Information Security Standard ISS-01-212

Title: TxDOT Information Security Risk and Authorization Management Program (IS-RAMP)

Effective Date: 2/1/2022

Date of Last Revision: N/A

Division of Primary Responsibility: TxDOT Information Security Office

Contents

1. Introduction

1.1 Purpose

The TxDOT Information Security Risk and Authorization Management Program (IS-RAMP) is a component of TxDOT's overarching Information Security Third-Party Risk Program and supports the goal of implementing an enterprise-wide security program within TxDOT by providing consistency in procedures and compliance levels for third parties authorized to create, access, transmit, use, or store TxDOT data.

IS-RAMP and its requirements are designed in accordance with Texas state laws and regulations, particularly the excerpts noted in the table below.

Applicable State Law	State Law Excerpt
Texas Government Code, Section 2054.138 – Security Controls for State Agency Data	Each 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.
Texas Government Code, Section 2054.0593 – Cloud Computing State Risk and Authorization Management Program	A state agency may not enter or renew a contract with a vendor to purchase cloud computing services for the agency that are subject to the state risk and authorization management program unless the vendor demonstrates compliance with program requirements. A state agency shall require a vendor contracting with the agency to provide cloud computing services for the agency that are subject to the state risk and authorization management program to maintain program compliance and certification throughout the term of the contract.
Title 1, Texas Administrative Code (TAC), Rule §202.24 – Agency Information Security Program	Each agency shall develop, document, and implement an agency-wide information security program, approved by the agency head under §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).

1.2 Scope

This document outlines steps to implement TxDOT IS-RAMP as required by TxDOT's Information Security and Privacy Controls Standards Catalog::

- CA-02, Control Assessments
- CA-06, Authorization
- SA-04, Acquisition Process
- SR-06, Supplier Assessments and Reviews

This document applies to all third parties authorized to create, access, transmit, use, or store TxDOT data.

1.3 Audience and Applicability

This document is intended for third parties and third-party representatives responsible for complying with TxDOT cybersecurity and privacy requirements, as well as TxDOT employees and contractors responsible for coordinating, managing, and monitoring third-party risk.

1.4 Organization of this Document

The remainder of this document is organized as follows:

- Section 2 provides guidance and security requirements relating to TxDOT IS-RAMP.
- Section 3 provides guidance for submitting documentation to TxDOT in a secure manner.
- Section 4 provides instruction to immediately notify TxDOT of a potential or confirmed cybersecurity or privacy incident potentially involving TxDOT data.
- Appendix A provides hyperlinks to applicable forms and references for additional guidance.

2. Guidance & Security Requirements

Before a third party is authorized to create, access, transmit, use, or store TxDOT data, the third party must provide evidence of compliance with TxDOT's cybersecurity and privacy requirements as documented in solicitation requirements or contractual agreements between the third party and TxDOT. A third party's cybersecurity and privacy requirements may vary depending on the Security Baseline and Security Overlay values noted in the solicitation details or existing contract. Security Baselines and Security Overlays are determined in accordance with the types of TxDOT data to be created, accessed, transmitted, used, or stored by the third party.

2.1 TxDOT Security Questionnaire Completion Requirements

For a TxDOT Security Questionnaire (TSQ) to be considered complete, the third party shall complete all required sections. Sections 1 and 2 are required for all third parties. Section 3 is required only if the third party's Security Baseline is determined to be Moderate or High. The table below indicates requirements for Sections 1-3 based on the Security Baseline noted in the solicitation or contract.

Security Baseline	TSQ Requirements Based on Security Baseline		
	Section 1	Section 2	Section 3
Low	X	X	
Moderate	X	X	X
High	X	X	X

Section 4 of the TSQ is required only if the Security Overlays noted in the solicitation or contract include Privacy. When a solicitation or contract notes the Privacy overlay, Section 4 is required in addition to Sections 1-3 as applicable based on the table above. The table below indicates requirements for Section 4 based on the Security Overlays noted in the solicitation or contract.

