

|  |
| --- |
| ISF-02-024-1 |

**TxDOT Security Questionnaire (TSQ) for**

**National Electric Vehicle Infrastructure (NEVI)**

***Instructions*** — Respondent/Vendor must complete Section 1 — Security Questions, and Section 2 — General Information. Unless otherwise stated in the question’s instructions, responses of “No” in Section 1 indicate non-compliance with TxDOT cybersecurity 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 grant agreement applicable to this review. Unless otherwise stated in the question’s instructions, for any “No” response in Section 1, 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 the Respondent/Vendor’s 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 TxDOT\_NEVI@txdot.gov.

***Document Usage*** — This document will be used by TxDOT to evaluate whether the Respondent/Vendor meets security requirements to be considered for a grant. 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 — Security Questions**

Respondent/Vendor must complete this section. Respondent/Vendor’s failure to complete this section will be determined as non-responsive and therefore not eligible for the associated grant. Unless otherwise stated in the question’s instructions, for “No” responses, Respondent/Vendor must provide remediation plan details, including timelines, as well as additional details in the Comments field 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.

The TxDOT Controls that are referenced at the end of each question are 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) webpage. The NEVI Controls that are referenced at the end of each question are listed on the [Joint Office of Energy and Transportation](https://driveelectric.gov/cybersecurity-clauses) website.

| **ID** | | **Question** | **Response** |
| --- | --- | --- | --- |
| 1.1 | | Is a cybersecurity program in place that addresses Electric Vehicle Supply Equipment (EVSE) security and documents potential risks and protections throughout the life cycle of the EVSE? (TxDOT Control: RA-03, NEVI ID: CP1) | 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. |
| 1.2 | | Are Respondent/Vendor cybersecurity roles and responsibilities defined and documented within the Respondent/Vendor's cybersecurity program? (TxDOT Control: PL-01, NEVI ID: CP2) | 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. |
| 1.3 | | Are the Respondent/Vendor's processes automated for timely and consistent deployment of security patches across all NEVI funded systems? (TxDOT Control: SI-02, NEVI ID: CVUM2) | 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. |
| 1.4 | | Will the Respondent/Vendor ensure that Electric Vehicle Service Provider (EVSP) subcontractors adhere to the same cybersecurity protections as established for the Respondent/Vendor? (TxDOT Control: SA-09, NEVI ID: CP5) | 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. |
| 1.5 | | Is a formal vulnerability management process in place to monitor vulnerabilities and ensure appropriate remediation in a timely manner for NEVI funded systems? (TxDOT Control: RA-05, NEVI ID: CVUM1) | 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. |
| 1.6 | | Is an incident notification policy in place to notify TxDOT of potentially harmful cybersecurity incidents associated with NEVI funded systems? (e.g., incidents which may cause harm to TxDOT's reputation) (TxDOT Control: IR-08, NEVI ID: CP4) | 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. |
| 1.7 | | Is an incident notification policy in place that requires the immediate reporting of unexpected or unauthorized physical access to NEVI funded infrastructure? (e.g., incidents which may cause harm to TxDOT's reputation) (TxDOT Control: PE-01, NEVI ID: PS2) | 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. |
| 1.8 | | 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. |
| 1.9 | | Will the Respondent/Vendor ensure only standardized secure encryption protocols will be used in NEVI funded systems as listed in the National Security Agency’s (NSA) Commercial National Security Algorithm (CNSA) Suite? (TxDOT Control: SC-13, NEVI ID: SC1) | 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. |
| 1.10 | | Does the Respondent/Vendor have centralized capabilities to authenticate, authorize, log, and monitor administrative and user access to NEVI funded systems? (TxDOT Control: AU-06, NEVI ID: IC1) | 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. |
| 1.11 | | Is a business continuity plan, contingency plan, disaster recovery plan, or similar document in place for NEVI funded solutions? (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. |
| 1.12 | | 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 |
| If Yes, 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. |
| 1.13 | | Do all personnel that administer EVSP data undergo a background screening prior to being granted access to the EVSP data? (TxDOT Control: PS-03, NEVI ID: SC3) | 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. |
| 1.14 | | Does the Respondent/Vendor employ multifactor authentication for administrative personnel who access EVSP data systems (usage data)? (TxDOT Control: IA-02(01), NEVI ID: IC3) | 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. |
| 1.15 | | Does the Respondent/Vendor ensure all EVSP data resides in the United States throughout its life cycle? (TxDOT Control: PT-03, NEVI ID: SC3) | 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. |
| 1.16 | | Does the Respondent/Vendor limit personal data collection to data that is strictly necessary for purposes of EV charging and protect it throughout its life cycle? (TxDOT Control: PM-25, NEVI ID: AC-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. |
| 1.17 | Has the Respondent/Vendor obtained the required level of Payment Card Industry (PCI) certification for their customer payment portal? (PCI-DSS Requirements) | | 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 2 — 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 be determined as non-responsive and therefore not eligible for the associated grant.

