secure state for the following failures on the indicated components while preserving system state information as defined in Std.01 in failure: all types of system failures on system components under configuration management.

Implementation Standards

Std.01 — Configure systems to preserve state information necessary to:

a. Determine cause of failure;

b. Return to operations with least disruption to mission and business processes; and

c. Permit investigations of failure.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Failure in a known state addresses security concerns in accordance with the mission and business needs of organizations. Failure in a known state prevents the loss of confidentiality, integrity, or availability of information in the event of failures of organizational systems or system components. Failure in a known safe state helps to prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving system state information facilitates system restart and return to the operational mode with less disruption of mission and business processes.

TxDOT Discussion

Information preserved in failure should include, for example, state variables and whether communication is permitted or blocked.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

FedRAMP Security Controls Baseline

Related Controls

CP-02, CP-04, CP-10, SA-08, SC-07, SC-22

SC-28 Protection of Information at Rest

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; Sensitive; TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Protect the confidentiality and integrity of the following information at rest: TxDOT data classified as Sensitive, Confidential, or Regulated.

Implementation Standards

Std.01 — All TxDOT data classified as Sensitive, Confidential, or Regulated must be encrypted at rest using an encryption algorithm compliant with SC-13 and SC-28(01).

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.02 PCI — If disk-level or partition-level encryption is used (rather than file-, column-, or field-level database encryption) to render primary account number (PAN) unreadable, it is managed as follows:

a. Logical access is managed separately and independently of native operating system authentication and access control mechanisms.

b. Decryption keys are not associated with user accounts.

c. Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely.

[Source: PCI DSS 3.5.1.3]

Std.03 PCI — If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render primary account number (PAN) unreadable, it is implemented only as follows:

a. On removable electronic media; or

b. If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1.

[Source: PCI DSS 3.5.1.2]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.04 CJIS —

a. Protect the confidentiality and integrity of the following information at rest: CJI when outside physically secure locations using cryptographic modules which are certified FIPS 140-3 with a symmetric cipher key of at least 128-bit strength, or FIPS 197 with a symmetric cipher key of at least 256-bit strength.

b. Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.

c. The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g., government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e., United States, U.S. territories, Indian Tribes, and Canada) and are under legal authority of an APB-member agency (i.e., United States– federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police).

[Source: CJIS SC-28]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Information at rest refers to the state of information when it is not in process or in transit and is located on system components. Such components include internal or external hard disk drives, storage area network devices, or databases. However, the focus of protecting information at rest is not on the type of storage device or frequency of access but rather on the state of the information. Information at rest addresses the confidentiality and integrity of information and covers user information and system information. System-related information that requires protection includes configurations or rule sets for firewalls, intrusion detection and prevention systems, filtering routers, and authentication information. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing write-once-read-many (WORM) technologies. When adequate protection of information at rest cannot otherwise be achieved, organizations may employ other controls, including frequent scanning to identify malicious code at rest and secure offline storage in lieu of online storage.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

The organization supports the capability to use cryptographic mechanisms to protect information at rest.

When leveraging encryption from underlying IaaS/PaaS: While some IaaS/PaaS services provide encryption by default, many require encryption to be configured, and enabled by the customer. The Cloud Service Provider (CSP) has the responsibility to verify encryption is properly configured.

Note that this enhancement requires the use of cryptography in accordance with SC-13.

[Source: FedRAMP Security Controls Baseline SC-28]

Note for systems subject to CJIS Requirements:

This restriction does not apply to exchanges of CJI with foreign government agencies under international exchange agreements (e.g., the Preventing and Combating Serious Crime agreements, fugitive extracts, and exchanges

made for humanitarian and criminal investigatory purposes in particular circumstances).

[Source: CJIS SC-28]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-56A, 800-56B, 800-56C, 800-57-1, 800-57-2, 800-57-3, 800-111, 800-124; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-03, AC-04, AC-06, AC-19, CA-07, CM-03, CM-05, CM-06, CP-09, MP-04, MP-05, PE-03, SC-08, SC-12, SC-13, SI-03, SI-07, SI-16

SC-28(01) Cryptographic Protection

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; Sensitive; TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on all digital media: TxDOT data classified as Sensitive, Confidential, or Regulated.

Implementation Standards

Std.01 — Implement encryption algorithms in accordance with SC-13.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.02 PCI — Primary account number (PAN) is rendered unreadable anywhere it is stored by using any of the following approaches:

a. One-way hashes based on strong cryptography of the entire PAN.

b. Truncation (hashing cannot be used to replace the truncated segment of PAN).

1. If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN.

c. Index tokens.

d. Strong cryptography with associated key-management processes and procedures.

[Source: PCI DSS 3.5.1]

e. Hashes used to render primary account number (PAN) unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7. [Source: PCI DSS 3.5.1.1]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.03 CJIS — Rescinded in V4.0.

Std.04 CJIS — Passphrases used to unlock ciphers for encryption on CJI at rest must comply with the TxDOT Identification and Authentication Standard.

Std.06 CJIS —Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on information systems and digital media outside physically secure locations: CJI. [Source: CJIS SC-28(01)]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.05 FedRAMP — Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on all information system components storing Federal data or system data that must be protected at the Moderate or High impact levels: TxDOT data classified as Sensitive, Confidential, or Regulated. [Source: FedRAMP Security Controls Baseline SC-28(1)]

Discussion

The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category or classification of the information. Organizations have the flexibility to encrypt information on system components or media or encrypt data structures, including files, records, or fields.

TxDOT Discussion

Note for systems subject to FedRAMP requirements:

Organizations should select a mode of protection that is targeted towards the relevant threat scenarios.

Examples:

a. Organizations may apply full disk encryption (FDE) to a mobile device where the primary threat is loss of the device while storage is locked.

b. For a database application housing data for a single customer, encryption at the file system level would often provide more protection than FDE against the more likely threat of an intruder on the operating system accessing the storage.

c. For a database application housing data for multiple customers, encryption with unique keys for each customer at the database record level may be more appropriate.

[Source: FedRAMP Security Controls Baseline SC-28(1)]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-56A, 800-56B, 800-56C, 800-57-1, 800-57-2, 800-57-3, 800-111, 800-124; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-19, SC-12, SC-13

SC-39 Process Isolation

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Maintain a separate execution domain for each executing system process.

Implementation Standards

Std.01 — Rescinded in V2.2.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.02 PCI — Primary functions requiring different security levels are managed as follows:

a. Only one primary function exists on a system component; or

b. Primary functions with differing security levels that exist on the same system component are isolated from each other; or

c. Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.

[Source: PCI DSS 2.2.3]

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SC-39.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. Process isolation technologies, including sandboxing or virtualization, logically separate software and firmware from other software, firmware, and data. Process isolation helps limit the access of potentially untrusted software to other system resources. The capability to maintain separate execution domains is available in commercial operating systems that employ multi-state processor technologies.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-160-1; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-03, AC-04, AC-06, SA-08, SC-02, SC-03, SI-16

SC-45 System Time Synchronization

Baselines

Low, Moderate, High

Overlays

PCI DSS; FedRAMP Moderate, FedRAMP High

Requirements

Synchronize system clocks within and between systems and system components.

Implementation Standards

Std.01 — Ensure that system clocks meet the degree of synchronization in accordance with AU-08.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.02 PCI — Systems are configured to the correct and consistent time as follows:

a. One or more designated time servers are in use.

b. Only the designated central time server(s) receives time from external sources.

c. Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC).

d. The designated time server(s) accept time updates only from specific industry-accepted external sources.

e. Where there is more than one designated time server, the time servers peer with one another to keep accurate time.

f. Internal systems receive time information only from designated central time server(s).

[Source: PCI DSS 10.6.2]

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Time synchronization of system clocks is essential for the correct execution of many system services, including identification and authentication processes that involve certificates and time-of-day restrictions as part of access control. Denial of service or failure to deny expired credentials may result without properly synchronized clocks within and between systems and system components. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. The granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks, such as clocks synchronizing within hundreds of milliseconds or tens of milliseconds. Organizations may define different time granularities for system components. Time service can be critical to other security capabilities—such as access control and identification and authentication—depending on the nature of the mechanisms used to support the capabilities.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

IETF 5905; FedRAMP Security Controls Baseline; PCI DSS

Related Controls

AC-03, AU-08, IA-02, IA-08

SC-45(01) Synchronization with Authoritative Time Source

Baselines

Moderate, High

Overlays

PCI DSS; Sensitive; FedRAMP Moderate, FedRAMP High

Requirements

a. Compare the internal system clocks at least once daily and at system boot with an approved authoritative time source as defined in Std.01; and

b. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than the granularity defined in AU-08.

Implementation Standards

Std.01 — Configure internal system clocks to synchronize with an agency approved, authoritative source.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.03 PCI — Time synchronization settings and data are protected as follows:

a. Access to time data is restricted to only personnel with a business need.

b. Any changes to time settings on critical systems are logged, monitored, and reviewed.

[Source: PCI DSS 10.6.3]

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.02 FedRAMP —

a. Compare the internal system clocks at least hourly with http://tf.nist.gov/tf-cgi/servers.cgi; and

b. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than any difference.

[Source: FedRAMP Security Controls Baseline SC-45(1)]

Discussion

Synchronization of internal system clocks with an authoritative source provides uniformity of time stamps for systems with multiple system clocks and systems connected over a network.

TxDOT Discussion

Note for systems subject to FedRAMP Requirements:

Synchronization of system clocks improves the accuracy of log analysis. [Source: FedRAMP Security Controls Baseline SC-45(1)]

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

IETF 5905; PCI DSS; FedRAMP Security Controls Baseline

Related Controls

None.

SI — System and Information Integrity

SI-01 Policy and Procedures

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level system and information integrity policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;

b. Designate a senior management official as defined in the system and information integrity policy to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and

c. Review and update the current system and information integrity:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — The Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 5.1.1 and 5.1.2.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Rescinded in v4.0.

Std.04 CJIS — Review and update the current system and information integrity policy and procedures following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. [Source: CJIS SI-01]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

System and information integrity policy and procedures address the controls in the SI family that are implemented within systems and organizations. The

risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and information integrity policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and information integrity policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; NIST SP 800-12, 800-100; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

PM-09, PS-08, SA-08, SI-03, SI-12

SI-02 Flaw Remediation

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Identify, report, and correct system flaws;

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Install security-relevant software and firmware updates within time periods defined in accordance with RA-05 Std.07 of the release of the updates; and

d. Incorporate flaw remediation into the organizational configuration management process.

Implementation Standards

Std.01 — TxDOT must identify, report, and correct information system flaws. [Source: DIR Control Standards Catalog SI-2]

Std.02 — Security Issues Related to Legacy Systems

a. A state agency shall, with available funds, identify information security issues and develop a plan to prioritize the remediation and mitigation of those issues. The agency shall include in the plan:

1. Procedures for reducing the agency's level of exposure with regard to information that alone or in conjunction with other information identifies an individual maintained on a legacy system of the agency;

2. The best value approach for modernizing, replacing, renewing, or disposing of a legacy system that maintains information critical to the agency's responsibilities;

b. A plan developed under this section, along with any information or communication prepared or maintained for use in the preparation of the

plan, is confidential and is not subject to disclosure under Chapter 552 (Public Information).

[Source: TGC 2054.575]

Std.03 — Review available published sources and alerts identifying software flaws.

Std.04 — Where feasible, test newly released security relevant patches, service packs, and hot fixes in a test environment.

Std.05 — Patches, service packs, and hot fixes not implemented in enterprise or specific systems must be documented in the risk register.

Std.06 — Monitor systems to verify that security releases have been installed and are functioning correctly.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement 5.20.4.1.

For systems processing CJIS data, SI-02c is superseded by CJIS requirement SI-02c:

Std.08 CJIS — Install security-relevant software and firmware updates within the number of days listed after the release of the updates:

- Critical – 15 days;
- High – 30 days;
- Medium – 60 days; or
- Low – 90 days.

[Source: CJIS SI-02]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low or Moderate baselines, the following standard applies:

Std.07 FedRAMP — Install security-relevant software and firmware updates within thirty days of the release of the updates. [Source: FedRAMP Security Controls Baseline SI-2]

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

The need to remediate system flaws applies to all types of software and firmware. Organizations identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Security-relevant updates include patches, service packs, and malicious code signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified.

Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of risk factors, including the security category of the system, the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw), the organizational risk tolerance, the mission supported by the system, or the threat environment. Some types of flaw remediation may require more testing than other types. Organizations determine the type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software or firmware updates is not necessary or practical, such as when implementing simple malicious code signature updates. In testing decisions, organizations consider whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

TGC 2054; DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; FIPS 140, 186; NIST SP 800-39, 800-40, 800-128; NIST IR 7788; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

CA-05, CM-03, CM-04, CM-05, CM-06, CM-08, MA-02, RA-05, SA-08, SA-10, SA-11, SI-03, SI-05, SI-07, SI-11

SI-02(02) Automated Flaw Remediation Status

Baselines

Moderate, High

Overlays

CJIS; Sensitive; FedRAMP Moderate, FedRAMP High

Requirements

Determine if system components have applicable security-relevant software and firmware updates installed using automated mechanisms where feasible at least once per quarter and on demand.

Implementation Standards

Std.01 — Where feasible, select remediation tools that include automated verification of remediation, or configure systems to automatically review files or configuration settings after remediation and mitigation activities.

Std.02 — Verification of remediation, whether automated or manual, must not employ exploit procedures (for example, penetration tests) or exploit codes without prior authorization and approval from the system's Authorizing Official (AO).

Std.03 — When flaw remediation and vulnerability mitigations are completed, update the system and component inventory to reflect current software versions and configurations.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.05 CJIS — Determine if system components have applicable security-relevant software and firmware updates installed using vulnerability scanning tools as least quarterly or following any security incidents involving CJI or systems used to process, store, or transmit CJI. [Source: CJIS SI-02(02)]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baseline, the following standard applies:

Std.04 FedRAMP — Determine if system components have applicable security-relevant software and firmware updates installed using automated mechanisms where feasible at least monthly. [Source: FedRAMP Security Controls Baseline SI-2(2)]

Discussion

Automated mechanisms can track and determine the status of known flaws for system components.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; FIPS 140, 186; NIST SP 800-39, 800-40, 800-128; NIST IR 7788; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

CA-07, SI-04

SI-02(03) Time to Remediate Flaws and Benchmarks for Corrective Actions

Baselines

N/A

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

a. Measure the time between flaw identification and flaw remediation; and

b. Establish the following benchmarks for taking corrective actions: in accordance with RA-05 Std.07.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organizations determine the time it takes on average to correct system flaws after such flaws have been identified and subsequently establish organizational benchmarks (i.e., time frames) for taking corrective actions.

Benchmarks can be established by the type of flaw or the severity of the potential vulnerability if the flaw can be exploited.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

SI-03 Malicious Code Protection

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Implement signature based, non-signature based, or both types of malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;

b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;

c. Configure malicious code protection mechanisms to:

1. Perform periodic scans of the system at least daily and real-time scans of files from external sources at endpoints and network entry and exit points as

the files are downloaded, opened, or executed in accordance with organizational policy; and

2. Block and quarantine malicious code and send alert to administrators in response to malicious code detection; and

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

Implementation Standards

Std.01 — Rescinded in V2.2.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 5.3.1.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.02 PCI — Rescinded in V3.0.

Std.03 PCI — An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware. [Source: PCI DSS 5.2.1]

Std.04 PCI — The deployed anti-malware solution(s):

a. Detects all known types of malware.

b. Removes, blocks, or contains all known types of malware.

[Source: PCI DSS 5.2.2]

Std.05 PCI —

a. Any system components that are not at risk for malware are evaluated periodically to include the following:

1. A documented list of all system components not at risk for malware.

2. Identification and evaluation of evolving malware threats for those system components.

3. Confirmation whether such system components continue to not require anti-malware protection.

[Source: PCI DSS 5.2.3]

b. The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1; at a minimum, at least once every six months. [Source: PCI DSS 5.2.3.1; PCI DSS v4.x: Targeted Risk Analysis Guidance]

Std.06 PCI — The anti-malware solution(s):

a. Performs periodic scans and active or real-time scans; or

b. Performs continuous behavioral analysis of systems or processes.

[Source: PCI DSS 5.3.2]

c. If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1; at a minimum, at least once a day (daily). [Source: PCI DSS 5.3.2.1; PCI DSS v4.x: Targeted Risk Analysis Guidance]

Std.07 PCI — Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period. [Source: PCI DSS 5.3.5]

Std.09 PCI — For removable electronic media, the anti-malware solution(s):

a. Performs automatic scans of when the media is inserted, connected, or logically mounted; or

b. Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.

[Source: PCI DSS 5.3.3]

Std.10 PCI — Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1. [Source: PCI DSS 5.3.4]

Std.11 PCI — Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks. [Source: PCI DSS 5.4.1]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.12 CJIS —

a. Implement signature-based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; and

b. Configure malicious code protection mechanisms to block or quarantine malicious code, take mitigating action(s), and when necessary, implement incident response procedures; and send alert to system/network administrators and/or organizational personnel with information security responsibilities in response to malicious code detection.

[Source: CJIS SI-03]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.08 FedRAMP — Send alerts to administrators or defined security personnel near-real-time in response to malicious code detection. [Source: FedRAMP Security Controls Baseline SI-3]

Discussion

System entry and exit points include firewalls, remote access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats contained within compressed or hidden files or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways, including by electronic mail, the world-wide web, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities. A variety of technologies and methods exist to limit or eliminate the effects of malicious code.

Malicious code protection mechanisms include both signature- and nonsignature-based technologies. Nonsignature-based detection mechanisms include artificial intelligence techniques that use heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide controls against such code for which signatures do not yet exist or for which existing signatures may not be effective. Malicious code for which active signatures do not yet exist or may be ineffective

includes polymorphic malicious code (i.e., code that changes signatures when it replicates). Nonsignature-based mechanisms also include reputation-based technologies. In addition to the above technologies, pervasive configuration management, comprehensive software integrity controls, and anti-exploitation software may be effective in preventing the execution of unauthorized code. Malicious code may be present in commercial off-the-shelf software as well as custom-built software and could include logic bombs, backdoors, and other types of attacks that could affect organizational mission and business functions.

In situations where malicious code cannot be detected by detection methods or technologies, organizations rely on other types of controls, including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to ensure that software does not perform functions other than the functions intended. Organizations may determine that, in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, the detection of malicious downloads, or the detection of maliciousness when attempting to open or execute files.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-83, 800-125B, 800-177; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-04, AC-19, CM-03, CM-08, IR-04, MA-03, MA-04, PL-09, RA-05, SC-07, SC-23, SC-28, SI-02, SI-04, SI-07, SI-08

SI-04 System Monitoring

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Monitor the system to detect:

1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: objectives defined in the Information Security Program Plan or the System Security Plan (SSP); and

2. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the system through the following techniques and methods: techniques and methods as defined in the SSP;

c. Invoke internal monitoring capabilities or deploy monitoring devices:

1. Strategically within the system to collect organization-determined essential information; and

2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Analyze detected events and anomalies;

e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;

f. Obtain legal opinion regarding system monitoring activities; and

g. Provide system monitoring information as defined in the applicable SSP to personnel or roles identified in the SSP as needed and at the frequency defined in the SSP.

Implementation Standards

Std.01 — Rescinded in V2.4.

Std.02 — Rescinded in V2.4.

Std.03 — Configure systems to address all applicable monitoring objectives in accordance with the Information Security Program Plan, including but not limited to:

a. Impact of security changes to the information system;

b. Unauthorized use of the system;

c. Information system attacks; and

d. Identified specific types of transactions of interest.

Std.04 — Intrusion Detection/Prevention System (IDS/IPS) devices must be installed at network perimeter points.

Std.05 — The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to:

a. Intrusion-detection and intrusion-prevention systems.

b. Network security controls.

c. Change-detection mechanisms for critical files.

d. Detection of unauthorized wireless access points.

[Source: PCI DSS 12.10.5]

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirement 12.10.5.

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.06 PCI — Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems:

a. Network security controls.

b. IDS/IPS.

c. Change-detection mechanisms.

d. Anti-malware solutions.

e. Physical access controls.

f. Logical access controls.

g. Audit logging mechanisms.

h. Segmentation controls (if used).

i. Audit log review mechanisms.

j. Automated security testing tools (if used).

[Source: PCI DSS 10.7.2]

Std.07 PCI — Intrusion-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions into the network as follows:

a. All traffic is monitored at the perimeter of the Cardholder Data Environment (CDE).

b. All traffic is monitored at critical points in the CDE.

c. Personnel are alerted to suspected compromises.

d. All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.

[Source: PCI DSS 11.5.1]

Std.08 PCI — The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to the change- and tamper-detection mechanism for payment pages. [Source: PCI DSS 12.10.5]

CJIS Correspondence

For systems processing CJIS data, SI-04a2, b, and g are superseded by CJIS SI-04a2, b, and g:

Std.09 CJIS —

a. Monitor the system to detect attacks and indicators of potential attacks in accordance with the following monitoring objectives:

1. Intrusion detection and prevention;

2. Malicious code protection;

3. Vulnerability scanning;

4. Audit record monitoring;

5. Network monitoring; and

6. Firewall monitoring.

b. Identify unauthorized use of the system through the following techniques and methods: event logging.

c. Provide intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring, and firewall monitoring software logs to organizational personnel with information security responsibilities weekly.

[Source: CJIS SI-04]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at external interfaces to the system. Internal monitoring includes the observation of events occurring within the system. Organizations monitor systems by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives guide and inform the determination of the events. System monitoring capabilities are achieved through a variety of tools and techniques, including intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software.

Depending on the security architecture, the distribution and configuration of monitoring devices may impact throughput at key internal and external boundaries as well as at other locations across a network due to the

introduction of network throughput latency. If throughput management is needed, such devices are strategically located and deployed as part of an established organization-wide security architecture. Strategic locations for monitoring devices include selected perimeter locations and near key servers and server farms that support critical applications. Monitoring devices are typically employed at the managed interfaces associated with controls SC-07 and AC-17. The information collected is a function of the organizational monitoring objectives and the capability of systems to support such objectives. Specific types of transactions of interest include Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. System monitoring is an integral part of organizational continuous monitoring and incident response programs, and output from system monitoring serves as input to those programs. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other controls (e.g., AC-02g, AC-02(07), AC-02(12)(a), AC-17(01), AU-13, AU-13(01), AU-13(02), CM-03f, CM-06d, MA-03a, MA-04a, SC-05(03)(b), SC-07a, SC-07(24)(b), SC-18b, SC-43b). Adjustments to levels of system monitoring are based on law enforcement information, intelligence information, or other sources of information. The legality of system monitoring activities is based on applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

TxDOT Discussion

Note for systems subject to FedRAMP requirements:

See US-CERT Incident Response Reporting Guidelines. [Source: FedRAMP Security Controls Baseline SI-4]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; FIPS 140; NIST SP 800-61, 800-83, 800-92, 800-94, 800-137; PCI DSS; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-02, AC-03, AC-04, AC-08, AC-17, AU-02, AU-06, AU-07, AU-09, AU-12, CA-07, CM-03, CM-06, CM-08, CM-11, IR-04, MA-03, MA-04, PL-09, PM-12, RA-05, SC-05, SC-07, SC-18, SI-03, SI-06, SI-07, SR-09, SR-10

SI-04(01) System-Wide Intrusion Detection System

Baselines

N/A

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Linking individual intrusion detection tools into a system-wide intrusion detection system provides additional coverage and effective detection capabilities. The information contained in one intrusion detection tool can be shared widely across the organization, making the system-wide detection capability more robust and powerful.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; FIPS 140; NIST SP 800-61, 800-83, 800-92, 800-94, 800-137; FedRAMP Security Controls Baseline

Related Controls

None.

SI-04(02) Automated Tools and Mechanisms for Real-Time Analysis

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Employ automated tools and mechanisms to support near real-time analysis of events.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SI-04(02).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Automated tools and mechanisms include host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or security information and event management (SIEM) technologies that provide real-time analysis of alerts and notifications generated by organizational systems. Automated monitoring techniques can create unintended privacy risks because automated controls may connect to external or otherwise unrelated systems. The matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; FIPS 140; NIST SP 800-61, 800-83, 800-92, 800-94, 800-137; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

PM-25

SI-04(04) Inbound and Outbound Communications Traffic

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;

b. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions as defined in system monitoring plans.

Implementation Standards

Std.01 — Aggregated inbound and outbound communications of Technical Reference Architecture traffic information must be searchable by TxDOT Information Security:

a. Information is provided to TxDOT Information Security in a format compliant with TxDOT, state, and federal (e.g., Continuous Diagnostics and Mitigation) requirements;

b. Information sources include Technical Reference Architecture traffic analysis information from local analysis tools and directly from any information technology component in an environment requiring a TxDOT Authority to Operate (ATO); and

c. TxDOT Information Security directed aggregated inbound and outbound communications of Technical Reference Architecture traffic information collection rules/requests (for example, sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.

Std.02 — Raw event information must be available in an unaltered format to TxDOT Information Security.

