ISF-02-024

**TxDOT Security Questionnaire (TSQ)**

***Instructions*** — Respondent/Vendor must complete Section 1 — General Information and Section 2 — Low, Moderate, and High Baseline Questions. Additionally, Section 3 — Moderate and High Baselines and Section 4 — Privacy Overlay must be completed **if indicated in the solicitation or contract** and left blank otherwise. Read all instructions in each section to determine applicability and specific requirements. In Sections 2, 3, and 4, responses of “No” indicate non-compliance with TxDOT cybersecurity and privacy requirements. Answer “Yes” only if Respondent/Vendor is currently in compliance or will be in compliance and verified as such prior to the start-date of the contract applicable to this review. For any “No” response in these sections, provide an overview of the remediation plan to comply with requirements, including an estimated timeline and completion date.

***Document Data Classification*** — This document, when filled out, contains sensitive vulnerability information, and is considered an assessment of the extent to which a Respondent/Vendor is vulnerable to unauthorized access or harm, and the extent to which TxDOT’s or contractors’ electronically stored information containing sensitive or critical information is vulnerable to alteration, damage, erasure, inappropriate use, or disclosure.

***Document Delivery*** — This document must be delivered in a secure manner to TxDOT and will be protected by TxDOT as a Confidential document. To request support or additional guidance, please contact, via email, the Procurement Official or Contract Manager noted in the solicitation or contract.

***Document Usage*** — This document will be used by TxDOT to evaluate whether the Respondent/Vendor meets security requirements to be considered for contract award or renewal. This document is not intended to replace any other TxDOT or independent security assessments. The document and information contained within will be provided only to the minimum personnel required to accomplish the usage stated above and will be stored and transmitted in a secure manner at all times.

# Section 1 — General Information

This section is for information purposes; however, the Respondent/Vendor must complete this section. Respondent/Vendor’s failure to complete this section will result in the response being considered non-responsive. Respondent/Vendor’s failure to complete this section may be cause for discontinuance of the work and termination of the contract. A “No” or “N/A” does not disqualify the Respondent/Vendor.

| **ID** | **Question** | **Response** |
| --- | --- | --- |
| 1.1 | What is the Respondent’s/Vendor’s legal entity name?  | Click or tap here to enter text. |
| Comments: Click or tap here to enter text.  |
| 1.2 | What is the legal entity’s Tax Identification Number (TIN)? | Click or tap here to enter text. |
| Comments: Click or tap here to enter text. |
| 1.3 | What is the solicitation/contract number associated with this solicitation response? | Click or tap here to enter text. |
| Comments: Click or tap here to enter text. |
| 1.4 | What is the Respondent’s/Vendor’s address (Street, City, State, Zip)? | Street: Click or tap here to enter text.City: Click or tap here to enter text.State: Click or tap here to enter text.Zip Code: Click or tap here to enter text. |
| Comments: Click or tap here to enter text. |
| 1.5 | Who can be contacted regarding this questionnaire? Please provide name, title, telephone number, and email address. | Name: Click or tap here to enter text.Title: Click or tap here to enter text.Telephone Number: Click or tap here to enter text.Email Address: Click or tap here to enter text. |
| Comments: Click or tap here to enter text. |
| 1.6 | What is the TxDOT Security Baseline of the TxDOT data accessed, transmitted, used, or stored by the Respondent/Vendor? *The Security Baseline is documented in the solicitation details or the existing contract.* | [ ]  Low[ ]  Moderate[ ]  High |
| Comments: Click or tap here to enter text. |
| 1.7 | Which of the following TxDOT Security Overlays apply to the TxDOT Data accessed, transmitted, used, or stored by the Respondent/Vendor? Select all that apply. *The Security Overlays are documented in the solicitation details or the existing contract.*  | [ ]  N/A[ ]  Sensitive[ ]  Privacy[x]  Payment Card Industry (PCI)[ ]  Criminal Justice Information Services (CJIS) |
| Comments: Click or tap here to enter text. |
| 1.8 | What is the TxDOT data classification of the TxDOT data accessed, transmitted, used, or stored by the Respondent/Vendor? *The data classification is documented in the solicitation details or the existing contract.* | [ ]  Public[ ]  Sensitive[ ]  Confidential[ ]  Regulated |
| Comments: Click or tap here to enter text. |
| 1.9 | If Respondent/Vendor is providing TxDOT Cloud Computing services, what level of TX-RAMP are the services required to meet?  | [ ]  TX-RAMP Level 1[ ]  TX-RAMP Level 2[ ]  N/A |
| Comments: Click or tap here to enter text. |
| 1.10 | How many Respondent/Vendor employees and subcontractors (across all Respondent/Vendor offices and locations) will have access to TxDOT data? | Click or tap here to enter text. |
| Comments: Click or tap here to enter text. |
| 1.11 | What is the name of the Respondent’s/Vendor’s Information Technology Security Official (or equivalent)? | Click or tap here to enter text. |
| Comments: Click or tap here to enter text. |
| 1.12 | Which country (or countries) will the Respondent/Vendor be accessing, transmitting, using, or storing TxDOT data? List all applicable countries in the Comments box. |  |
| Comments: Click or tap here to enter text. |
| 1.13 | Has the Respondent/Vendor (including subcontractors) experienced any cybersecurity breaches in the past year that compromised the information processed, stored, or managed through the type of engagement being provided? If yes, provide details. | [ ]  Yes – provide details in the Comments box[ ]  No |
| Comments: Click or tap here to enter text. |

# Section 2 — Low, Moderate, and High Baseline Questions

Respondent/Vendor must complete this section. Respondent’s failure to complete this section will result in the response being considered non-responsive. Vendor’s failure to complete this section may be cause for discontinuance of the work and termination of the contract. For “No” responses, Respondent/Vendor must provide remediation plan details, including timelines, as well as additional details in the Comments box to describe the cause for the “No” and any compensating controls or mitigating factors. This section is reviewed for completeness and evaluated based on responses provided.

