Information Security Updates

2023 PEPS Conference

Peter Lee

Information Security Officer – Risk Management

December 6, 2023

Presentation Topics

1. TX-RAMP Program Manual v3 and IS-RAMP changes
2. Main Threats to TxDOT
3. Best Defenses
4. Resources
5. Questions

TX-RAMP – Quick Overview In Case You Haven’t Had the Joy

Texas' 87th Legislature passed SB475 mandating DIR establish a certification program for cloud based services (IaaS, PaaS, SaaS) provided to TxDOT – Does not happen in PEPS contracts often

Levels based on data

Some types of “low-impact” SaaS excluded

Certification required prior to signing a new contract or a renewal

- Level 1 required as of 1/1/2024 (originally 1/1/2023)
- Level 2 required immediately

TX-RAMP does not require the same level of effort as StateRAMP or FedRAMP!

- No 3PAO requirement; SOC2 Type 2 covers most of the requirements
- Orgs with Fed/StateRAMP can get TX-RAMP easily

TX-RAMP – What's new in v3

3rd version of the Program Manual is published, effective date 12/1/2023

Levels based on impact

- "Low Impact" systems require Level 1
- "Moderate/High Impact" require Level 2 – Generally these are systems with Confidential data or that have Life/Death implications

BUT – Agencies can make certain types of systems out of scope for TX-RAMP

- Low Impact + No Confidential Data = No TX-RAMP
- Moderate Impact + meets criteria = No TX-RAMP

TX-RAMP & TxDOT IS-RAMP – What It Means For You

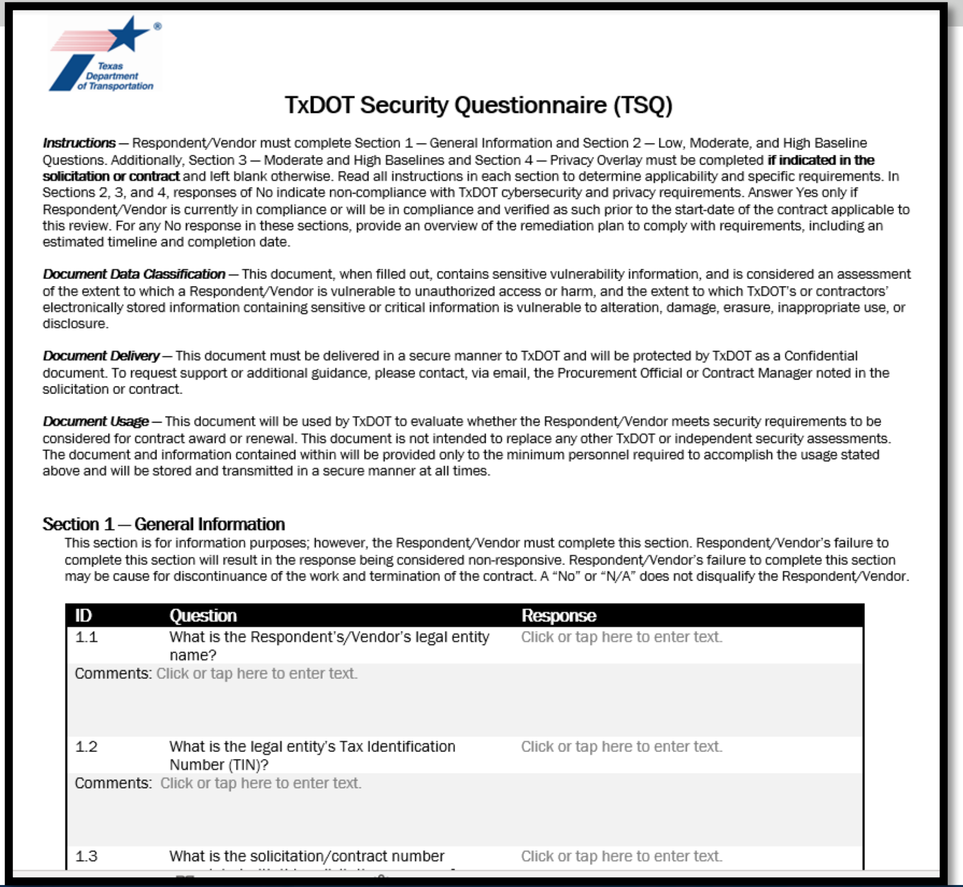
- Level 1 is out of scope for TxDOT systems
- Only systems that have Confidential/Regulated Data or are High baseline (Life/Death) require TX-RAMP level 2
  - Other Moderate systems – case by case (see TxDOT IS-RAMP)

TxDOT Security Questionnaire

- Different legislation in the 87th session requires agencies to evaluate third parties – TxDOT does this using the TxDOT Security Questionnaire (TSQ)
- Even if a system doesn't require TX-RAMP, it may still need a TSQ
- Reviewed/developed with ACEC – American Council of Engineering Companies
- If a vendor answers "No" - not a deal breaker
  - Does require Risk Acceptance by IO, CIO, and CISO – TPR team will help walk that through

TxDOT Security Questionnaire Review

TxDOT Security Questionnaire



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	Click or tap here to enter text.

How Do You Know if TX-RAMP or TSQ Is Needed?