Std.03 — Where a system cannot monitor inbound and outbound communications traffic, provide a monitoring capability on a separate system to monitor localized, targeted, and network-wide events.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SI-04(04).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Unusual or unauthorized activities or conditions related to system inbound and outbound communications traffic includes internal traffic that indicates the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information. Evidence of malicious code or unauthorized use of legitimate code or credentials is used to identify potentially compromised systems or system components.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; FIPS 140; NIST SP 800-61, 800-83, 800-92, 800-94, 800-137; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

None.

SI-04(05) System-Generated Alerts

Baselines

Moderate, High

Overlays

CJIS; Sensitive; FedRAMP Moderate, FedRAMP High

Requirements

Alert personnel or roles identified in the System Security Plan (SSP) when the following system-generated indications of compromise or potential compromise occur: indicators defined in SI-04.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SI-04(05).

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Alerts may be generated from a variety of sources, including audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated and may be transmitted telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the alert notification list can include system administrators, mission or business owners, system owners, information owners/stewards, senior agency information security officers, senior agency officials for privacy, system security officers, or privacy officers. In contrast to alerts generated by the system, alerts generated by organizations in SI-04(12) focus on information sources external to the system, such as suspicious activity reports and reports on potential insider threats.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; FIPS 140; NIST SP 800-61, 800-83, 800-92, 800-94, 800-137; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AU-04, AU-05, PE-06

SI-04(10) Visibility of Encrypted Communications

Baselines

N/A

Overlays

FedRAMP High

Requirements

Make provisions so that all encrypted communications traffic is visible to system monitoring tools and mechanisms as specified in the System Security Plan (SSP).

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.01 FedRAMP — The service provider must support Agency requirements to comply with M-21-31 (https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf) and M-22-09 (https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf). [Source: FedRAMP Security Controls Baseline SI-4(10)]

Discussion

Organizations balance the need to encrypt communications traffic to protect data confidentiality with the need to maintain visibility into such traffic from a monitoring perspective. Organizations determine whether the visibility requirement applies to internal encrypted traffic, encrypted traffic intended for external destinations, or a subset of the traffic types.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

SI-04(11) Analyze Communications Traffic Anomalies

Baselines

N/A

Overlays

FedRAMP High

Requirements

Analyze outbound communications traffic at the external interfaces to the system and selected internal managed interfaces to discover anomalies.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Organization-defined interior points include subnetworks and subsystems. Anomalies within organizational systems include large file transfers, long-time persistent connections, attempts to access information from unexpected locations, the use of unusual protocols and ports, the use of unmonitored network protocols (e.g., IPv6 usage during IPv4 transition), and attempted communications with suspected malicious external addresses.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

SI-04(12) Automated Organization-generated Alerts

Baselines

N/A

Overlays

FedRAMP High

Requirements

Alert personnel or roles as defined in the System Security Plan (SSP) using automated mechanisms as defined in the SSP when the following indications of inappropriate or unusual activities with security or privacy implications occur: attacks and indicators of potential attacks as defined in SI-04.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Organizational personnel on the system alert notification list include system administrators, mission or business owners, system owners, senior agency information security officer, senior agency official for privacy, system security officers, or privacy officers. Automated organization-generated alerts are the security alerts generated by organizations and transmitted using automated means. The sources for organization-generated alerts are focused on other entities such as suspicious activity reports and reports on potential insider threats. In contrast to alerts generated by the organization, alerts generated by the system in SI-04(05) focus on information sources that are internal to the systems, such as audit records.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

SI-04(14) Wireless Intrusion Detection

Baselines

N/A

Overlays

CJIS; FedRAMP High

Requirements

Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement 5.20.1.1.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Wireless signals may radiate beyond organizational facilities. Organizations proactively search for unauthorized wireless connections, including the conduct of thorough scans for unauthorized wireless access points. Wireless scans are not limited to those areas within facilities containing systems but also include areas outside of facilities to verify that unauthorized wireless access points are not connected to organizational systems.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; FIPS 140; NIST SP 800-61, 800-83, 800-92, 800-94, 800-137; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

AC-18, IA-03

SI-04(16) Correlate Monitoring Information

Baselines

N/A

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

Correlate information from monitoring tools and mechanisms employed throughout the system.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Correlating information from different system monitoring tools and mechanisms can provide a more comprehensive view of system activity. Correlating system monitoring tools and mechanisms that typically work in isolation—including malicious code protection software, host monitoring, and network monitoring—can provide an organization-wide monitoring view and may reveal otherwise unseen attack patterns. Understanding the capabilities and limitations of diverse monitoring tools and mechanisms and how to maximize the use of information generated by those tools and mechanisms can help organizations develop, operate, and maintain effective monitoring programs. The correlation of monitoring information is especially important

during the transition from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols).

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

AU-06

SI-04(18) Analyze Traffic and Covert Exfiltration

Baselines

N/A

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: key internal managed interfaces within the system.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Organization-defined interior points include subnetworks and subsystems. Covert means that can be used to exfiltrate information include steganography.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

SI-04(19) Risk for Individuals

Baselines

N/A

Overlays

FedRAMP High

Requirements

Implement monitoring in accordance with AC-02(07) of individuals who have been identified by account managers, information owners, or security personnel as posing an increased level of risk.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Indications of increased risk from individuals can be obtained from different sources, including personnel records, intelligence agencies, law enforcement organizations, and other sources. The monitoring of individuals is coordinated with the management, legal, security, privacy, and human resource officials who conduct such monitoring. Monitoring is conducted in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

None.

SI-04(20) Privileged Users

Baselines

N/A

Overlays

FedRAMP High

Requirements

Implement the following additional monitoring of privileged users: monitoring in accordance with AC-02(07).

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Privileged users have access to more sensitive information, including security-related information, than the general user population. Access to such information means that privileged users can potentially do greater damage to systems and organizations than non-privileged users. Therefore, implementing additional monitoring on privileged users helps to ensure that organizations can identify malicious activity at the earliest possible time and take appropriate actions.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

AC-18

SI-04(22) Unauthorized Network Services

Baselines

N/A

Overlays

FedRAMP High

Requirements

a. Detect network services that have not been authorized or approved by configuration change control per CM-03; and

b. Alert personnel or roles as defined in the System Security Plan (SSP) when detected.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Unauthorized or unapproved network services include services in service-oriented architectures that lack organizational verification or validation and may therefore be unreliable or serve as malicious rogues for valid services.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

CM-07

SI-04(23) Host-Based Devices

Baselines

N/A

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

Implement the following host-based monitoring mechanisms at external managed interfaces to the system and at key internal managed interfaces within the system: monitoring mechanisms as specified in the System Security Plan (SSP).

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Host-based monitoring collects information about the host (or system in which it resides). System components in which host-based monitoring can be implemented include servers, notebook computers, and mobile devices. Organizations may consider employing host-based monitoring mechanisms from multiple product developers or vendors.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

AC-18, AC-19

SI-05 Security Alerts, Advisories, and Directives

Baselines

Low, Moderate, High

Overlays

CJIS; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Receive system security alerts, advisories, and directives from external organizations per Std.02 on an ongoing basis;

b. Generate internal security alerts, advisories, and directives as deemed necessary;

c. Disseminate security alerts, advisories, and directives to: personnel or roles defined in Std.03; and

d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — External organizations from which system security alerts, advisories, and directives must be received include:

a. Cybersecurity and Infrastructure Security Agency (CISA);

b. Texas Department of Information Resources (DIR); and

c. Contracted service providers.

Std.03 — Security alerts, advisories, and directives must be disseminated to personnel or roles with information security, system administration, monitoring, or incident handling responsibilities, as identified in access control policies.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SI-05.

Std.04 CJIS — Rescinded in V4.0.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.05 FedRAMP — Service Providers must address the CISA Emergency and Binding Operational Directives applicable to their cloud service offering per FedRAMP guidance. This includes listing the applicable directives and stating compliance status. [Source: FedRAMP Security Controls Baseline SI-5]

Discussion

The Cybersecurity and Infrastructure Security Agency (CISA) generates security alerts and advisories to maintain situational awareness throughout the Federal Government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance with security directives is essential due to the critical nature of many of these directives and the potential (immediate) adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include supply chain partners, external mission or business partners, external service providers, and other peer or supporting organizations.

TxDOT Discussion

Alerts and advisories may be received and disseminated from other entities, including but not limited to agency partners, peers, vendors not yet contracted, and national cybersecurity organizations such as SANS.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

NIST SP 800-40; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

PM-15, RA-05, SI-02

SI-05(01) Automated Alerts and Advisories

Baselines

High

Overlays

FedRAMP High

Requirements

Broadcast security alert and advisory information throughout the organization using automated mechanisms as identified in applicable System Security Plans (SSPs).

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

The significant number of changes to organizational systems and environments of operation requires the dissemination of security-related information to a variety of organizational entities that have a direct interest

in the success of organizational mission and business functions. Based on information provided by security alerts and advisories, changes may be required at one or more of the three levels related to the management of risk, including the governance level, mission and business process level, and the information system level.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-40; FedRAMP Security Controls Baseline

Related Controls

None.

SI-06 Security and Privacy Function Verification

Baselines

High

Overlays

FedRAMP Moderate, FedRAMP High

Requirements

a. Verify the correct operation of security and privacy functions defined in the System Security Plan (SSP);

b. Perform the verification of the functions specified in SI-06a at system startup and restart, upon command by a user with appropriate privilege, and periodically every 30 days;

c. Alert personnel or roles as identified in the SSP to failed security and privacy verification tests; and

d. Shut the system down, restart the system, or take other defined alternative action(s) as specified in the SSP when anomalies are discovered.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Transitional states for systems include system startup, restart, shutdown, and abort. System notifications include hardware indicator lights, electronic alerts to system administrators, and messages to local computer consoles. In contrast to security function verification, privacy function verification ensures that privacy functions operate as expected and are approved by the senior agency official for privacy or that privacy attributes are applied or used as expected.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; FedRAMP Security Controls Baseline

Related Controls

CA-07, CM-04, CM-06, SI-07

SI-07 Software, Firmware, and Information Integrity

Baselines

Moderate, High

Overlays

CJIS; PCI DSS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: organization-controlled software, firmware, and information as identified in the System Security Plan (SSP); and

b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: actions as identified in the SSP.

Implementation Standards

Std.01 — Tools and mechanisms must be, as feasible:

a. Enabled on each device or system on the network, so long as performance is not impaired;

b. Checked against baselines to effectively verify variations from normal work-related activities; and

c. Able to provide a means to determine the date and time a resource was last accessed or modified.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standards apply:

Std.02 PCI — File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts. [Source: PCI DSS 10.3.4]

Std.03 PCI — A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows:

a. To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files.

b. To perform critical file comparisons at least once weekly.

[Source: PCI DSS 11.5.2]

Std.04 PCI — Failures of any critical security controls systems are responded to promptly, including but not limited to:

a. Restoring security functions.

b. Identifying and documenting the duration (date and time from start to end) of the security failure.

c. Identifying and documenting the cause(s) of failure and documenting required remediation.

d. Identifying and addressing any security issues that arose during the failure.

e. Determining whether further actions are required as a result of the security failure.

f. Implementing controls to prevent the cause of failure from reoccurring.

g. Resuming monitoring of security controls.

[Source: PCI DSS 10.7.3]

Std.05 PCI — A change- and tamper-detection mechanism is deployed as follows:

a. To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser.

b. The mechanism is configured to evaluate the received HTTP header and payment page.

c. The mechanism functions are performed as follows:

1. At least once every seven days; or

2. Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1; at a minimum, at least once every seven days.

[Source: PCI DSS 11.6.1; PCI DSS v4.x: Targeted Risk Analysis Guidance]

Std.06 PCI — All payment page scripts that are loaded and executed in the consumer's browser are managed as follows:

a. A method is implemented to confirm that each script is authorized.

b. A method is implemented to assure the integrity of each script.

c. An inventory of all scripts is maintained with written justification as to why each is necessary.

[Source: PCI DSS 6.4.3]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.07 CJIS —

a. Employ integrity verification tools to detect unauthorized changes to software, firmware, and information systems that contain or process CJI; and

b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: notify organizational personnel responsible for software, firmware, and/or information integrity and implement incident response procedures as appropriate.

[Source: CJIS SI-07]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes operating systems (with key internal components, such as kernels or drivers), middleware, and applications. Firmware interfaces include Unified Extensible Firmware Interface (UEFI) and Basic Input/Output System (BIOS). Information includes personally identifiable information and metadata that contains security and privacy attributes associated with information. Integrity-checking mechanisms—including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools—can automatically monitor the integrity of systems and hosted applications.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; FIPS 140, 186, 202; NIST SP 800-70, 800-147; PCI DSS; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-04, CM-03, CM-07, CM-08, MA-03, MA-04, RA-05, SA-08, SA-09, SA-10, SC-08, SC-12, SC-13, SC-28, SI-03, SR-03, SR-04, SR-05, SR-06, SR-09, SR-10, SR-11

SI-07(01) Integrity Checks

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Perform an integrity check of software, firmware, and information at system startup and at least once per day.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SI-07(01).

