Information Technology Division (ITD) Review Process

2022 PEPS Conference

Dan Neal, P.E.

Steven Pryor

November 30, 2022

Training Topics

1. Background
2. ITD Intake Form (TxDOT)
3. TxDOT Security Questionnaire (Consultants)
4. Cybersecurity Resources
5. Summary
6. Questions

Background

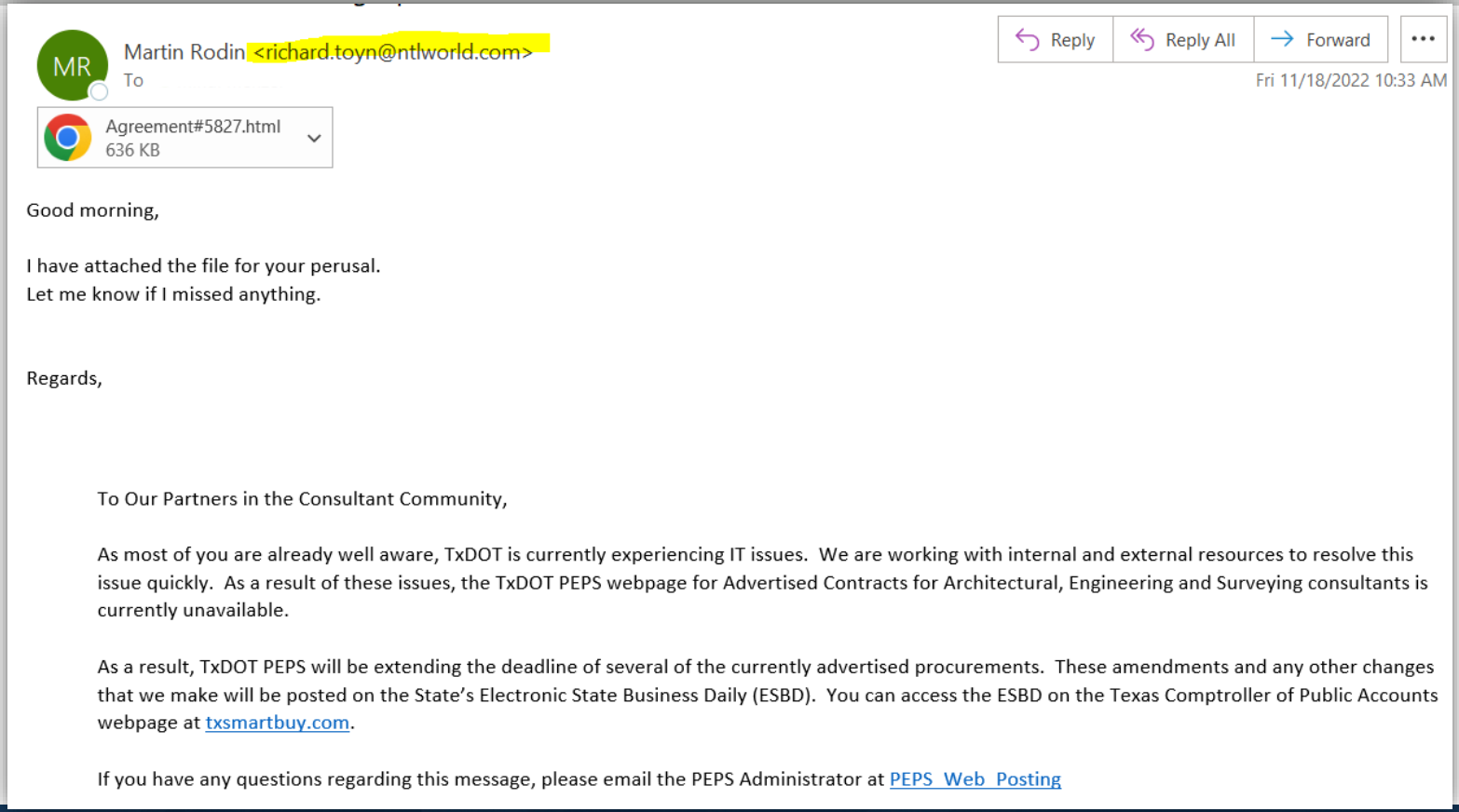
ITD Contract Review Process History

- **2017** – Auditors found TxDOT IT procurement non-compliant
- **2019** – ITD published the first IT and Security requirements attachment.
- **2020** – ITD updated the IT and security requirements attachment and started the ITD Contract Review Process
- **2022** – ITD published the TxDOT security questionnaire and DIR started TX-RAMP