ITD Contract Review (ITDCR)

- Procurement team submits form
- Several ITD Sections will review and provide needed actions

InfoSec will give statements to be added to the contract that specify requirements and parts of T&C in scope

Attachment I (our Standard Terms and Conditions) includes the requirements vendors must comply with

PEPS Contract Attachment Reference

What Threats Does TxDOT Face?

- Phishing still the biggest threat
  - Don’t open attachments from senders you don’t know
  - Don’t click on links from senders you don’t know
  - If you think it’s a phish, forward the message to spam@txdot.gov
- Out of date software
  - If you’re an owner of an information system, ensure it gets patched
    - ITD won’t always patch without owner say-so, we don’t want to disrupt operations
- Ransomware…because of the first two

What We Are Doing to Mitigate Threats

Multi-factor Authentication

- Best defense against account compromise
- Not always convenient, but worth the effort

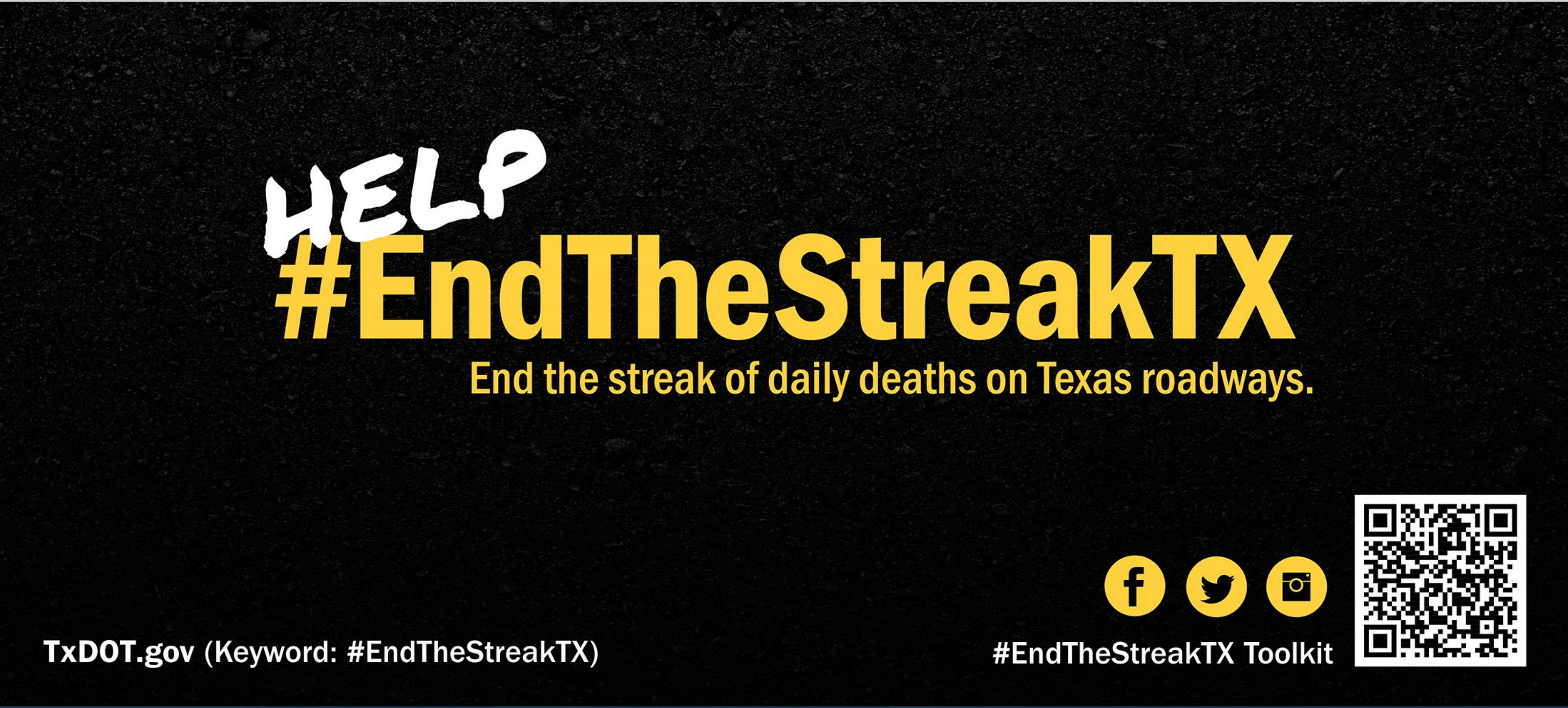
Vulnerability Management Program

- More proactive about patching critical risks
- Focused on the infrastructure that supports systems, so system specific patching still needs owner involvement

Expanding monitoring capabilities

Resources

- Information Security SharePoint page
- Cybersecurity At TxDOT external facing website – Also where to report a suspected/actual cybersecurity incident
- Spam@txdot.gov – send any suspicious emails here
- If you think you've been compromised, contact the help desk



HELP

#EndTheStreakTX

End the streak of daily deaths on Texas roadways.

TxDOT.gov (Keyword: #EndTheStreakTX)

#EndTheStreakTX Toolkit

Questions and Discussion

Peter Lee

Information Security Officer

✉ Peter.lee@txdot.gov

☎ 512-774-9596