TX-RAMP Correspondence

For systems subject to TX-RAMP Level 2, the following standard applies:

Std.01 TX-RAMP — Perform an integrity check of organization-defined software, firmware, and information upon security-relevant events. [Source: TX-RAMP Manual SI-7(1)]

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.02 FedRAMP — Perform an integrity check of software, firmware, and information at security-relevant events at least monthly. [Source: FedRAMP Security Controls Baseline SI-7(1)]

Discussion

Security-relevant events include the identification of new threats to which organizational systems are susceptible and the installation of new hardware, software, or firmware. Transitional states include system startup, restart, shutdown, and abort.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; FIPS 140, 180, 186, 202; NIST SP 800-70, 800-147; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

SI-07(02) Automated Notifications of Integrity Violations

Baselines

High

Overlays

FedRAMP High

Requirements

Employ automated tools that provide notification to personnel or roles identified in the System Security Plan (SSP) upon discovering discrepancies during integrity verification.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

The employment of automated tools to report system and information integrity violations and to notify organizational personnel in a timely matter is essential to effective risk response. Personnel with an interest in system and information integrity violations include mission and business owners, system owners, senior agency information security official, senior agency official for privacy, system administrators, software developers, systems integrators, information security officers, and privacy officers.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; FIPS 140, 180, 186, 202; NIST SP 800-70, 800-147; FedRAMP Security Controls Baseline

Related Controls

None.

SI-07(05) Automated Response to Integrity Violations

Baselines

High

Overlays

PCI DSS; FedRAMP High

Requirements

Automatically implement controls defined in the System Security Plan (SSP) when integrity violations are discovered.

Implementation Standards

Std.01 — Specify which of the following controls is to be implemented:

a. Shut the information system down;

b. Restart the information system; or

c. Take another action to safeguard the security of the system.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.02 PCI — The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to:

a. Intrusion-detection and intrusion-prevention systems.

b. Network security controls.

c. Change-detection mechanisms for critical files.

d. The change-and tamper-detection mechanism for payment pages.

e. Detection of unauthorized wireless access points.

[Source: PCI DSS 12.10.5]

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Organizations may define different integrity-checking responses by type of information, specific information, or a combination of both. Types of information include firmware, software, and user data. Specific information

includes boot firmware for certain types of machines. The automatic implementation of controls within organizational systems includes reversing the changes, halting the system, or triggering audit alerts when unauthorized modifications to critical security files occur.

TxDOT Discussion

Acceptable actions in response to integrity violation should be defined in detail in the SSP. Shutting down or restarting a system may not always be feasible upon the identification of an anomaly, particularly for high-availability systems. In this case, other control actions must be defined and shutdown and restart scheduled in accordance with operational requirements.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

OMB A-130; FIPS 140, 180, 186, 202; NIST SP 800-70, 800-147; PCI DSS; FedRAMP Security Controls Baseline

Related Controls

None.

SI-07(07) Integration of Detection and Response

Baselines

Moderate, High

Overlays

CJIS; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Incorporate the detection of the following unauthorized changes into the organizational incident response capability: security-relevant changes to the system as defined in the System Security Plan (SSP).

Implementation Standards

Std.01 — Where the system cannot detect unauthorized security-relevant changes, compensating controls (for example, manual procedures) must be employed. [Source: SP 800-82]

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SI-07(07).

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Integrating detection and response helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important for being able to identify and discern adversary actions over an extended time period and for possible legal actions. Security-relevant changes include unauthorized changes to established configuration settings or the unauthorized elevation of system privileges.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; FIPS 140, 180, 186, 202; NIST SP 800-70, 800-147; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AU-02, AU-06, IR-04, IR-05, SI-04

SI-07(15) Code Authentication

Baselines

N/A

Overlays

FedRAMP High

Requirements

Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: all software and firmware inside the boundary.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

Cryptographic authentication includes verifying that software or firmware components have been digitally signed using certificates recognized and approved by organizations. Code signing is an effective method to protect against malicious code. Organizations that employ cryptographic mechanisms also consider cryptographic key management solutions.

TxDOT Discussion

None.

TxDOT References

None.

State References

None.

Federal References

FedRAMP Security Controls Baseline

Related Controls

CM-05, SC-12, SC-13

SI-08 Spam Protection

Baselines

Moderate, High

Overlays

CJIS; Sensitive; FedRAMP Moderate, FedRAMP High

Requirements

a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and

b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SI-08.

Std.01 CJIS — Rescinded in V4.0.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

System entry and exit points include firewalls, remote-access servers, electronic mail servers, web servers, proxy servers, workstations, notebook computers, and mobile devices. Spam can be transported by different means, including email, email attachments, and web accesses. Spam protection mechanisms include signature definitions.

TxDOT Discussion

Note for systems subject to FedRAMP requirements:

When Cloud Service Offering (CSO) sends email on behalf of the government as part of the business offering, Control Description should include implementation of Domain-based Message Authentication, Reporting & Conformance (DMARC) on the sending domain for outgoing messages as described in DHS Binding Operational Directive (BOD) 18-01.

https://cyber.dhs.gov/bod/18-01/

Cloud Service Providers (CSPs) should confirm DMARC configuration (where appropriate) to ensure that policy=reject and the rua parameter includes reports@dmarc.cyber.dhs.gov. DMARC compliance should be documented in the SI-08 control implementation solution description, and list the FROM: domain(s) that will be seen by email recipients.

[Source: FedRAMP Security Controls Baseline SI-8]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-45, 800-177; CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

PL-09, SC-05, SC-07, SI-04

SI-08(02) Automatic Updates

Baselines

Moderate, High

Overlays

CJIS; FedRAMP Moderate, FedRAMP High

Requirements

Automatically update spam protection mechanisms at least monthly.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.01 CJIS — Automatically update spam protection mechanisms at least daily. [Source: CJIS SI-08(02)]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Using automated mechanisms to update spam protection mechanisms helps to ensure that updates occur on a regular basis and provide the latest content and protection capabilities.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

NIST SP 800-45, 800-177; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

SI-10 Information Input Validation

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Check the validity of the following information inputs: all inputs to web/application servers, database servers, and any system or application input (as defined in applicable System Security Plans (SSPs)).

Implementation Standards

Std.01 — Configure systems to:

a. Check all arguments or input data strings submitted by users, external processes, or untrusted internal processes as close to the point of origin as possible, and before passing to any other application or interpreter;

b. Validate all values that originate externally to the application program itself, including arguments, environment variables, and information system parameters;

c. Reject and discard invalid values, parameters, strings, or objects.

Std.02 — For Web and mobile apps, test user input form fields for malicious commands (e.g. SQL injection).

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.04 CJIS — Check the validity of the following information inputs: all inputs to web/application servers, database servers, and any system or application input that might receive or process CJI. [Source: CJIS SI-10]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.03 FedRAMP — Validate all information inputs and document any exceptions. [Source: FedRAMP Security Controls Baseline SI-10]

Discussion

Checking the valid syntax and semantics of system inputs—including character set, length, numerical range, and acceptable values—verifies that inputs match specified definitions for format and content. For example, if the organization specifies that numerical values between 1-100 are the only acceptable inputs for a field in a given application, inputs of "387," "abc," or "%K%" are invalid inputs and are not accepted as input to the system. Valid inputs are likely to vary from field to field within a software application. Applications typically follow well-defined protocols that use structured

messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the corrupted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing them to interpreters prevents the content from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevents attacks such as cross-site scripting and a variety of injection attacks.

TxDOT Discussion

For Web and mobile apps, SQL queries should be crafted with user content passed into a bind variable and should avoid creation by dynamic string concatenation.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

OMB A-130; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

None.

SI-11 Error Handling

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and

b. Reveal error messages only to authorized personnel as identified in the System Security Plan (SSP).

Implementation Standards

Std.01 — Perform risk analysis to identify error conditions to be identified and required timelines for error handling.

Std.02 — Error messages revealed to users must not include file pathnames or system architecture information nor should error messages reveal details about the internal functionality of the application.

Std.03 — Error messages and alerts revealed to the administrator should include file pathnames or system architecture information, may include criticality or severity level if determined, and must be written to the application's error log and audit trail.

Std.04 — Turn off debugging on production web servers.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SI-11.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baselines, the following standard applies:

Std.05 FedRAMP — Reveal error messages only to authorized personnel as identified in the System Security Plan (SSP), to include the ISSO and/or similar role within the organization. [Source: FedRAMP Security Controls Baseline SI-11]

Discussion

Organizations consider the structure and content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes stack traces and implementation details; erroneous logon attempts with passwords mistakenly entered as the username; mission or business information that can be derived from, if not stated explicitly by, the information recorded; and personally identifiable information, such as account numbers, social security numbers, and credit card numbers. Error messages may also provide a covert channel for transmitting information.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AU-02, AU-03, SI-02

SI-12 Information Management and Retention

Baselines

Low, Moderate, High

Overlays

CJIS; Privacy; TX-RAMP Level 1, TX-RAMP Level 2; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.

Implementation Standards

Std.01 — Rescinded in V2.2.

Std.02 — Document output handling, media protection, and retention requirements in the System Security Plan (SSP) and retain and dispose of information system output accordingly.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SI-12.

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 1 and Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Information management and retention requirements cover the full life cycle of information, in some cases extending beyond system disposal. Information to be retained may also include policies, procedures, plans, reports, data output from control implementation, and other types of administrative information. The National Archives and Records Administration (NARA) provides federal policy and guidance on records retention and schedules. If organizations have a records management office, consider coordinating with records management personnel. Records produced from the output of implemented controls that may require management and retention include, but are not limited to: All XX-01, AC-06(09), AT-04, AU-12, CA-02, CA-03, CA-05, CA-06, CA-07, CA-08, CA-09, CM-02, CM-03, CM-04, CM-06, CM-08, CM-09, CM-12, CM-13, CP-02, IR-06, IR-08, MA-02, MA-04, PE-02, PE-08, PE-16, PE-17, PL-02, PL-04, PL-07, PL-08, PM-05, PM-08, PM-09, PM-18, PM-21, PM-27, PM-28, PM-30, PM-31, PS-

02, PS-06, PS-07, PT-02, PT-03, PT-07, RA-02, RA-03, RA-05, RA-08, SA-04, SA-05, SA-08, SA-10, SI-04, SR-02, SR-04, SR-08.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

USC 2901; OMB A-130; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

AC-01, AT-01, AU-01, AU-05, AU-11, CA-01, CA-02, CA-03, CA-05, CA-06, CA-07, CA-09, CM-01, CM-05, CM-09, CP-01, CP-02, IA-01, IR-01, IR-08, MA-01, MP-01, MP-02, MP-03, MP-04, MP-06, PE-01, PL-01, PL-02, PL-04, PM-01, PM-04, PM-08, PM-09, PS-01, PS-02, PS-06, PT-01, PT-02, PT-03, RA-01, RA-02, RA-03, SA-01, SA-05, SA-08, SC-01, SI-01, SR-01, SR-02

SI-12(01) Limit Personally Identifiable Information Elements

Baselines

N/A

Overlays

CJIS; Privacy

Requirements

Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: elements of sensitive personal information (SPI) defined in accordance with the TxDOT Data Classification Policy and identified in the privacy risk assessment.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.01 CJIS — Limit personally identifiable information being processed in the information life cycle to the minimum PII necessary to achieve the purpose for which it is collected. [Source: CJIS SI-12(01)]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for operational purposes helps to reduce the level of privacy risk created by a system. The information life cycle includes information creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining which elements of personally identifiable information may create risk.

TxDOT Discussion

None.

TxDOT References

Data Classification Policy; Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

USC 2901; OMB A-130; CJIS Security Policy

Related Controls

PM-25

SI-12(02) Minimize Personally Identifiable Information in Testing, Training, and Research

Baselines

N/A

Overlays

CJIS; PCI DSS; Privacy

Requirements

Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: techniques as defined in SI-19.

Implementation Standards

Std.01 — Where feasible, use fictional or synthetic information for research, testing, or training.

Std.02 — Where live data must be used for research or testing, purge data or sanitize systems at the conclusion of such activities.