Why – Multiple US and Texas IT Procurement Laws

- (2005) **Texas Government Code §2054.391,** Use of Statewide Data Centers
- (2015) **Texas Administrative Code §202,** Information Security Standards
- (2018) **US Code of Federal Regulations §2.200.216 and 200.471,** Prohibitions on certain telecommunication and video surveillance services
- (2019) **Texas Government Code §2054.077,** Vulnerability Reports
- (2019) **Texas Business and Commerce Code §521.052,** Business Duty to Protect Sensitive Personal Information
- (2021) **Texas Government Code §2054.138,** Security Controls for State Agency Data
- (2021) **Texas Government Code §2054.0593,** Cloud Computing State Risk and Authorization Management Program (aka – TX-RAMP)
- (2021) **Texas Government Code 2062,** Restrictions on State Agency Use of Certain Individual Identifying Information
- (2022) US Critical Infrastructure Cyber Incident Reporting Act
- (2022) Bipartisan Infrastructure Law

Why – Growing Cybersecurity Threats



MR

Martin Rodin <richard.toyn@ntlworld.com>
To

Reply | Reply All | Forward | ...

Fri 11/18/2022 10:33 AM

Agreement#5827.html
636 KB

Good morning,

I have attached the file for your perusal.
Let me know if I missed anything.

Regards,

To Our Partners in the Consultant Community,

As most of you are already well aware, TxDOT is currently experiencing IT issues. We are working with internal and external resources to resolve this issue quickly. As a result of these issues, the TxDOT PEPS webpage for Advertised Contracts for Architectural, Engineering and Surveying consultants is currently unavailable.

As a result, TxDOT PEPS will be extending the deadline of several of the currently advertised procurements. These amendments and any other changes that we make will be posted on the State's Electronic State Business Daily (ESBD). You can access the ESBD on the Texas Comptroller of Public Accounts webpage at txsmartbuy.com.

If you have any questions regarding this message, please email the PEPS Administrator at PEPS_Web_Posting

ITD Intake Form

General Process for Assessment of the Contracts

Identify the data or IT elements

Assess the security level

Provider verification that it meets the requirements

Overview of ITD Review Process Steps

The ITD Intake Form must be submitted about four weeks prior to advertisement.

Copy the PEPS_COE_Process box when you submit the ITD Intake Form and on all correspondence to ITD.

COE will track the ITD review process.

Contact COE if ITD requires the inclusion of the Questionnaire.

As the review process becomes more defined by ITD, COE will develop additional guidance and training.

ITD Intake Form and Guidance

ITD Updated the Intake Form effective September 2022

They split the form into two parts:

Intake Form – core information

And

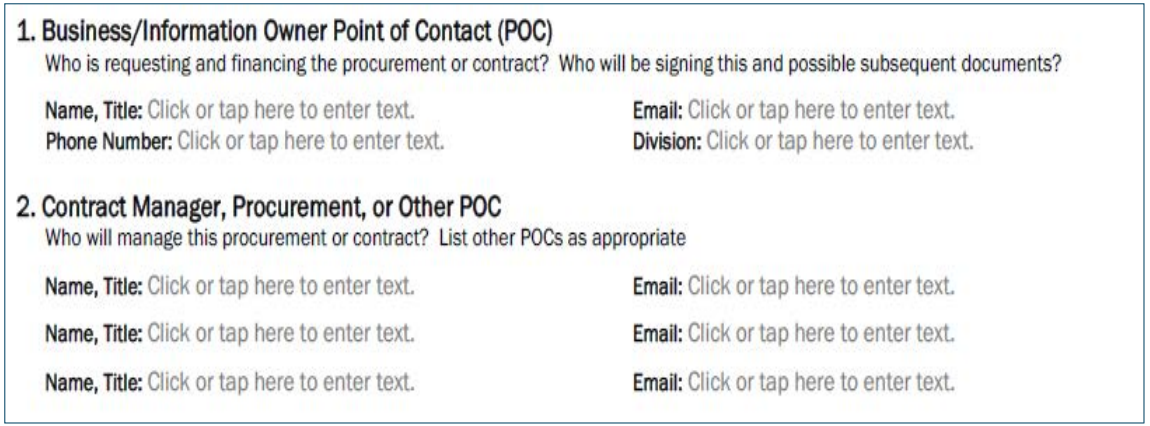
Intake Form Part B – data security questions

ITD Intake Form

Who is responsible for filling out this form? PEPS Procurement Engineer

1. Who will be the Business Point of Contact?
   Martin Rodin*

2. Who will be the Contract Manager?
   D/D Project Manager
   Procurement POC?
   Procurement Engineer



1. Business/Information Owner Point of Contact (POC)
Who is requesting and financing the procurement or contract? Who will be signing this and possible subsequent documents?

Name, 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. **Division:** Click or tap here to enter text.

2. Contract Manager, Procurement, or Other POC
Who will manage this procurement or contract? List other POCs as appropriate

Name, Title: Click or tap here to enter text. **Email:** Click or tap here to enter text.
Name, Title: Click or tap here to enter text. **Email:** Click or tap here to enter text.
Name, Title: Click or tap here to enter text. **Email:** Click or tap here to enter text.