Each TxDOT Control referenced at the end of each question is available to view in the TxDOT *Information Security and Privacy Controls Standard Catalog* available on the [TxDOT Cybersecurity Resources](https://www.txdot.gov/about/contact-us/cybersecurity/cybersecurity-resources.html) page.

| **ID** | **Question** | **Response** |
| --- | --- | --- |
| 2.1 | Does the Respondent/Vendor have a function/branch/division/office/program within the organization responsible for cybersecurity? (TxDOT Control PM-01) | [ ]  Yes[ ]  No |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text. |
| 2.2 | Are Respondent/Vendor information security roles and responsibilities defined and documented? (TxDOT Control PL-01) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text. |
| 2.3 | Is a risk assessment program in place to periodically review the Respondent/Vendor’s solution and identify threats and vulnerabilities? (TxDOT Control RA-03) | [ ]  Yes[ ]  No |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.4 | Is the Respondent/Vendor’s solution, including its components (servers, databases, web applications, etc.), patched in a timely manner as patches become available? (TxDOT Control SI-02) | [ ]  Yes[ ]  No |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.5 | Will all Respondent/Vendor personnel be required to sign an agreement (Data Use Agreement, Acceptable Use Agreement, Rules of Behavior form, or similar document)? (TxDOT Control PS-06) | [ ]  Yes[ ]  No |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.6 | Are Respondent/Vendor accounts approved prior to provisioning, reviewed periodically, and disabled when no longer necessary or the employee is terminated? (TxDOT Control AC-02) | [ ]  Yes[ ]  No |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.7 | Are Respondent/Vendor users assigned a unique username or unique identifier? (TxDOT Control IA-02) | [ ]  Yes[ ]  No |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.8 | Are Respondent/Vendor inactive accounts disabled after a defined period of inactivity? [TxDOT Control AC-02(03)] | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.9 | Are Respondent/Vendor accounts automatically locked after a number of incorrect login attempts? (TxDOT Control AC-07) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.10 | Are Respondent/Vendor passwords required to be sufficiently strong, are default passwords required to change after first use? If two-factor authentication is not used, are passwords set to automatically expire after a period of time? [TxDOT Control IA-05(01)] | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.11 | Are Respondent/Vendor account actions (for example, user logins, failed login attempts, add/modify/remove user accounts/permissions, configuration changes, etc.) logged? (TxDOT Control AU-12) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.12 | If any TxDOT information is published publicly, is it reviewed by an authorized individual prior to publication? (TxDOT Control AC-22) | [ ]  Yes[ ]  No [ ]  N/A |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.13 | Does a process exist to evaluate proposed changes for security risks before they are applied to IT assets? (Examples of IT assets include but are not limited to information systems, applications, servers, databases, operating systems, network devices, etc.) (TxDOT Control CM-04) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.14 | Is system data (including TxDOT data) backed up periodically? (TxDOT Control CP-09) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.15 | Is the solution monitored to detect potential attacks and initiate further analysis, investigation, and reporting? (TxDOT Control SI-04) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.16 | Are anti-virus or malware products deployed and monitored? (TxDOT Control SI-03) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.17 | Does a records retention policy exist to ensure solution outputs are retained for an appropriate amount of time? (TxDOT Control SI-12) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.18 | Is there an individual responsible for cybersecurity within the Respondent’s/Vendor’s organization? (TxDOT Control PM-02) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.19 | Are processes in place to ensure compliance with applicable information security legislative, regulatory, and contractual requirements? (TxDOT Control PM-01) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.20 | Does Respondent/Vendor ensure that subcontractors abide by all the same terms and conditions that Respondent/Vendor agrees to regarding TxDOT data? (TxDOT Control SA-09)  | [ ]  Yes[ ]  No [ ]  N/A |
| If No or N/A, please provide explanation, plans to remediate, and any compensating controls or mitigating factors. Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.21 | Is a vulnerability management process in place to monitor vulnerabilities and ensure appropriate remediation in a timely manner? (TxDOT Control RA-05) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.22 | Is an incident notification policy in place to notify TxDOT of a cybersecurity incident potentially involving TxDOT data? (TxDOT Control IR-08) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.23 | Is a cybersecurity training and awareness program in place to increase awareness of cybersecurity and privacy threats and best practices? (TxDOT Control AT-02) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.24 | Is the Respondent/Vendor providing TxDOT a cloud computing service certified through the Texas Risk and Authorization Management Program (TX-RAMP)? (TxDOT Control SA-04)If service is DIR TX-RAMP Certified, select Yes* TX-RAMP Level 1 (N/A if awarded/renewed before January 1, 2024)
* TX-RAMP Level 2