Std.03 — Information acquired by TxDOT or a component of the agency under a pledge of confidentiality and for exclusively statistical purposes shall be used by officers, employees, or agents of the agency exclusively for statistical purposes. [Source: OMB A-130 Appendix II Sec. 6]

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.04 PCI — Live primary account numbers (PANs) are not used in pre-production environments, except where those environments are included in the Cardholder Data Environment (CDE) and protected in accordance with all applicable PCI DSS requirements. [Source: PCI DSS 6.5.5]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.05 CJIS — Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: data obfuscation, randomization, anonymization, or use of synthetic data. [Source: CJIS SI-12(02)]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Organizations can minimize the risk to an individual's privacy by employing techniques such as de-identification or synthetic data. Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for research, testing, or training helps reduce the level of privacy risk created by a system. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining the techniques to use and when to use them.

TxDOT Discussion

Statistical purpose refers to the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that comprise such groups.

TxDOT and agency components should protect the integrity and confidentiality of this information against unauthorized access, use, disclosure, modification, or destruction throughout the life cycle of the information. TxDOT and agency components shall also adhere to legal requirements and should follow best practices for protecting the confidentiality of data, including training their employees and agents, and ensuring the physical and information system security of confidential information. [Source: OMB A-130 Appendix II Sec. 6]

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

USC 2901; OMB A-130; PCI DSS; CJIS Security Policy

Related Controls

PM-22, PM-25, SI-19

SI-12(03) Information Disposal

Baselines

N/A

Overlays

CJIS; Privacy

Requirements

Use the following techniques to dispose of, destroy, or erase information following the retention period: techniques as outlined in MP-06.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.01 CJIS — Use the following techniques to dispose of, destroy, or erase information following the retention period: as defined in MP-06. [Source: CJIS SI-12(03)]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Organizations can minimize both security and privacy risks by disposing of information when it is no longer needed. The disposal or destruction of information applies to originals as well as copies and archived records, including system logs that may contain personally identifiable information.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog

Federal References

USC 2901; OMB A-130; CJIS Security Policy

Related Controls

MP-06

SI-16 Memory Protection

Baselines

Moderate, High

Overlays

CJIS; Sensitive; TX-RAMP Level 2; FedRAMP Moderate, FedRAMP High

Requirements

Implement the following controls to protect the system memory from unauthorized code execution: detection, prevention, and recovery controls as specified in the System Security Plan (SSP).

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standards apply:

Std.01 CJIS — Implement the following controls to protect the system memory from unauthorized code execution: data execution prevention and address space layout randomization. [Source: CJIS SI-16]

TX-RAMP Correspondence

Compliance with this TxDOT control satisfies TX-RAMP Level 2 requirements.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Moderate and High baselines.

Discussion

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Controls employed to protect memory include data execution prevention and address space layout randomization. Data execution prevention controls can either be hardware-enforced or software-enforced with hardware enforcement providing the greater strength of mechanism.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

DIR Security Control Standards Catalog; TX-RAMP Program Manual

Federal References

FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

SC-03, SI-07

SI-19 De-identification

Baselines

N/A

Overlays

Privacy

Requirements

a. Remove the following elements of personally identifiable information from datasets: all elements of personally identifiable information (PII) as defined in Std.02; and

b. Evaluate at least annually for effectiveness of de-identification.

Implementation Standards

Std.01 — TxDOT shall destroy or arrange for the destruction of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business by modifying the sensitive personal information in the records to make the information unreadable or indecipherable through any means. [Source: TBC 521.052(b)(3)]

Std.02 — Sensitive personal information (SPI) meeting the definitions in Texas Business and Commerce Code 521 must be de-identified when identifiers are no longer needed for the purpose for which the data was collected.

Std.03 — Where feasible and within the limits of technology, locate and remove or redact SPI and/or use anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

De-identification is the general term for the process of removing the association between a set of identifying data and the data subject. Many datasets contain information about individuals that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records. Datasets may also contain other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Personally identifiable information is removed from datasets by trained individuals when such information is not (or no longer) necessary to satisfy the requirements envisioned for the data. For example, if the dataset is only used to produce aggregate statistics, the identifiers that are not needed for producing those statistics are removed. Removing identifiers improves privacy protection since information that is removed cannot be inadvertently disclosed or improperly used. Organizations may be subject to specific de-identification definitions or methods under applicable laws, regulations, or policies. Re-identification is a residual risk with de-identified data. Re-identification attacks can vary, including combining new datasets or other improvements in data analytics. Maintaining awareness of potential attacks and evaluating for the effectiveness of the de-identification over time support the management of this residual risk.

TxDOT Discussion

Personally identifiable information (PII) is defined as:

Information that alone or in conjunction with other information identifies an individual, including an individual's name, Social Security number, date of birth, government-issued identification number, mother's maiden name, unique biometric data, such as the individual's fingerprint, voice print, and retina or iris image. The definition also includes unique electronic identification number, address, or routing code. [Source: TBC 521.002(a)(1)]

Sensitive personal information (SPI) is defined as:

An individual's first name or first initial and last name in combination with any one or more of the following unencrypted items: social security number, driver's license number or government-issued identification number, account number, credit or debit card number in combination with any required security code, access code, or password that would permit access to an

individual's financial account. Also, information that identifies an individual and relates to the physical or mental health or condition of the individual, the provision of health care to the individual, payment for the provision of health care to the individual. However, the term "sensitive personal information" does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government. [Source: TBC 521.002(a)(2)]

TxDOT References

Information Security and Privacy Policy

State References

TBC 521

Federal References

OMB A-130; NIST SP 800-188

Related Controls

MP-06, PM-22, RA-02, SI-12

SR — Supply Chain Risk Management

SR-01 Policy and Procedures

Baselines

Low, Moderate, High

Overlays

CJIS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop, document, and disseminate to appropriate personnel:

1. Organization-level supply chain risk management policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;

b. Designate a senior management official as defined in the supply chain risk management policy to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and

c. Review and update the current supply chain risk management:

1. Policy every year and following major changes to legislation or security requirements; and

2. Procedures every year and following major changes to legislation or security requirements.

Implementation Standards

Std.01 — Security requirements shall be identified, documented, and addressed in all phases of supply chain risk management.

Std.02 — The Information Security Officer shall be responsible for:

a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of 1 TAC 202 and the agency's information security risks;

b. Providing guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities under 1 TAC 202; and

c. Recommending and collaborating to establish policies, procedures, and practices, in cooperation with the agency Information Resources Manager, information-owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, access, exposure, or disclosure. [Source: 1 TAC 202.21(b)(3, 5, 8)]

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.03 CJIS — Review and update the current supply chain risk management policy and procedures following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. [Source: CJIS SR-01]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Supply chain risk management policy and procedures address the controls in the SR family as well as supply chain-related controls in other families that

are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of supply chain risk management policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to supply chain risk management policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

1 TAC 202

Federal References

Secure Technology Act; 41 CFR 201; EO 13873; NIST SP 800-12, 800-30, 800-39, 800-100, 800-161; CNSSD 505; FedRAMP Security Controls Baseline ; CJIS Security Policy

Related Controls

PM-09, PM-30, PS-08, SI-12

SR-02 Supply Chain Risk Management Plan

Baselines

Low, Moderate, High

Overlays

CJIS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: all systems, system components, or system services under configuration management;

b. Review and update the supply chain risk management plan annually or as required, to address threat, organizational or environmental changes; and

c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

Implementation Standards

Std.01 — Develop a supply chain risk management plan template in accordance with the guidance presented in SP 800-161 (as amended).

Std.02 — Include external provider plan requirements in contracts as applicable.

Std.03 — Ensure that systems owners are aware of supply chain risk management (SCRM) plans.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SR-02.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

The dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers, present an increasing level of risk to an organization. Threat actions that may increase security or privacy risks include unauthorized production, the insertion or use of counterfeits, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain. Supply chain risks can be endemic or systemic within a system element or component, a system, an organization, a sector, or the Nation. Managing supply chain risk is a complex, multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with internal and external stakeholders. Supply chain risk management (SCRM) activities include identifying and assessing risks, determining appropriate risk response actions, developing SCRM plans to document response actions, and monitoring performance against plans. The SCRM plan (at the system-level) is implementation specific, providing policy implementation, requirements, constraints and implications. It can either be stand-alone, or incorporated into system security and privacy plans. The SCRM plan addresses managing, implementation, and monitoring of SCRM controls and the development/sustainment of systems across the SDLC to support mission and business functions.

Because supply chains can differ significantly across and within organizations, SCRM plans are tailored to the individual program, organizational, and operational contexts. Tailored SCRM plans provide the basis for determining whether a technology, service, system component, or system is fit for purpose, and as such, the controls need to be tailored accordingly. Tailored SCRM plans help organizations focus their resources on the most critical mission and business functions based on mission and business requirements and their risk environment. Supply chain risk management plans include an expression of the supply chain risk tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the plan, a description of and justification for supply chain risk mitigation measures taken, and associated roles and responsibilities. Finally, supply chain risk management plans address requirements for developing trustworthy, secure, privacy-protective, and resilient system components and systems,

including the application of the security design principles implemented as part of life cycle-based systems security engineering processes (see SA-08).

TxDOT Discussion

Correlate identified critical components/services to the information about the supply chain, the supply chain infrastructure, historical data, and SDLC to identify critical supply chain paths. [Source: SP 800-161]

Protect against supply chain threats to the information system, system component, or information system service by employing best practices and methodologies; and wherever possible, selecting components that have been previously reviewed by other government entities (e.g., National Information Assurance Partnership (NIAP)) as part of a comprehensive, defense-in-breadth information security strategy. [Source: SP 800-53r4 SA-12]

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

Secure Technology Act; 41 CFR 201; EO 13873; NIST SP 800-30, 800-39, 800-160-1, 800-161, 800-181; NIST IR 7622, 8272; CNSSD 505; FedRAMP Security Controls Baseline ; CJIS Security Policy

Related Controls

CA-02, CP-04, IR-04, MA-02, MA-06, PE-16, PL-02, PM-09, PM-30, RA-03, RA-07, SA-08, SI-04

SR-02(01) Establish SCRM Team

Baselines

Low, Moderate, High

Overlays

CJIS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Establish a supply chain risk management team consisting of personnel, roles, and responsibilities as identified in the supply chain risk management policy to lead and support the following SCRM activities: supply chain risk management activities as defined in the supply chain risk management plan.

Implementation Standards

Std.01 — Ensure that all activities are auditable.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.02 CJIS — Establish a supply chain risk management team to lead and support the following SCRM activities: information technology, contracting, information security, privacy, mission or business, legal, supply chain and logistics, acquisition, business continuity, and other relevant functions. [Source: CJIS SR-2(1)]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

To implement supply chain risk management plans, organizations establish a coordinated, team-based approach to identify and assess supply chain risks and manage these risks by using programmatic and technical mitigation techniques. The team approach enables organizations to conduct an analysis of their supply chain, communicate with internal and external partners or stakeholders, and gain broad consensus regarding the appropriate resources for SCRM. The SCRM team consists of organizational personnel with diverse roles and responsibilities for leading and supporting SCRM activities, including risk executive, information technology, contracting, information security, privacy, mission or business, legal, supply chain and logistics, acquisition, business continuity, and other relevant functions. Members of the SCRM team are involved in various aspects of the SDLC and, collectively,

have an awareness of and provide expertise in acquisition processes, legal practices, vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects and dependencies of systems. The SCRM team can be an extension of the security and privacy risk management processes or be included as part of an organizational risk management team.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

Secure Technology Act; 41 CFR 201; EO 13873; NIST SP 800-30, 800-39, 800-160-1, 800-161; NIST IR 7622, 8272; FedRAMP Security Controls Baseline ; CJIS Security Policy

Related Controls

None.

SR-03 Supply Chain Controls and Processes

Baselines

Low, Moderate, High

Overlays

FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of any system or system component under configuration management in coordination with personnel or roles as identified in the supply chain risk management policy;

b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or

consequences from supply chain-related events: supply chain controls as defined in the System Security Plan (SSP); and

c. Document the selected and implemented supply chain processes and controls in the SSP; supply chain risk management plan; SDLC; and maintenance plans (as applicable).