| **ID** | **Question** | **Response** |
| --- | --- | --- |
| 2.1 | What is the Respondent’s/Vendor’s legal entity name? | Click or tap here to enter text. |
| 2.2 | 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. |
| 2.3 | What is the name of the Respondent’s/Vendor’s Information Technology Security Official (or equivalent)? | 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 Grant Administrator 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. | |
| **Business Street** | Click or tap here to enter text. | |
| **Business City** | Click or tap here to enter text. | |
| **Business State** | Click or tap here to enter text. | |
| **Business Zip** | Click or tap here to enter text. | |
| **Signature (Digital signature is required, paper copies will *not* be accepted.)** | | **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 TxDOT\_NEVI@txdot.gov.

| **Question ID** | **Response Guidance** |
| --- | --- |
| **1.1** | Answer “Yes” if Respondent/Vendor has a risk assessment program in place to assess and evaluate risk resulting from threats and vulnerabilities to NEVI funded resources and technology. |
| **1.2** | 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). |
| **1.3** | 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.). |
| **1.4** | Answer Yes if Respondent/Vendor will require EVSP subcontractors to implement the same cybersecurity protections as established for the Respondent/Vendor. |
| **1.5** | 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. |
| **1.6** | Answer Yes if Respondent/Vendor has, or will have, written policies and procedures requiring the respondent/vendor to notify TxDOT of a cybersecurity incident that could potentially cause harm to TxDOT’s reputation. 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. |
| **1.7** | Answer Yes if Respondent/Vendor has, or will have, written policies and procedures requiring the respondent/vendor to notify TxDOT of unexpected or unauthorized physical access to NEVI funded infrastructure that could potentially cause harm to TxDOT’s reputation. |
| **1.8** | 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> |
| **1.9** | Answer Yes if Respondent/Vendor will implement encryption algorithms to the level recommend by the NSA’s Commercial National Security Algorithm (CNSA) Suite. |
| **1.10** | 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. |
| **1.11** | 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. |
| **1.12** | 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. |
| **1.13** | 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. |
| **1.14** | Answer Yes if Respondent/Vendor requires to use two or more different factors of authentication for administrative personnel who access EVSP data systems. 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. |
| **1.15** | Answer Yes if all EVSP data accessed, transmitted, used, or stored, including data backups, will remain in the continental United States. |
| **1.16** | Answer Yes if Respondent/Vendor limits the access and use of PII to the minimum extent necessary and requires approval prior to its use. |
| **1.17** | Answer Yes if Respondent/Vendor has reviewed Payment Card Industry (PCI) requirements for their customer payment portal and currently meets all PCI certification requirements for that system. <https://www.pcisecuritystandards.org/> |
| **2.1** | 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”). |
| **2.2** | Provide the name, title, telephone number, and email address of Respondent/Vendor point of contact associated with this solicitation/contract. |
| **2.3** | Provide the name and title of the individual responsible for maintaining the security of the NEVI funded solutions. This individual should be able to assist in answering any questions regarding responses to Section 1. |

**Recent Revisions**

|  |  |  |
| --- | --- | --- |
| Version | Date | Brief Description of Change |
| 2024.1 | 8/5/2024 | Updated document for TxDOT Brand conformance and requested update in Publication Request Form by Anna Pauline McClean, TxDOT Information Security Policy Technical Writer. |

**For Internal Use Only**

|  |
| --- |
| Control Section Job (CSJ) |
|  |