If service has a TX-RAMP Provisional Certification, select No – TX-RAMP Provisional Certification. Further approval by the TxDOT Information Security will be required.If service is not TX-RAMP Certified, Select NoIf service does not require TX-RAMP Certification, select N/A | [ ]  Yes – DIR TX-RAMP Certified [ ]  No – TX-RAMP ProvisionalCertification[ ]  No[ ]  N/A |
| If Yes, please provide the TX-RAMP Certification Number. If No or N/A, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 2.25 | Does the Respondent/Vendor’s solution AVOID using services, software, equipment, or systems that (a) are provided or manufactured by or (b) have components provided or manufactured by any entity determined to be a Prohibited Technology by the Texas Department of Information Resources? See [Prohibited Technologies list](https://ftp.txdot.gov/pub/txdot/itd/cybersecurity/prohibited-technologies-list-cybersecurity.pdf). (TxDOT Control SR-06) | [ ]  Yes[ ]  No |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text. |

# Section 3 — Moderate and High Baselines

This section is required for Respondents/Vendors with Security Baselines of Moderate or High. Respondents/Vendors with Low Security Baselines are not required to complete this section and may leave the section blank. If the Security Baseline is Moderate or High, this section is reviewed for completeness and evaluated based on provided responses. For “No” responses, provide remediation plan details, including timelines, as well as additional details to describe the cause for the “No” as well as any compensating controls or mitigating factors.

| **ID** | **Question** | **Response** |
| --- | --- | --- |
| 3.1 | Are information security policies communicated to affected constituents (full- and part-time employees, contractors, and temporary employees) at time of hire and at least annually thereafter? (TxDOT Control PM-01) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.2 | Are exceptions to policy escalated to appropriate individuals based on the level of risk associated with the policy exception and the authority delegated to the individual making the decision? (TxDOT Control PM-01) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.3 | Does a Respondent/Vendor have a policy or similar publication that considers TxDOT’s data classification requirements and is the publication reviewed and reaffirmed on annual basis, and communicated to affected stakeholders at least annually? [TxDOT Control PM-05(01)] | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.4 | Does a threat awareness capability exist for sharing threat information with TxDOT in the case of a suspected cybersecurity incident? (TxDOT Controls PM-16) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.5 | Does the Respondent/Vendor have documentation that describes how the proposed solution that would access, transmit, use, or store TxDOT data complies with the applicable security and privacy requirements? (TxDOT Control PL-02) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.6 | As cybersecurity deficiencies are identified, are remediation plans developed, updated as needed, and reviewed/validated prior to resolution/closure? (TxDOT Control CA-05) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.7 | Does a policy related to security awareness training / education exist and is the policy reviewed and reaffirmed on annual basis, and communicated to affected stakeholders at least annually? (TxDOT Control AT-01) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.8 | Does the Respondent/Vendor maintain a dedicated staff to manage physical security where TxDOT data is accessed, transmitted, used, or stored? (TxDOT Control PE-01) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.9 | Do Respondent/Vendor accounts that access TxDOT data allow only the minimum level of access needed to accomplish assigned organizational tasks? (TxDOT Control AC-03) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.10 | Do all system actions require authentication to a user account? (TxDOT Control AC-14) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.11 | If remote or external access is allowed, is it permitted only to the minimum necessary and approved prior to providing access? (TxDOT Control AC-17) | [ ]  Yes[ ]  No [ ]  N/A |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.12 | If mobile devices are used to access, transmit, use, or store TxDOT data, are they properly configured and authorized to operate. (TxDOT Control AC-19) | [ ]  Yes[ ]  No [ ]  N/A |
| If No or N/A, please provide explanation, plans to remediate, and any compensating controls or mitigating factors. Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.13 | Does a password management policy exist and is it reviewed, updated, and reaffirmed on at least an annual basis, and communicated to affected stakeholders at least annually? (TxDOT Control IA-01) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.14 | Are Respondent-/Vendor-controlled configuration settings enabled to provide only what is needed for the solution to function? (TxDOT Control CM-06) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.15 | If present within the Respondent/Vendor solution, is TxDOT sensitive, confidential, and regulated data encrypted at rest and in transit? (TxDOT Control SC-13) | [ ]  Yes[ ]  No [ ]  N/A |
| If No or N/A, please provide explanation, plans to remediate, and any compensating controls or mitigating factors. Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.16 | Are changes to the Respondent/Vendor solution analyzed for cybersecurity impacts in a test environment prior to implementation in a production environment? [TxDOT Control CM-04(01)] | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.17 | Is a network diagram or component inventory (list of components for the solution) documented? (TxDOT Control CM-08) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.18 | Are vulnerability scans performed on Respondent-/Vendor-controlled internal- and external- facing networks at least once a month? (TxDOT Control RA-05) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.19 | Is an information security risk assessment performed at least annually by appropriately skilled individuals or teams? (TxDOT Control RA-03) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.20 | Are external or internal security-related audits performed to identify risks from all significant information security threats at least annually? (TxDOT Control RA-03) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.21 | Is there an internal audit, risk management, or compliance department with responsibility for identifying and tracking resolution of information security issues and audit findings? (TxDOT Control RA-07) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.22 | Are the logs of critical infrastructure assets such as firewalls, routers, wireless access points, and authentication servers reviewed for unauthorized traffic? (TxDOT Control AU-06) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.23 | Is a business continuity plan, contingency plan, disaster recovery plan, or similar document in place for Respondent/Vendor solutions that access, transmit, use or store TxDOT data that ensures appropriate confidentiality, integrity, and availability of the TxDOT data during a contingency? (TxDOT Control CP-02) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text. |
| 3.24 | Is a business continuity plan, contingency plan, disaster recovery plan, or similar document for solutions that access, transmit, use or store TxDOT data tested on a recurring basis and updated as deficiencies are identified? (TxDOT Control CP-04) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.25 | Are incident response capabilities tested periodically and updated as deficiencies are identified? (TxDOT Control IR-03) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.26 | Can TxDOT data be recovered from backup or recreated in a timely manner? (TxDOT Control CP-10) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.27 | Is all TxDOT data stored within the Respondent/Vendors environment properly sanitized or destroyed when required by the contract? (TxDOT Control MP-06) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.28 | Do all personnel with access to TxDOT data undergo background screenings prior to authorizing access to TxDOT data? (TxDOT Control PS-03)  | [ ]  Yes [ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.29 | Do privileged accounts (for example, administrator and management accounts) require at a minimum two-factor authentication (2FA)? [TxDOT Control IA-02(01)] | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.30 | Are penetration tests conducted prior to implementation and whenever there is a major change on internet websites that process TxDOT confidential or regulated information? (TxDOT Control CA-08) | [ ]  Yes[ ]  No[ ]  N/A |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.31 | Are penetration tests conducted prior to implementation and whenever there is a major change on mobile applications that process TxDOT confidential or regulated information? (TxDOT Control CA-08) | [ ]  Yes[ ]  No[ ]  N/A |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 3.32 | Will all access, transmittal, usage, or storage of TxDOT confidential information by the organization or subcontractors occur entirely within the United States? If no, list additional countries. (TxDOT Control PT-03) | [ ]  Yes[ ]  No[ ]  N/A |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |

# Section 4 — Privacy Overlay

This section is required for Respondents/Vendors with TxDOT Security Overlays containing Privacy. If Privacy has not been identified as an applicable TxDOT Security Overlay, Respondents/Vendors are not required to complete this section and may leave the section blank. If Respondent’s/Vendor’s Security Overlays contain Privacy, this section is reviewed for completeness and evaluated based on provided responses. If the Security Overlays do not contain Privacy, this section is not reviewed or evaluated. For “No” responses, provide remediation plan details, including timelines, as well as additional details to describe the cause for the “No” as well as any compensating controls or mitigating factors.

| **ID** | **Question** | **Response** |
| --- | --- | --- |
| 4.1 | Is there an individual in the organization responsible for privacy? If Yes, provide individual contact information. (TxDOT Control PT-01)Name: Click or tap here to enter text.Title: Click or tap here to enter text.Address (City, State, Zip): Click or tap here to enter text.Telephone Number: Click or tap here to enter text.Email Address: Click or tap here to enter text. | [ ]  Yes[ ]  No [x]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 4.2 | Does the organization have privacy policies that address the collection and use of personal information? (TxDOT Control PT-01) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 4.3 | Do procedures exist to notify data subjects whose target privacy data has been breached? (TxDOT Control IR-01) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 4.4 | Does the Respondent/Vendor provide the public with access to information about the privacy program and a way to engage the organization on privacy-related matters? (TxDOT Control PM-20) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 4.5 | Will the access, transmittal, usage, or storage of any TxDOT Personally Identifiable Information (PII) by the organization or subcontractors occur entirely within the United States? If no, list additional countries. (TxDOT Control PT-03) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 4.6 | Do procedures exist to communicate with TxDOT if questions, complaints, or requests to access, correct, and delete TxDOT privacy data are received from data subjects? (TxDOT Control PT-02) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 4.7 | Does the Respondent/Vendor (including subcontractors) restrict TxDOT Personally Identifiable Information (PII) data to the minimum necessary and receive explicit approval from TxDOT prior to use in testing, training, and research? (TxDOT Control PM-25) | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 4.8 | Is a privacy incident notification policy in place to notify TxDOT if privacy information is potentially lost or inappropriately accessed, used, or disclosed? [TxDOT Control IR-08(01)] | [ ]  Yes[ ]  No  |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 4.9 | Are penetrations tests conducted prior to implementation and whenever there is a major change on internet websites that process Texas sensitive personal information or personally identifiable information? (TxDOT Control CA-08) | [ ]  Yes[ ]  No[ ]  N/A |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |
| 4.10 | Are penetrations tests prior to implementation and whenever there is a major change on mobile applications that process Texas sensitive personal information or personally identifiable information? (TxDOT Control CA-08) | [ ]  Yes[ ]  No[ ]  N/A |
| If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. | Planned Remediation Date:Click or tap here to enter text.  |

**Signature and Submission**

I certify that all information provided in this TSQ is truthful and correct to the best of my knowledge. If I learn that any provided information is not correct, I agree to notify TxDOT immediately.

**Reminder**: Submit this completed, signed TSQ to the appropriate TxDOT Contract Manager(s) in a secure manner.

|  |  |
| --- | --- |
| **Name** | Click or tap here to enter text. |
| **Title** | Click or tap here to enter text. |
| **Email** | Click or tap here to enter text. |
| **Phone Number** | Click or tap here to enter text. |
| **Signature (digital signature preferred)** | **Date** |
|  | Click or tap here to enter text. |

**Appendix A: TSQ Response Aid**

As needed, use the additional guidance below to assist in completing the TSQ. To request support or additional guidance, please contact, via email, the Procurement Official or Contract Manager noted in the solicitation or contract.