Implementation Standards

Std.01 — Identify changes to mission/business, operations, project/program procurement requirements or the supply chain to appropriately assess the impact to the organization's supply chain infrastructure. [Source: CNSSD 505]

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.02 FedRAMP — Cloud Service Offering (CSO) must document and maintain the supply chain custody, including replacement devices, to ensure the integrity of the devices before being introduced to the boundary. [Source: FedRAMP Security Controls Baseline SR-3]

Discussion

Supply chain elements include organizations, entities, or tools employed for the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of systems and system components. Supply chain processes include hardware, software, and firmware development processes; shipping and handling procedures; personnel security and physical security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the development, acquisition, maintenance and disposal of systems and system components. Supply chain elements and processes may be provided by organizations,

system integrators, or external providers. Weaknesses or deficiencies in supply chain elements or processes represent potential vulnerabilities that can be exploited by adversaries to cause harm to the organization and affect its ability to carry out its core missions or business functions. Supply chain personnel are individuals with roles and responsibilities in the supply chain.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

Secure Technology Act; 41 CFR 201; EO 13873; ISO 20243; NIST SP 800-30, 800-161; NIST IR 7622; FedRAMP Security Controls Baseline

Related Controls

CA-02, MA-02, MA-06, PE-03, PE-16, PL-08, PM-30, SA-02, SA-03, SA-04, SA-05, SA-08, SA-09, SA-10, SA-15, SC-07, SI-07, SR-06, SR-09, SR-11

SR-04 Provenance

Baselines

High

Overlays

N/A

Requirements

Document, monitor, and maintain valid provenance of the following systems, system components, and associated data: all systems and system components under configuration management, and associated data as required by CM-08.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

None.

Discussion

Every system and system component has a point of origin and may be changed throughout its existence. Provenance is the chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data. Organizations consider developing procedures (see SR-01) for allocating responsibilities for the creation, maintenance, and monitoring of provenance for systems and system components; transferring provenance documentation and responsibility between organizations; and preventing and monitoring for unauthorized changes to the provenance records. Organizations have methods to document, monitor, and maintain valid provenance baselines for systems, system components, and related data. These actions help track, assess, and document any changes to the provenance, including changes in supply chain elements or configuration, and help ensure non-repudiation of provenance information and the provenance change records. Provenance considerations are addressed throughout the system development life cycle and incorporated into contracts and other arrangements, as appropriate.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

Secure Technology Act; 41 CFR 201; EO 13873; ISO 27036, 20243; NIST SP 800-160-1, 800-161; NIST IR 7622, 8112, 8272

Related Controls

CM-08, MA-02, MA-06, RA-09, SA-03, SA-08, SI-04

SR-05 Acquisition Strategies, Tools, and Methods

Baselines

Low, Moderate, High

Overlays

CJIS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: strategies, contract tools, and procurement methods as defined in the supply chain risk management plan.

Implementation Standards

Std.01 — Use the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to:

a. Reduce the likelihood of unauthorized modifications at each stage in the supply chain; and

b. Protect information systems and information system components until the agency takes delivery of such systems/components.

PCI DSS Correspondence

None.

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.02 CJIS — Use preferred suppliers who can provide attestation or demonstration of compliance with state or federal standards. [Source: CJIS SR-5]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

The use of the acquisition process provides an important vehicle to protect the supply chain. There are many useful tools and techniques available, including obscuring the end use of a system or system component, using blind or filtered buys, requiring tamper-evident packaging, or using trusted or controlled distribution. The results from a supply chain risk assessment can guide and inform the strategies, tools, and methods that are most applicable to the situation. Tools and techniques may provide protections against unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or backdoors, and poor development practices throughout the system development life cycle. Organizations also consider providing incentives for suppliers who implement controls, promote transparency into their processes and security and privacy practices, provide contract language that addresses the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy suppliers. Organizations consider providing training, education, and awareness programs for personnel regarding supply chain risk, available mitigation strategies, and when the programs should be employed. Methods for reviewing and protecting development plans, documentation, and evidence are commensurate with the security and privacy requirements of the organization. Contracts may specify documentation protection requirements.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

Secure Technology Act; 41 CFR 201; EO 13873; ISO 27036, 20243; NIST SP 800-30, 800-161; NIST IR 7622, 8272; FAR 52.204-25; FedRAMP Security Controls Baseline ; CJIS Security Policy

Related Controls

AT-03, SA-02, SA-03, SA-04, SA-05, SA-08, SA-09, SA-10, SA-15, SR-06, SR-09, SR-10, SR-11

SR-06 Supplier Assessments and Reviews

Baselines

Low, Moderate, High

Overlays

PCI DSS; FedRAMP Moderate, FedRAMP High

Requirements

Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide prior to entering into a contract and annually thereafter.

Implementation Standards

Std.01 — Ensure that contracts for the purchase of hardware and software using Federal funds comply with all applicable Federal supply chain restrictions including NDAA, FAR, and other regulations.

Std.02 — Ensure that all new or renewed contracts comply with TxDOT's technology prohibitions available at https://ftp.txdot.gov/pub/txdot/itd/cyversecurity/prohibited-techologies-list-cybersecurity.pdf.

PCI DSS Correspondence

Compliance with this TxDOT control satisfies PCI DSS requirements 12.8.3 and 12.8.4.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Moderate or High baseline, the following standard applies:

Std.03 FedRAMP — Cloud Service Offerings (CSOs) must ensure that their supply chain vendors build and test their systems in alignment with NIST SP 800-171 or a commensurate security and compliance framework. CSOs must ensure that vendors are compliant with physical facility access and logical access controls to supplied products. [Source: FedRAMP Security Controls Baseline SR-6]

Discussion

An assessment and review of supplier risk includes security and supply chain risk management processes, foreign ownership, control or influence (FOCI), and the ability of the supplier to effectively assess subordinate second-tier and third-tier suppliers and contractors. The reviews may be conducted by the organization or by an independent third party. The reviews consider documented processes, documented controls, all-source intelligence, and publicly available information related to the supplier or contractor. Organizations can use open-source information to monitor for indications of stolen information, poor development and quality control practices, information spillage, or counterfeits. In some cases, it may be appropriate or required to share assessment and review results with other organizations in accordance with any applicable rules, policies, or inter-organizational agreements or contracts.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy; Prohibited Software and Applications

State References

Statewide Security Plan for Prohibited Technologies

Federal References

Secure Technology Act; 41 CFR 201; EO 13873; ISO 27036, 20243; FIPS 140, 180, 186, 202; NIST SP 800-30, 800-161; NIST IR 7622, 8272; FAR 52.204-25; PCI DSS

Related Controls

SR-03, SR-05

SR-08 Notification Agreements

Baselines

Low, Moderate, High

Overlays

CJIS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises; results of assessments or audits; and information as defined in Std.01.

Implementation Standards

Std.01 — Ensure that contracts include specific requirements for provider to notify agency, as applicable, of:

a. End-of-support/End-of-Life;

b. Major changes in a maintenance organization's structure or process (for example, physical move to a different location, change in ownership, outsourcing, or changes in personnel);

c. Successful and attempted threat events that may affect agency's systems;

d. Available protective or mitigating measures to address identified vulnerabilities; and

e. Any system, service, or component-specific information that affects maintenance or continuity plans.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirement SR-08.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.02 FedRAMP — Cloud Service Offerings (CSOs) must ensure and document how they receive notifications from their supply chain vendor of newly discovered vulnerabilities including zero-day vulnerabilities. [Source: FedRAMP Security Controls Baseline SR-8]

Discussion

The establishment of agreements and procedures facilitates communications among supply chain entities. Early notification of compromises and potential compromises in the supply chain that can potentially adversely affect or have adversely affected organizational systems or system components is essential for organizations to effectively respond to such incidents. The results of assessments or audits may include open-source information that contributed to a decision or result and could be used to help the supply chain entity resolve a concern or improve its processes.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

Secure Technology Act; 41 CFR 201; EO 13873; ISO 27036; NIST SP 800-30, 800-161; NIST IR 7622; FedRAMP Security Controls Baseline; CJIS Security Policy

Related Controls

IR-04, IR-06, IR-08

SR-09 Tamper Resistance and Detection

Baselines

High

Overlays

PCI DSS; FedRAMP High

Requirements

Implement a tamper protection program for the system, system component, or system service.

Implementation Standards

Std.01 — Protect assets from tampering or unapproved substitution.

Std.02 — Monitor for evidence of tampering indicators.

Std.03 — Prevent security mechanisms from being compromised by adverse physical conditions.

Std.04 — Require authorization for all disabling of tamper detection and response mechanisms.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.05 PCI — Point of Interaction (POI) devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following:

a. Maintaining a list of POI devices.

b. Periodically inspecting POI devices to look for tampering or unauthorized substitution.

c. Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.

[Source: PCI DSS 9.5.1]

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the High baseline, the following standard applies:

Std.05 FedRAMP — Cloud Service Offerings (CSOs) must ensure vendors provide authenticity of software and patches supplied to the service provider including documenting the safeguards in place. [Source: FedRAMP Security Controls Baseline SR-9]

Discussion

Anti-tamper technologies, tools, and techniques provide a level of protection for systems, system components, and services against many threats, including reverse engineering, modification, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems and components during distribution and when in use.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

ISO 20243; PCI DSS; FedRAMP Security Controls Baseline

Related Controls

PE-03, PM-30, SA-15, SI-04, SI-07, SR-03, SR-04, SR-05, SR-10, SR-11

SR-09(01) Multiple Stages of System Development Life Cycle

Baselines

High

Overlays

FedRAMP High

Requirements

Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the High baseline.

Discussion

The system development life cycle includes research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal. Organizations use a combination of hardware and software techniques for tamper resistance and detection. Organizations use obfuscation and self-checking to make reverse engineering and modifications more difficult, time-consuming, and expensive for adversaries. The customization of systems and system components can make substitutions easier to detect and therefore limit damage.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

ISO 20243; FedRAMP Security Controls Baseline

Related Controls

SA-03

SR-10 Inspection of Systems or Components

Baselines

Low, Moderate, High

Overlays

CJIS; PCI DSS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Inspect the following systems or system components: at random; upon receipt and before reassignment; and whenever indicators of compromise are reported to detect tampering: all systems or system components under configuration management.

Implementation Standards

Std.01 — Examine inconsistencies in tracking and labeling of physical or digital components to identify counterfeit components.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.02 PCI —

a. Point of Interaction (POI) device surfaces are periodically inspected to detect tampering and unauthorized substitution. [Source: PCI DSS 9.5.1.2]

b. The frequency of periodic Point of Interaction (POI) device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1; at a minimum, at least once every month (monthly). [Source: PCI DSS 9.5.1.2.1; PCI DSS v4.x: Targeted Risk Analysis Guidance]

CJIS Correspondence

For systems processing CJIS data, the following additional Implementation Standard applies:

Std.02 CJIS — Inspect the following systems or system components upon initial procurement and periodically as needed to detect tampering: systems used to process, store, or transmit CJI. [Source: CJIS SR-10]

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

The inspection of systems or systems components for tamper resistance and detection addresses physical and logical tampering and is applied to systems and system components removed from organization-controlled areas. Indications of a need for inspection include changes in packaging, specifications, factory location, or entity in which the part is purchased, and when individuals return from travel to high-risk locations.

TxDOT Discussion

Indications of counterfeit that may be detectable upon delivery include (but are not limited to):

1. Mismatched lot and the date code;

2. Absent or mismatched manufacturer's logo and label on the ICT component and its documentation;

3. Mismatched bar code and printed part number; and

4. Inconsistent descriptions between package materials and datasheet descriptions.

These comparisons can be done via visual inspections, or a variety of pattern-matching techniques used in supply chain logistics. [Source: SP 800-161]

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

ISO 20243; PCI DSS; FedRAMP Security Controls Baseline ; CJIS Security Policy

Related Controls

AT-03, PM-30, SI-04, SI-07, SR-03, SR-04, SR-05, SR-09, SR-11

SR-11 Component Authenticity

Baselines

Low, Moderate, High

Overlays

FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and

b. Report counterfeit system components to: source of counterfeit component; approved external reporting organizations; personnel or roles as identified in the supply chain risk management policy.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

For systems subject to FedRAMP requirements at the Low, Moderate, or High baselines, the following standard applies:

Std.01 FedRAMP — Cloud Service Offerings (CSOs) must ensure that their supply chain vendors provide authenticity of software and patches and the vendor must have a plan to protect the development pipeline. [Source: FedRAMP Security Controls Baseline SR-11]

Discussion

Sources of counterfeit components include manufacturers, developers, vendors, and contractors. Anti-counterfeiting policies and procedures support tamper resistance and provide a level of protection against the introduction of malicious code. External reporting organizations include CISA.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

ISO 20243; FedRAMP Security Controls Baseline

Related Controls

PE-03, SA-04, SI-07, SR-09, SR-10

SR-11(01) Anti-Counterfeit Training

Baselines

Low, Moderate, High

Overlays

PCI DSS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Train personnel or roles as defined in the supply chain risk management policy to detect counterfeit system components (including hardware, software, and firmware).

Implementation Standards

Std.01 — Ensure that role-based training for SCRM meets frequencies defined in AT-03.

PCI DSS Correspondence

For systems processing PCI DSS data, or that support PCI DSS processes, the following additional Implementation Standard applies:

Std.02 PCI — Training is provided for personnel in Point of Interaction (POI) environments to be aware of attempted tampering or replacement of POI devices, and includes:

a. Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices.

b. Procedures to ensure devices are not installed, replaced, or returned without verification.

c. Being aware of suspicious behavior around devices.

d. Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.