Security Overlay	TSQ Requirements Based on Security Overlays
	Section 4
Sensitive	
Privacy	X
PCI	
CJIS	

2.2 TxDOT Security Questionnaire Submission Frequency

TSQs shall be submitted at the cadence determined by the Security Baseline. The table below outlines the frequencies at which the TSQ shall be completed and submitted to TxDOT.

Security Baseline	TSQ Submission Frequency		
	Upon Solicitation Response	Upon Renewal*	Annually
Low	X	X	
Moderate	X		X
High	X		X

** TSQ required upon renewal if date of most recent TSQ exceeds six months from planned renewal date.*

The third party may receive data from TxDOT that originates from another regulatory or federal source that has additional assessment requirements beyond what is mentioned above. The third party must refer to its contractual agreement with TxDOT for any added requirements.

2.3 Cloud Computing Service Provider Requirements

Third parties providing cloud computing services to TxDOT must be authorized, or willing to become authorized, via the Department of Information Resources (DIR) Texas Risk and Authorization Management Program (TX-RAMP). See the TX-RAMP Program Manual for a further definition of "cloud computing services."

Third parties providing cloud computing services to TxDOT must achieve TX-RAMP certifications in accordance with the table below before TxDOT can award a new contract or renew an existing contract.

Security Baseline	Required TX-RAMP Certification	Effective Date
Low*	Level 1	1/1/2023
Moderate	Level 2	1/1/2022
High	Level 2	1/1/2022

** Exclusions apply – see TX-RAMP Program Manual.*

If a third party is unable to obtain TX-RAMP Level 1 or Level 2 prior to contract award or renewal, TxDOT may elect to sponsor a TX-RAMP Provisional Certification. The Provisional Certification requires:

- Evidence that a TX-RAMP certification request has been submitted to DIR
- TxDOT review of a third-party attestation report and
- Approvals from TxDOT Leadership.

Examples of third-party attestation reports include but are not limited to:

- Statement on Standards for Attestation Engagements no. 18 (SSAE18), Service Organization Control 2 (SOC II) report
- Cloud Security Alliance (CSA) Security, Trust, Assurance and Risk (STAR) Level 2 certification
- International Organization for Standardization (ISO) 27001:2013 certification

If TxDOT approves sponsorship of a TX-RAMP Provisional Certification, Texas DIR must also review and approve or disapprove. If fully approved, a TX-RAMP Provisional Certification expires after 18 months and requires TX-RAMP Level 1 or Level 2 certification thereafter. Contact a TxDOT Procurement Official or Contract Manager for additional information regarding sponsorship of a TX-RAMP Provisional Certification.

Security Baseline	TX-RAMP Certification Level Requirement	
	Level 1	Level 2
Low	X	
Moderate		X
High		X*

** Additional requirements may apply.*

3. Submitting Documentation

All information security documentation concerning TxDOT data is classified as confidential. Documentation shall be submitted in a manner compliant with TxDOT cybersecurity controls SC-08, Transmission of Confidential Data, and SC-28, Protection of Data at Rest. Third parties shall contact the TxDOT point of contact noted in the solicitation or contract for additional guidance related to submitting documentation to TxDOT.

4. Reporting Breaches or Potential Incidents

In the event TxDOT data is compromised or potentially compromised, third parties must immediately notify TxDOT via the Report Cybersecurity Incident form on TxDOT.gov.

"Breach" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Texas Business & Commerce. Code §521.053

"Potential Cybersecurity Incident" means an event which may result in the accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information or information resources. Title 1, TAC 202.1(40)

Appendix A: Additional Guidance

See TxDOT's cybersecurity resources page for forms, templates, and guidance applicable to IS-RAMP, such as the TxDOT Security Questionnaire, TxDOT Data Classification Policy, and the TxDOT Information Security and Privacy Controls Standards Catalog.

See DIR's TX-RAMP site for the TX-RAMP Program Manual and additional guidance and resources, such as the vendor request form.