| **Question ID** | **Response Guidance** |
| --- | --- |
| **1.1** | Provide the legal name of the business (the name used for legal purposes, like filing a federal or state tax form on behalf of the business, and not a trade or assumed name or “dba”). |
| **1.2** | Provide the legal tax identification number of the entity or applicant/bidder. |
| **1.3** | Provide the solicitation/contract number associated with this solicitation response. |
| **1.4** | Provide the address of the corporate or primary office of the business. |
| **1.5** | Provide the name, title, telephone number, and email address of Respondent/Vendor point of contact associated with this solicitation/contract. |
| **1.6** | Provide the appropriate security baseline of the TxDOT data accessed, transmitted, used, or stored by the Respondent/Vendor. The security baseline is documented in the solicitation details or the existing contract. This question’s response shall not differ from the determination noted in the solicitation or existing contract. Security baselines are applied to indicate potential impact to TxDOT if events occur which jeopardize the security (confidentiality, integrity, availability) of the system or information within the system. |
| **1.7** | Provide applicable TxDOT Security Overlays in accordance with TxDOT data types that are accessed, transmitted, used, or stored by the Respondent/Vendor. Security overlays, if any, are documented in the solicitation details or the existing contract. This question’s response shall not differ from the determination noted in the solicitation or existing contract. Security overlays are applied to tailor applicable security controls, requirements and guidance based on involved data types [Sensitive, Privacy, Payment Card Industry (PCI), and Criminal Justice Information (CJI)]. |
| **1.8** | Provide applicable data classification of the TxDOT data access, transmitted, used, or stored by the Respondent/Vendor. TxDOT’s [Data Classification Policy](https://ftp.txdot.gov/pub/txdot/itd/cybersecurity/data-classification-policy.pdf) is available on TxDOT.gov. The data classification is documented in the solicitation details or the existing contract. This question’s response shall not differ from the determination noted in the solicitation or existing contract. Data classification is applied to tailor applicable security controls, requirements, and guidance based on involved data classification types (Public, Sensitive, Confidential, Regulated). |
| **1.9** | Provide the appropriate applicable TX-RAMP level required for Respondent/Vendor cloud computing services that will access, transmit, use, or store TxDOT data.TX-RAMP Level 1 — Required for any Respondent/Vendor that will access, transmit, use, or store TxDOT Low Baseline data through use of cloud computing services. Certification Required by January 1, 2024.TX-RAMP Level 2 — Required for any Respondent/Vendor that will access, transmit, use, or store TxDOT Moderate Baseline data through use of cloud computing services. Certification Required by January 1, 2022.Select N/A if Respondent/Vendor is not using cloud computing services or is using cloud computing services that meet TX-RAMP characteristics and categories of cloud computing services not subject to TX-RAMP. See the [TX-RAMP Program Manual](https://dir.texas.gov/information-security/texas-risk-and-authorization-management-program-tx-ramp), Characteristics and Categories of Cloud Computing Services Not Subject to TX-RAMP.“Cloud Computing Service” refers to a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is referenced in Texas Government Code Title 10, Subtitle D, Chapter 2157, Subchapter A, Section 2157.007 and is defined in NIST 800-145.* Cloud services delivery methods: Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS).
* Cloud deployment models: Private, Community, Public, and Hybrid cloud deployments.
 |
| **1.10** | Provide the estimated number of employees and contractors that will have access to TxDOT data. |
| **1.11** | Provide the name and title of the individual responsible for maintaining the security of Respondent/Vendor solutions that will access, transmit, use, or store TxDOT data. This individual should be able to assist in answering any questions regarding responses to Sections 2 and 3. |
| **1.12** | Use the comments field to list the country (or countries) where the Respondent/Vendor will be accessing, transmitting, using, or storing TxDOT data. |
| **1.13** | Answer Yes if Respondent/Vendor has experienced a cybersecurity breach within the past year involving the information system, data, and services related to this engagement. Breaches include incidents that may include but are not limited to privacy breach, loss, theft, unauthorized access, malware infections, and occurrences of negligence, human error, or malicious acts. If Yes, as authorized, please provide details to include severity, dates/timelines, root cause, corrective actions, etc. |
| **2.1** | Answer Yes if Respondent/Vendor identifies an area of the business to handle cybersecurity initiatives that works to ensure the availability, integrity, authentication, confidentiality, and nonrepudiation of systems, data, and users. |
| **2.2** | Answer Yes if Respondent/Vendor has written policies in place that define common information security roles and responsibilities such as user roles (information owner, information custodian, information users), specific roles (Privacy Officer), management and senior leadership (Chief Information Officer, Chief Information Security Officer).  |
| **2.3** | Answer Yes if Respondent/Vendor has a risk assessment program in place to assess and evaluate risk within information resources and technology resulting from threats and vulnerabilities. |
| **2.4** | Answer Yes if Respondent/Vendor has implemented patch management processes that involve ongoing identification, testing, distribution, and installation of service packs/patches to the information system and its various components (servers, databases, web applications, etc.). |
| **2.5** | Answer Yes if Respondent/Vendor has written policies or acceptable use agreements requiring employees and subcontractors to review and sign for compliance. Acceptable use agreements refer to agreements between a data provider and a data recipient, communicating terms under which the data can be used, and further communicates system and data handling requirements and best practices. |
| **2.6** | Answer Yes if Respondent/Vendor has account provisioning, monitoring, control, and deprovisioning processes in place to ensure access to computing systems that access, transmit, use, or store TxDOT data, is limited to authorized personnel. |