[Source: PCI DSS 9.5.1.3]

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

None.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

ISO 20243; PCI DSS; FedRAMP Security Controls Baseline

Related Controls

AT-03

SR-11(02) Configuration Control for Component Service and Repair

Baselines

Low, Moderate, High

Overlays

FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: all system components under configuration management.

Implementation Standards

None.

PCI DSS Correspondence

None.

CJIS Correspondence

None.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

None.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

ISO 20243; FedRAMP Security Controls Baseline

Related Controls

CM-03, MA-02, MA-04, SA-10

SR-12 Component Disposal

Baselines

Low, Moderate, High

Overlays

CJIS; FedRAMP Low, FedRAMP Moderate, FedRAMP High

Requirements

Dispose of system components using the following techniques and methods: techniques and methods in accordance with Stds.01-03.

Implementation Standards

Std.01 — Sanitize all components prior to disposal in accordance with MP-06.

Std.02 — Securely dispose of or destroy all components subject to configuration management.

Std.03 — Document all disposals in component inventories.

PCI DSS Correspondence

None.

CJIS Correspondence

Compliance with this TxDOT control satisfies CJIS requirements SR-12 and 5.20.1.1.

TX-RAMP Correspondence

None.

FedRAMP Correspondence

Compliance with this TxDOT control satisfies the corresponding FedRAMP control at the Low, Moderate, and High baselines.

Discussion

Data, documentation, tools, or system components can be disposed of at any time during the system development life cycle (not only in the disposal or retirement phase of the life cycle). For example, disposal can occur during research and development, design, prototyping, or operations/maintenance and include methods such as disk cleaning, removal of cryptographic keys, partial reuse of components. Opportunities for compromise during disposal affect physical and logical data, including system documentation in paper-based or digital files; shipping and delivery documentation; memory sticks with software code; or complete routers or servers that include permanent media, which contain sensitive or proprietary information. Additionally,

proper disposal of system components helps to prevent such components from entering the gray market.

TxDOT Discussion

None.

TxDOT References

Information Security and Privacy Policy

State References

None.

Federal References

CJIS Security Policy; FedRAMP Security Controls Baseline

Related Controls

MP-06

Controls Contents

AC — Access Control 12
AC-01 Policy and Procedures 12
AC-02 Account Management 14
AC-02(01) Automated System Account Management 20
AC-02(02) Automated Temporary and Emergency Account Management 22
AC-02(03) Disable Accounts 24
AC-02(04) Automated Audit Actions 26
AC-02(05) Inactivity Logout 27
AC-02(07) Privileged User Accounts 28
AC-02(09) Restrictions on Use of Shared and Group Accounts 30
AC-02(11) Usage Conditions 31
AC-02(12) Account Monitoring for Atypical Usage 33
AC-02(13) Disable Accounts for High-risk Individuals 34
AC-03 Access Enforcement 36
AC-03(14) Individual Access 38
AC-04 Information Flow Enforcement 39
AC-04(04) Flow Control of Encrypted Information 42
AC-04(21) Physical or Logical Separation of Information Flows 44
AC-05 Separation of Duties 45
AC-06 Least Privilege 48
AC-06(01) Authorize Access to Security Functions 50
AC-06(02) Non-privileged Access for Nonsecurity Functions 53
AC-06(03) Network Access to Privileged Commands 54
AC-06(05) Privileged Accounts 55
AC-06(07) Review of User Privileges 57
AC-06(08) Privilege Levels for Code Execution 58
AC-06(09) Log Use of Privileged Functions 60
AC-06(10) Prohibit Non-privileged Users from Executing Privileged Functions 61
AC-07 Unsuccessful Logon Attempts 62
AC-07(02) Purge or Wipe Mobile Device 66
AC-08 System Use Notification 68

AC-10 Concurrent Session Control 71
AC-11 Device Lock 72
AC-11(01) Pattern-hiding Displays 74
AC-12 Session Termination 76
AC-14 Permitted Actions Without Identification or Authentication 78
AC-17 Remote Access 79
AC-17(01) Monitoring and Control 83
AC-17(02) Protection of Confidentiality and Integrity Using Encryption 84
AC-17(03) Managed Access Control Points 86
AC-17(04) Privileged Commands and Access 87
AC-17(09) Disconnect or Disable Access 88
AC-18 Wireless Access 90
AC-18(01) Authentication and Encryption 94
AC-18(03) Disable Wireless Networking 96
AC-18(04) Restrict Configurations by Users 97
AC-18(05) Antennas and Transmission Power Levels 99
AC-19 Access Control for Mobile Devices 100
AC-19(05) Full Device or Container-Based Encryption 105
AC-20 Use of External Systems 107
AC-20(01) Limits on Authorized Use 110
AC-20(02) Portable Storage Devices — Restricted Use 112
AC-21 Information Sharing 113
AC-22 Publicly Accessible Content 116
AT — Awareness and Training 118
AT-01 Policy and Procedures 118
AT-02 Literacy Training and Awareness 121
AT-02(02) Insider Threat 125
AT-02(03) Social Engineering and Mining 126
AT-03 Role-Based Training 128
AT-03(05) Processing Personally Identifiable Information 134
AT-04 Training Records 136
AU — Audit and Accountability 138
AU-01 Policy and Procedures 138

AU-02 Event Logging 140
AU-03 Content of Audit Records 145
AU-03(01) Additional Audit Information 147
AU-03(03) Limit Personally Identifiable Information Elements 150
AU-04 Audit Log Storage Capacity 151
AU-05 Response to Audit Logging Process Failures 152
AU-05(01) Storage Capacity Warning 154
AU-05(02) Real-Time Alerts 155
AU-06 Audit Record Review, Analysis, and Reporting 157
AU-06(01) Automated Process Integration 160
AU-06(03) Correlate Audit Record Repositories 162
AU-06(04) Central Review and Analysis 164
AU-06(05) Integrated Analysis of Audit Records 165
AU-06(06) Correlation with Physical Monitoring 167
AU-06(07) Permitted Actions 168
AU-07 Audit Record Reduction and Report Generation 170
AU-07(01) Automatic Processing 171
AU-08 Time Stamps 173
AU-09 Protection of Audit Information 175
AU-09(02) Store on Separate Physical Systems or Components 177
AU-09(03) Cryptographic Protection 178
AU-09(04) Access by Subset of Privileged Users 180
AU-10 Non-Repudiation 181
AU-11 Audit Record Retention 183
AU-12 Audit Record Generation 185
AU-12(01) System-Wide and Time-Correlated Audit Trail 187
AU-12(03) Changes by Authorized Individuals 188
CA — Assessment, Authorization, and Monitoring 190
CA-01 Policy and Procedures 190
CA-02 Control Assessments 193
CA-02(01) Independent Assessors 198
CA-02(02) Specialized Assessments 201
CA-02(03) Leveraging Results from External Organizations 202

CA-03 Information Exchange 204
CA-03(06) Transfer Authorizations 209
CA-05 Plan of Action and Milestones 211
CA-06 Authorization 213
CA-07 Continuous Monitoring 216
CA-07(01) Independent Assessment 221
CA-07(04) Risk Monitoring 222
CA-08 Penetration Testing 224
CA-08(01) Independent Penetration Testing Agent or Team 229
CA-08(02) Red Team Exercises 231
CA-09 Internal System Connections 232
CM — Configuration Management 235
CM-01 Policy and Procedures 235
CM-02 Baseline Configuration 238
CM-02(02) Automation Support for Accuracy and Currency 240
CM-02(03) Retention of Previous Configurations 242
CM-02(07) Configure Systems and Components for High-Risk Areas 243
CM-03 Configuration Change Control 245
CM-03(01) Automated Documentation, Notification, and Prohibition of Changes 249
CM-03(02) Testing, Validation, and Documentation of Changes 250
CM-03(04) Security and Privacy Representatives 252
CM-03(06) Cryptography Management 253
CM-04 Impact Analyses 255
CM-04(01) Separate Test Environments 256
CM-04(02) Verification of Controls 258
CM-05 Access Restrictions for Change 259
CM-05(01) Automated Access Enforcement and Audit Records 261
CM-05(05) Privilege Limitation for Production and Operation 262
CM-06 Configuration Settings 264
CM-06(01) Automated Management, Application, and Verification 268
CM-06(02) Respond to Unauthorized Changes 270
CM-07 Least Functionality 271

CM-07(01) Periodic Review 274
CM-07(02) Prevent Program Execution 276
CM-07(04) Unauthorized Software — Deny-by-Exception 278
CM-07(05) Authorized Software — Allow-by-Exception 279
CM-08 System Component Inventory 281
CM-08(01) Updates During Installation and Removal 286
CM-08(02) Automated Maintenance 288
CM-08(03) Automated Unauthorized Component Detection 289
CM-08(04) Accountability Information 291
CM-09 Configuration Management Plan 292
CM-10 Software Usage Restrictions 295
CM-11 User-Installed Software 296
CM-12 Information Location 298
CM-12(01) Automated Tools to Support Information Location 300
CM-14 Signed Components 302
CP — Contingency Planning 304
CP-01 Policy and Procedures 304
CP-02 Contingency Plan 306
CP-02(01) Coordinate with Related Plans 311
CP-02(02) Capacity Planning 313
CP-02(03) Resume Mission and Business Functions 314
CP-02(05) Continue Mission and Business Functions 316
CP-02(08) Identify Critical Assets 317
CP-03 Contingency Training 319
CP-03(01) Simulated Events 322
CP-04 Contingency Plan Testing 323
CP-04(01) Coordinate with Related Plans 326
CP-04(02) Alternate Processing Site 327
CP-06 Alternate Storage Site 329
CP-06(01) Separation from Primary Site 331
CP-06(02) Recovery Time and Recovery Point Objectives 332
CP-06(03) Accessibility 334
CP-07 Alternate Processing Site 335

CP-07(01) Separation from Primary Site 337
CP-07(02) Accessibility 339
CP-07(03) Priority of Service 340
CP-07(04) Preparation for Use 341
CP-08 Telecommunications Services 343
CP-08(01) Priority of Service Provisions 345
CP-08(02) Single Points of Failure 346
CP-08(03) Separation of Primary and Alternate Providers 348
CP-08(04) Provider Contingency Plan 349
CP-09 System Backup 350
CP-09(01) Testing for Reliability and Integrity 353
CP-09(02) Test Restoration Using Sampling 355
CP-09(03) Separate Storage for Critical Information 357
CP-09(05) Transfer to Alternate Storage Site 358
CP-09(08) Cryptographic Protection 360
CP-10 System Recovery and Reconstitution 361
CP-10(02) Transaction Recovery 363
CP-10(04) Restore Within Time Period 365
CP-11 Alternate Communications Protocols 366
IA — Identification and Authentication 368
IA-01 Policy and Procedures 368
IA-02 Identification and Authentication (Organizational Users) 371
IA-02(01) Multi-Factor Authentication to Privileged Accounts 374
IA-02(02) Multi-Factor Authentication to Non-Privileged Accounts 376
IA-02(05) Individual Authentication with Group Authentication 378
IA-02(06) Access to Accounts — Separate Device 379
IA-02(08) Access to Accounts — Replay Resistant 381
IA-02(12) Acceptance of PIV Credentials 383
IA-03 Device Identification and Authentication 384
IA-04 Identifier Management 386
IA-04(04) Identify User Status 388
IA-05 Authenticator Management 390
IA-05(01) Password-Based Authentication 402

IA-05(02) Public Key-Based Authentication 414
IA-05(06) Protection of Authenticators 416
IA-05(07) No Embedded Unencrypted Static Authenticators 418
IA-05(08) Multiple System Accounts 420
IA-05(13) Expiration of Cached Authenticators 421
IA-06 Authentication Feedback 422
IA-07 Cryptographic Module Authentication 424
IA-08 Identification and Authentication (Non-Organizational Users) 425
IA-08(01) Acceptance of PIV Credentials from Other Agencies 427
IA-08(02) Acceptance of External Authenticators 429
IA-08(04) Use of Defined Profiles 430
IA-11 Re-Authentication 432
IA-12 Identity Proofing 434
IA-12(02) Identity Evidence 435
IA-12(03) Identity Evidence Validation and Verification 437
IA-12(04) In-Person Validation and Verification 444
IA-12(05) Address Confirmation 445
IR — Incident Response 449
IR-01 Policy and Procedures 449
IR-02 Incident Response Training 451
IR-02(01) Simulated Events 454
IR-02(02) Automated Training Environments 455
IR-02(03) Breach 457
IR-03 Incident Response Testing 458
IR-03(02) Coordination with Related Plans 461
IR-04 Incident Handling 462
IR-04(01) Automated Incident Handling Processes 466
IR-04(02) Dynamic Reconfiguration 467
IR-04(04) Information Correlation 469
IR-04(06) Insider Threats 470
IR-04(11) Integrated Incident Response Team 472
IR-05 Incident Monitoring 473
IR-05(01) Automated Tracking, Data Collection, and Analysis 475