| **2.7** | Answer Yes if Respondent/Vendor establishes a unique username to represent the identity of each of its employees, subcontractors, and any other persons under Respondent/Vendor direct control who will access, transmit, use, or store TxDOT data. Examples may involve a name, a code, serial numbers, and random numbers (for example, an account or directory ID, Media Access Control Address, bar codes, card numbers). |
| **2.8** | Answer Yes if Respondent/Vendor has account management processes in place to prompt notification to a responsible resource to review and disable user accounts after defined periods of inactivity. |
| **2.9** | Answer Yes if Respondent/Vendor has account management processes in place to automatically disable/lock user accounts after a certain number of failed login attempts. |
| **2.10** | Answer Yes if Respondent/Vendor has implemented a system for changing the password initially assigned to new users (also known as default passwords) and requires users to change their passwords after a period of time and prohibits the creation of weak passwords for all systems that access or store TxDOT. |
| **2.11** | Answer Yes if Respondent/Vendor information systems with TxDOT data log various user actions to identify unauthorized actions and suspicious behavior. |
| **2.12** | Answer Yes if Respondent/Vendor publishes various information publicly (that is, a public website) and has mechanisms/processes in place to ensure content for release is considered appropriate for public consumption. |
| **2.13** | Answer Yes if Respondent/Vendor has change management processes in place involving developing, testing, validating, and documenting changes before authorized implementation of changes to IT assets (information systems, applications, servers, databases, operating systems, network devices, etc.). Best practices for implementing changes to IT assets include initial deployment within a test environment, functionality and security testing, and approval prior to implementation to a production environment. |
| **2.14** | Answer Yes if Respondent/Vendor performs backups of its of IT assets (information systems, applications, servers, databases, operating systems, network devices, etc.) that access, transmit, use, or store TxDOT data. If Yes, the Respondent/Vendor must also perform backups of TxDOT data. Backups enable the recovery of data, information systems and involved components, in the event of loss or damage (natural disasters, system disk and other systems failures, intentional or unintentional human acts, data entry errors, or systems operator errors). |
| **2.15** | Answer Yes if Respondent/Vendor-involved computing systems are monitored for operation and performance, detecting and alerting upon possible adverse or malicious activity. 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. Alerts are to be analyzed and reported to Respondent/Vendor security personnel for investigation, identifying recourse and follow-up as needed. |
| **2.16** | Answer Yes if Respondent/Vendor-involved computing systems that access, transmit, use, or store TxDOT data contain up-to-date anti-malware and antivirus protection. Malicious code includes viruses, worms, trojan horses and spyware. Malicious code can be inserted into systems in a variety of ways, including by electronic mail, the internet, and through portable storage devices. |
| **2.17** | Answer Yes if Respondent/Vendor manages and retains log information of activity within the system and of communications to other systems in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. |
| **2.18** | Answer Yes if Respondent/Vendor appoints a senior security resource with the mission and resources to protect TxDOT systems and data by preventing, detecting, and responding to cyber events. |
| **2.19** | Answer Yes if Respondent/Vendor has program management processes or plans in place (Information Security Program Plan or similar) to ensure that the Respondent/Vendor organization and its operations are in compliance with applicable information security legislative, regulatory, and contractual requirements. Events that may prompt an update in processes to maintain security legislative, regulatory, and contractual requirement currency may include, but are not limited to, organization-wide assessment or audit findings, security incidents or breaches, changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. |
| **2.20** | Answer Yes if Respondent/Vendor will require that subcontractors who will access, transmit, use, or store TxDOT data, comply with security and privacy requirements as defined by TxDOT, for example: contract requirements, applied Information Security and Privacy Controls Baseline Standards, Service Level Agreements (SLAs).  |
| **2.21** | Answer Yes if Respondent/Vendor scans and monitors its computing systems with vulnerability scanning and monitoring tools, identifying vulnerabilities potentially affecting the system. Vulnerabilities are to be reported and remediated in a prioritized and timely manner according to criticality and risk. |
| **2.22** | Answer Yes if Respondent/Vendor has, or will have, written policies and procedures requiring the respondent/vendor to notify TxDOT of a cybersecurity incident potentially involving TxDOT data. Cybersecurity incidents may limit or compromise the availability, integrity, authentication, confidentiality, and nonrepudiation of systems, data, and users. Cybersecurity incidents may include, but are not limited to malware, phishing, denial-of-service, unauthorized attempts to access systems or data, privilege escalation, and advanced persistent threats.  |
| **2.23** | Answer Yes if Respondent/Vendor maintains a formalized Cybersecurity Awareness and Training Program, requiring training of Respondent/Vendor constituents with access to TxDOT data on matters related to confidentiality, privacy, and security, stressing the importance of promptly reporting any event or breach. Awareness and training programs should be required. Programs should track employees for completion and identify those who failed to complete the training.  |
| **2.24** | Respondent/Vendor may not enter or renew a contract with TxDOT until TX-RAMP Certification or Provisional Status achieved. All cloud computing services will require TX-RAMP certification or provisional status prior to award/renewal — there are no waivers. Respondent/Vendor must engage Texas Department of Information Resources (DIR) to start the TX-RAMP certification process .Answer “Yes – DIR TX-RAMP Certified” if Respondent/Vendor cloud computing systems that access, transmit, use, or store TxDOT data have an approved DIR TX-RAMP certification as result of completed DIR TX-RAMP assessment and certification of award from DIR. * Respondent/Vendor must comply with the requirements of the TX-RAMP program and maintain program compliance and certification through the term of the contract via TX-RAMP Level 1 or Level 2 Certification, or provisional status.

Answer “No – Provisional” if Respondent/Vendor is not TX-RAMP certified but has been granted TX-RAMP Provisional Certification status.Answer “No” if Respondent/Vendor is providing TxDOT a service through a Cloud Computer Service that is not TX-RAMP certified or does not currently have TX-RAMP Provisional Status.Answer “N/A” if Respondent/Vendor is providing TxDOT a service that either does not involve cloud computing services or meets exclusionary criteria for TX-RAMP requirements per the DIR TX-RAMP Program Manual. |
| **2.25** | Answer Yes if the Respondent/Vendor’s solution does not use services, software, equipment, or systems that (a) are provided or manufactured by or (b) have components provided or manufactured by any entity determined to be a Prohibited Technology by the Texas Department of Information Resources? <https://ftp.txdot.gov/pub/txdot/itd/cybersecurity/prohibited-technologies-list-cybersecurity.pdf>  |
| **3.1** | Answer Yes if Respondent/Vendor has written information security policies in place, communicating required security and best practices, that are shared for review and compliance at time of hire, and at least annually by all involved resources. |
| **3.2** | Answer Yes if Respondent/Vendor has policy exception processes in place, where an authorized individual is given management approval to allow individuals to operate outside of normal conditions and requirements as communicated through policy. Management’s review of the exception request should consider the risk associated with the exception. |
| **3.3** | Answer Yes if Respondent/Vendor has a written policy or similar document that includes a reference to applicable TxDOT data classifications that is reviewed at least annually and shared with affected stakeholders, communicating the organization’s plan used to categorize information systems and data applying security protections based on sensitivity levels to the business. Refer to the TxDOT Data Classification Policy located on the [TxDOT Cybersecurity Resources](https://www.txdot.gov/about/contact-us/cybersecurity/cybersecurity-resources.html) page for more information. |
| **3.4** | Answer Yes if Respondent/Vendor has notification capability and processes in place to inform TxDOT of suspected cybersecurity incidents that may impact TxDOT systems, data, and users. |
| **3.5** | Answer Yes if Respondent/Vendor has documentation, such as a System Security Plan (SSP), that details the responsibilities and implementations of various security and privacy requirements (for example, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security and privacy controls). |
| **3.6** | Answer Yes if Respondent/Vendor documents and tracks planned remedial actions to address system weaknesses and deficiencies found during system scans (update, malware, vulnerability, configuration, audit) or other assessments. |
| **3.7** | Answer Yes if Respondent/Vendor has a written security awareness and training policy or related general security policy that is reviewed and approved at least annually and shared with affected stakeholders, communicating the organization’s implementation of its security awareness program, training, and training requirements. |
| **3.8** | Answer Yes if Respondent/Vendor employs full-time staff with the responsibility to manage physical and environmental protections (for example, fences, gates, locks, CCTV, surveillance cameras, data center utilities and tools, access cards) applied to protect systems and data involved with TxDOT systems, data, and users.  |
| **3.9** | Answer Yes if Respondent/Vendor provides system users with the lowest and least levels of access permissions required to perform business responsibilities. These practices are commonly referred to as least privilege, or least function.  |
| **3.10** | Answer Yes if Respondent/Vendor verifies the identity of a user, process, or device, before allowing access to information systems and resources that involve TxDOT systems and data. |
| **3.11** | Answer Yes if Respondent/Vendor remote workforce accesses organizational systems and resources securely (for example, VPN) and are provided limited access based on applicable user roles, responsibilities, and related user profiles. |
| **3.12** | Answer Yes if Respondent/Vendor authorizes the use of mobile devices, and applies necessary configurations for system administration and management, prior to delivering services and performing functions that involve creating, accessing, transmitting, using, or storing TxDOT data. |
| **3.13** | Answer Yes if Respondent/Vendor has a written password management policy that is reviewed at least annually and shared with affected stakeholders, communicating password guidance and requirements (for example, resetting default passwords, complexity requirements, password management). |
| **3.14** | Answer Yes if Respondent/Vendor-involved system (hardware, software, or firmware components) are configured to operate within only necessary operating parameters, ensuring optimal functionality while minimizing impact to the security of the system. |
| **3.15** | Answer Yes if Respondent/Vendor encrypts information while the information is at rest (not actively moving between data systems or stores) and in transit (actively moving between data systems and stores).  |
| **3.16** | Answer Yes if Respondent/Vendor has change management processes in place requiring that changes to IT assets be developed, tested, and validated within a test environment, tested for any issues or potential vulnerabilities introduced by the change to be addressed, and approved prior to implementation/deployment to production environment and systems. |
| **3.17** | Answer Yes if Respondent/Vendor develops, documents, and maintains accurate, current information system and component inventories (hardware, software, firmware). Inventory information is effective for maintaining accountability of systems and related components. |
| **3.18** | Answer Yes if Respondent/Vendor performs/facilitates ongoing and periodic vulnerability assessment of security defenses, including regularly scheduled vulnerability scans and at least one penetration test annually. Vulnerability assessment activities test and evaluate security controls and security defenses to ensure that required security posture levels are met. |
| **3.19** | Answer Yes if Respondent/Vendor performs/facilitates risk assessments at least annually to identify security and privacy weaknesses in information systems which may interact with TxDOT information systems and data. |
| **3.20** | Answer Yes if Respondent/Vendor performs/facilitates internal or external audits upon all significant information security threats that may impact systems that access, transmit, use, or store TxDOT data. Audit processes involve internal or independent review and examination of records and activities to assess the efficiency of system security and privacy controls, while ensuring compliance with established policies and operational procedures. |