IR-06 Incident Reporting 477
IR-06(01) Automated Reporting 480
IR-06(03) Supply Chain Coordination 482
IR-07 Incident Response Assistance 483
IR-07(01) Automation Support for Availability of Information and Support 485
IR-08 Incident Response Plan 486
IR-08(01) Breaches 489
IR-09 Information Spillage Response 493
IR-09(02) Training 494
IR-09(03) Post-spill Operations 496
IR-09(04) Exposure to Unauthorized Personnel 497
MA — Maintenance 499
MA-01 Policy and Procedures 499
MA-02 Controlled Maintenance 501
MA-02(02) Automated Maintenance Activities 504
MA-03 Maintenance Tools 505
MA-03(01) Inspect Tools 507
MA-03(02) Inspect Media 509
MA-03(03) Prevent Unauthorized Removal 510
MA-04 Nonlocal Maintenance 512
MA-04(03) Comparable Security and Sanitization 514
MA-05 Maintenance Personnel 515
MA-05(01) Individuals Without Appropriate Access 518
MA-06 Timely Maintenance 520
MP — Media Protection 522
MP-01 Policy and Procedures 522
MP-02 Media Access 524
MP-03 Media Marking 526
MP-04 Media Storage 528
MP-05 Media Transport 530
MP-06 Media Sanitization 532
MP-06(01) Review, Approve, Track, Document, and Verify 537

MP-06(02) Equipment Testing 539
MP-06(03) Nondestructive Techniques 540
MP-07 Media Use 542
PE — Physical and Environmental Protection 546
PE-01 Policy and Procedures 546
PE-02 Physical Access Authorizations 549
PE-03 Physical Access Control 551
PE-03(01) System Access 555
PE-04 Access Control for Transmission 556
PE-05 Access Control for Output Devices 558
PE-06 Monitoring Physical Access 560
PE-06(01) Intrusion Alarms and Surveillance Equipment 562
PE-06(04) Monitoring Physical Access to Systems 564
PE-08 Visitor Access Records 565
PE-08(01) Automated Records Maintenance and Review 568
PE-08(03) Limit Personally Identifiable Information Elements 569
PE-09 Power Equipment and Cabling 571
PE-10 Emergency Shutoff 572
PE-11 Emergency Power 574
PE-11(01) Alternate Power Supply — Minimal Operational Capability 575
PE-12 Emergency Lighting 577
PE-13 Fire Protection 578
PE-13(01) Detection Systems — Automatic Activation and Notification 580
PE-13(02) Suppression Systems — Automatic Activation and Notification 582
PE-14 Environmental Controls 583
PE-14(02) Monitoring with Alarms and Notifications 585
PE-15 Water Damage Protection 586
PE-15(01) Automation Support 588
PE-16 Delivery and Removal 589
PE-17 Alternate Work Site 590
PE-18 Location of System Components 593
PL — Planning 595

PL-01 Policy and Procedures 595
PL-02 System Security and Privacy Plans 598
PL-04 Rules of Behavior 602
PL-04(01) Social Media and External Site/Application Usage Restrictions 605
PL-08 Security and Privacy Architectures 607
PL-09 Central Management 610
PL-10 Baseline Selection 612
PL-11 Baseline Tailoring 614
PM — Program Management 617
PM-01 Information Security Program Plan 617
PM-02 Information Security Program Leadership Role 624
PM-03 Information Security and Privacy Resources 626
PM-04 Plan of Action and Milestones Process 627
PM-05 System Inventory 629
PM-05(01) Inventory of Personally Identifiable Information 632
PM-06 Measures of Performance 633
PM-07 Enterprise Architecture 635
PM-08 Critical Infrastructure Plan 637
PM-09 Risk Management Strategy 638
PM-10 Authorization Process 642
PM-11 Mission and Business Process Definition 644
PM-12 Insider Threat Program 646
PM-13 Security and Privacy Workforce 649
PM-14 Testing, Training, and Monitoring 650
PM-15 Security and Privacy Groups and Associations 652
PM-16 Threat Awareness Program 654
PM-16(01) Automated Means for Sharing Threat Intelligence 656
PM-18 Privacy Program Plan 657
PM-19 Privacy Program Leadership Role 659
PM-20 Dissemination of Privacy Program Information 661
PM-20(01) Privacy Policies on Websites, Applications, and Digital Services 663

PM-21 Accounting of Disclosures 665
PM-22 Personally Identifiable Information Quality Management 667
PM-23 Data Governance Body 669
PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research 672
PM-26 Complaint Management 674
PM-27 Privacy Reporting 675
PM-28 Risk Framing 677
PM-30 Supply Chain Risk Management Strategy 679
PM-30(01) Suppliers of Critical or Mission-Essential Items 681
PM-31 Continuous Monitoring Strategy 682
PM-32 Purposing 685
PS — Personnel Security 687
PS-01 Policy and Procedures 687
PS-02 Position Risk Designation 689
PS-03 Personnel Screening 691
PS-03(03) Information Requiring Special Protective Measures 695
PS-04 Personnel Termination 696
PS-04(02) Automated Actions 698
PS-05 Personnel Transfer 700
PS-06 Access Agreements 702
PS-07 External Personnel Security 704
PS-08 Personnel Sanctions 706
PS-09 Position Descriptions 708
PT — Personally Identifiable Information Processing and Transparency 710
PT-01 Policy and Procedures 710
PT-02 Authority to Process Personally Identifiable Information 712
PT-03 Personally Identifiable Information Processing Purposes 715
PT-04 Consent 717
PT-05 Privacy Notice 719
PT-07 Specific Categories of Personally Identifiable Information 722
PT-07(01) Social Security Numbers 724

RA — Risk Assessment 726
RA-01 Policy and Procedures 726
RA-02 Security Categorization 730
RA-03 Risk Assessment 733
RA-03(01) Supply Chain Risk Assessment 737
RA-05 Vulnerability Monitoring and Scanning 738
RA-05(02) Update Vulnerabilities to Be Scanned 749
RA-05(03) Breadth and Depth of Coverage 751
RA-05(04) Discoverable Information 752
RA-05(05) Privileged Access 754
RA-05(08) Review Historic Audit Logs 755
RA-05(11) Public Disclosure Program 757
RA-07 Risk Response 758
RA-08 Privacy Impact Assessments 760
RA-09 Criticality Analysis 762
SA — System and Services Acquisition 765
SA-01 Policy and Procedures 765
SA-02 Allocation of Resources 768
SA-03 System Development Life Cycle 769
SA-04 Acquisition Process 772
SA-04(01) Functional Properties of Controls 776
SA-04(02) Design and Implementation Information for Controls 778
SA-04(05) System, Component, and Service Configurations 780
SA-04(09) Functions, Ports, Protocols, and Services in Use 781
SA-04(10) Use of Approved PIV Products 783
SA-05 System Documentation 784
SA-08 Security and Privacy Engineering Principles 787
SA-08(33) Minimization 791
SA-09 External System Services 792
SA-09(01) Risk Assessments and Organizational Approvals 801
SA-09(02) Identification of Functions, Ports, Protocols, and Services 802
SA-09(05) Processing, Storage, and Service Location 804
SA-10 Developer Configuration Management 806

SA-10(01) Software and Firmware Integrity Verification 808
SA-11 Developer Testing and Evaluation 809
SA-11(01) Static Code Analysis 812
SA-11(02) Threat Modeling and Vulnerability Analyses 815
SA-11(05) Penetration Testing 817
SA-11(08) Dynamic Code Analysis 819
SA-15 Development Process, Standards, and Tools 821
SA-15(03) Criticality Analysis 824
SA-16 Developer-provided Training 825
SA-17 Developer Security and Privacy Architecture and Design 827
SA-21 Developer Screening 829
SA-22 Unsupported System Components 831
SC — System and Communications Protection 834
SC-01 Policy and Procedures 834
SC-02 Separation of System and User Functionality 837
SC-03 Security Function Isolation 838
SC-04 Information in Shared System Resources 840
SC-05 Denial-of-Service Protection 841
SC-07 Boundary Protection 844
SC-07(03) Access Points 847
SC-07(04) External Telecommunications Services 849
SC-07(05) Deny by Default — Allow by Exception 851
SC-07(07) Split Tunneling for Remote Devices 853
SC-07(08) Route Traffic to Authenticated Proxy Servers 855
SC-07(10) Prevent Exfiltration 857
SC-07(12) Host-Based Protection 858
SC-07(18) Fail Secure 860
SC-07(20) Dynamic Isolation and Segregation 861
SC-07(21) Isolation of System Components 862
SC-07(24) Personally Identifiable Information 864
SC-08 Transmission Confidentiality and Integrity 866
SC-08(01) Cryptographic Protection 868
SC-10 Network Disconnect 871

SC-12 Cryptographic Key Establishment and Management 873
SC-12(01) Availability 877
SC-13 Cryptographic Protection 879
SC-15 Collaborative Computing Devices and Applications 883
SC-17 Public Key Infrastructure Certificates 885
SC-18 Mobile Code 887
SC-20 Secure Name/Address Resolution Service (Authoritative Source) 889
SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver) 891
SC-22 Architecture and Provisioning for Name/Address Resolution Service 893
SC-23 Session Authenticity 895
SC-24 Fail in Known State 896
SC-28 Protection of Information at Rest 898
SC-28(01) Cryptographic Protection 901
SC-39 Process Isolation 904
SC-45 System Time Synchronization 906
SC-45(01) Synchronization with Authoritative Time Source 908
SI — System and Information Integrity 910
SI-01 Policy and Procedures 910
SI-02 Flaw Remediation 913
SI-02(02) Automated Flaw Remediation Status 916
SI-02(03) Time to Remediate Flaws and Benchmarks for Corrective Actions 918
SI-03 Malicious Code Protection 919
SI-04 System Monitoring 924
SI-04(01) System-Wide Intrusion Detection System 929
SI-04(02) Automated Tools and Mechanisms for Real-Time Analysis .. 930
SI-04(04) Inbound and Outbound Communications Traffic 931
SI-04(05) System-Generated Alerts 933
SI-04(10) Visibility of Encrypted Communications 935
SI-04(11) Analyze Communications Traffic Anomalies 936
SI-04(12) Automated Organization-generated Alerts 938

SI-04(14) Wireless Intrusion Detection 939
SI-04(16) Correlate Monitoring Information 941
SI-04(18) Analyze Traffic and Covert Exfiltration 942
SI-04(19) Risk for Individuals 943
SI-04(20) Privileged Users 945
SI-04(22) Unauthorized Network Services 946
SI-04(23) Host-Based Devices 947
SI-05 Security Alerts, Advisories, and Directives 949
SI-05(01) Automated Alerts and Advisories 951
SI-06 Security and Privacy Function Verification 952
SI-07 Software, Firmware, and Information Integrity 954
SI-07(01) Integrity Checks 957
SI-07(02) Automated Notifications of Integrity Violations 959
SI-07(05) Automated Response to Integrity Violations 960
SI-07(07) Integration of Detection and Response 962
SI-07(15) Code Authentication 964
SI-08 Spam Protection 965
SI-08(02) Automatic Updates 967
SI-10 Information Input Validation 968
SI-11 Error Handling 970
SI-12 Information Management and Retention 972
SI-12(01) Limit Personally Identifiable Information Elements 974
SI-12(02) Minimize Personally Identifiable Information in Testing, Training, and Research 976
SI-12(03) Information Disposal 978
SI-16 Memory Protection 979
SI-19 De-identification 981
SR — Supply Chain Risk Management 984
SR-01 Policy and Procedures 984
SR-02 Supply Chain Risk Management Plan 987
SR-02(01) Establish SCRM Team 989
SR-03 Supply Chain Controls and Processes 991
SR-04 Provenance 993

SR-05 Acquisition Strategies, Tools, and Methods 995
SR-06 Supplier Assessments and Reviews 997
SR-08 Notification Agreements 999
SR-09 Tamper Resistance and Detection 1001
SR-09(01) Multiple Stages of System Development Life Cycle 1003
SR-10 Inspection of Systems or Components 1004
SR-11 Component Authenticity 1006
SR-11(01) Anti-Counterfeit Training 1008
SR-11(02) Configuration Control for Component Service and Repair . 1009
SR-12 Component Disposal 1010