| **3.21** | Answer Yes if Respondent/Vendor can identify an area of the business who has the responsibility to respond to findings from security, privacy, and risk assessments, findings, continuous monitoring, as well as audits.  |
| **3.22** | Answer Yes if Respondent/Vendor reviews and analyzes various system audit records for indications of inappropriate or unusual activity. These activities may be part of a continuous monitoring program, intended to perform audit record review, analysis, and reporting across security- and privacy-related logging performed by systems involving TxDOT systems and data. |
| **3.23** | Answer Yes if Respondent/Vendor has developed contingency plans and processes (or similar documents) to restore computing systems and business processes in the event of a system failure/outage, compromise, or breach. |
| **3.24** | Answer Yes if Respondent/Vendor tests and updates developed contingency plans (or similar documents) recurring basis. 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. Contingency plans should be updated as a result of contingency plan test results or findings. |
| **3.25** | Answer Yes if Respondent/Vendor tests effectiveness of incident response capabilities of in-scope systems at least annually. Incident response testing includes ensuring various potentially suspicious behavior is monitored, identified, reported, investigated, and corrected as needed in a timely manner.  |
| **3.26** | Answer Yes if Respondent/Vendor has backup processes in place to recover or recreate data to a known point in time, in response to experienced disruption, compromise, or failure. |
| **3.27** | Answer Yes if Respondent/Vendor has media sanitization processes in place to properly remove TxDOT data from information from system media such that the information cannot be retrieved or reconstructed.  |
| **3.28** | Answer Yes if Respondent/Vendor has personnel screening processes in place to screen individuals prior to authorizing access to systems and data. 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.  |
| **3.29** | Answer Yes if Respondent/Vendor requires privileged accounts to use two or more different factors to authenticate to a system, gaining access to system resources and data. Factors include “something you know,” such as a password, “something you have,” such as an access card or Microsoft Authenticator token, and “something you are,” such as a fingerprint or iris scan. Requiring two separate passwords both fall into the “something you know” category and does not constitute MFA. A privileged account refers to a trusted/authorized user who performs security-relevant functions (creating users, removing users, modifying user permissions, modifying configuration settings, etc.) that ordinary users are not authorized to perform. |
| **3.30** | Answer Yes if the Respondent/Vendor conducts a penetration test on any internet website that processes TxDOT confidential or regulated data that is required prior to the website going live and whenever a major change on the website is done.  |
| **3.31** | Answer Yes if the Respondent/Vendor conducts a penetration test on any mobile application that processes TxDOT confidential or regulated data that is required prior to the website going live and whenever a major change on the mobile application is done.  |
| **3.32** | Answer Yes if the Respondent/Vendor and subcontractors will access, transmit, use, or store TxDOT Confidential data *only* within the United States. If No, list any additional countries in the comments field. |
| **4.1** | Answer Yes if Respondent/Vendor identifies an area of the business to handle privacy initiatives that work to ensure the availability, integrity, authentication, confidentiality, and nonrepudiation of TxDOT privacy data. This individual should be able to assist in answering any questions regarding responses to Section 4. |
| **4.2** | Answer Yes if Respondent/Vendor has written policies approved by management that define personal information such as Personal Identifiable Information (PII), Sensitive Personal Information (SPI), etc.  |
| **4.3** | Answer Yes if Respondent/Vendor have procedures in place to notify data subjects involved in a privacy data breach. |
| **4.4** | Answer Yes if Respondent/Vendor has publicly available privacy programs or process as well as points of contact to report on or inquire of privacy matters (processes, breaches, contact information, etc.). |
| **4.5** | Answer Yes if all TxDOT PII data accessed, transmitted, used, or stored, including data backups, will remain in the continental United States. Additional regulations may apply if privacy data navigates outside the United States. |
| **4.6** | Answer Yes if Respondent/Vendor has or will have procedures in place to notify TxDOT of any data subject inquiries pertaining to TxDOT privacy data.  |
| **4.7** | Answer Yes if Respondent/Vendor limits the access and use of TxDOT PII to the minimum extent necessary and requires approval prior to its use. |
| **4.8** | Answer Yes if Respondent/Vendor has, or will have, written policies and procedures requiring the Respondent/Vendor to notify TxDOT of a potential/suspected incident potentially involving TxDOT privacy data. |
| **4.9** | Answer Yes if the Respondent/Vendor conducts a penetration test on any internet website that processes Texas personally identifiable or sensitive personal data is required prior to the website going live and whenever a major change on the website is done.  |
| **4.10** | Answer Yes if the Respondent/Vendor conducts a penetration test on any mobile application that processes Texas personally identifiable or sensitive personal data is required prior to the website going live and whenever a major change on the mobile application is done.  |

**Recent Revisions**

|  |  |  |
| --- | --- | --- |
| Version | Date | Brief Description of Change |
| 2025.1 | 3/18/2025 | Updated questions 1.12 and 3.31 and reformatted form to align with current TxDOT brand standards. |
| 3 | 12/1/2023 | Updated to align with requirements issued TX-RAMP v3, including changing the guidance for question 2.24 to reflect that contractors must go to the Department of Information Resources to obtain TX-RAMP provisional or full certifications. Updated hyperlinks. |

See [Version History](https://txdot.sharepoint.com/%3Aw%3A/r/sites/division-itd/imd/is/InternalIS/Shared%20Documents/Everyone/Publications/05-Forms/ISF-02-024_TxDOTSecurityQuestionnaire/ISF-02-024_versionHistory.docx?d=wf0c32cc6948c441399257af1dcaa4dda&csf=1&web=1&e=OaV9op) for the complete list of changes in the TxDOT Security Questionnaire.