*Recent change to ensure that any risk identified on the IT Security Questionnaire that would involve a determination compliance risk is addressed by the PEPS Division Director before contract is executed.

ITD Intake Form

3. At what stage is the procurement?

- Solicitation Development

- Amendment/Change Order

- Renewal

3. Procurement/Contract Stage (New, Amendment, or Renewal) Choose one of the following

☐ **SOLICITATION DEVELOPMENT** (The draft solicitation is planned or exists but has not gone out for bid)
Please also submit the draft Statement of Work (SOW) with this ITDCR, if available.

PeopleSoft RFQ Number: Click or tap here to enter text.

☐ **AMENDMENT/CHANGE ORDER** (The contract is being modified)
PeopleSoft Purchase Order Number: Click or tap here to enter text.

OR/AND

Other Identification Number: Click or tap here to enter text.

Brief Amendment/Change Order Reason Details:
Please summarize the reason for the amendment/change order and what is being modified (as examples: date, time, services provided, financial changes, and so forth)

☐ **RENEWAL** (The contract has an upcoming renewal)
Please also submit the contract and purchase order with this ITDCR and provide the TxDOTNOW SCTASK/RITM number:

Current PeopleSoft Purchase Order Number: Click or tap here to enter text.

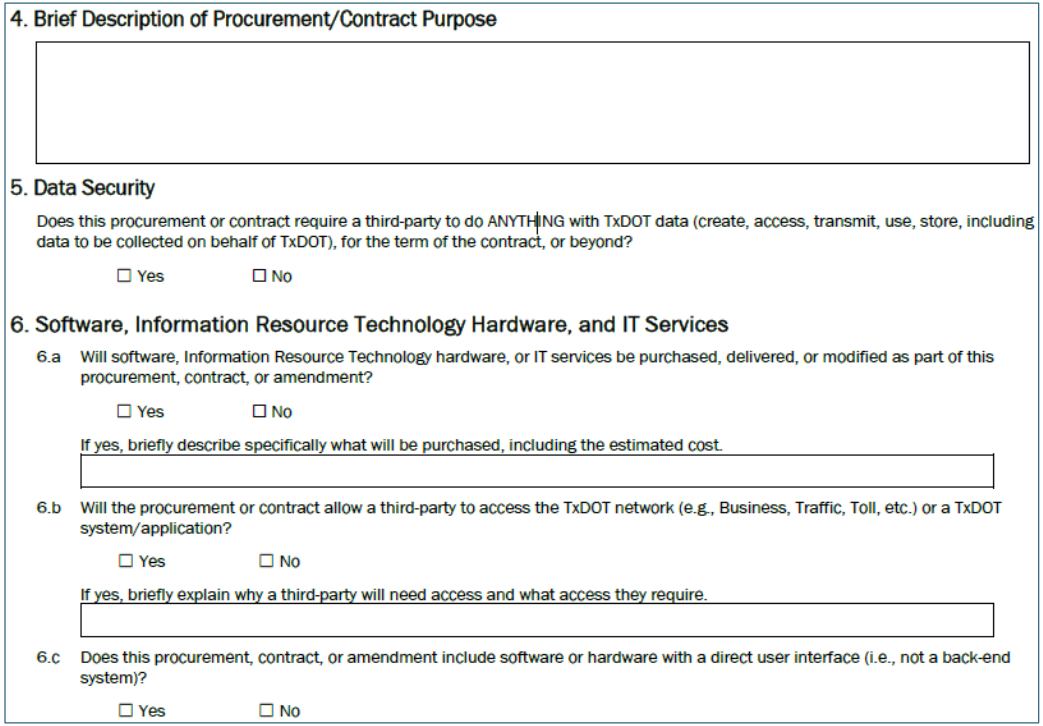
TxDOTNOW SCTASK/RITM Number: Click or tap here to enter text.

ITD Intake Form

4. Give a description of the scope of work

5. Does Procurement or contract require a third-party to do ANYTHING with TxDOT data (create, access, transmit, use, store, including data to be collected on behalf of TxDOT), for the term of the contract, or beyond?

6.a. Does the procurement include purchase of software, IT hardware or IT services?



4. Brief Description of Procurement/Contract Purpose

5. Data Security

Does this procurement or contract require a third-party to do ANYTHING with TxDOT data (create, access, transmit, use, store, including data to be collected on behalf of TxDOT), for the term of the contract, or beyond?

☐ Yes ☐ No

6. Software, Information Resource Technology Hardware, and IT Services

6.a Will software, Information Resource Technology hardware, or IT services be purchased, delivered, or modified as part of this procurement, contract, or amendment?

☐ Yes ☐ No

If yes, briefly describe specifically what will be purchased, including the estimated cost.

6.b Will the procurement or contract allow a third-party to access the TxDOT network (e.g., Business, Traffic, Toll, etc.) or a TxDOT system/application?

☐ Yes ☐ No

If yes, briefly explain why a third-party will need access and what access they require.

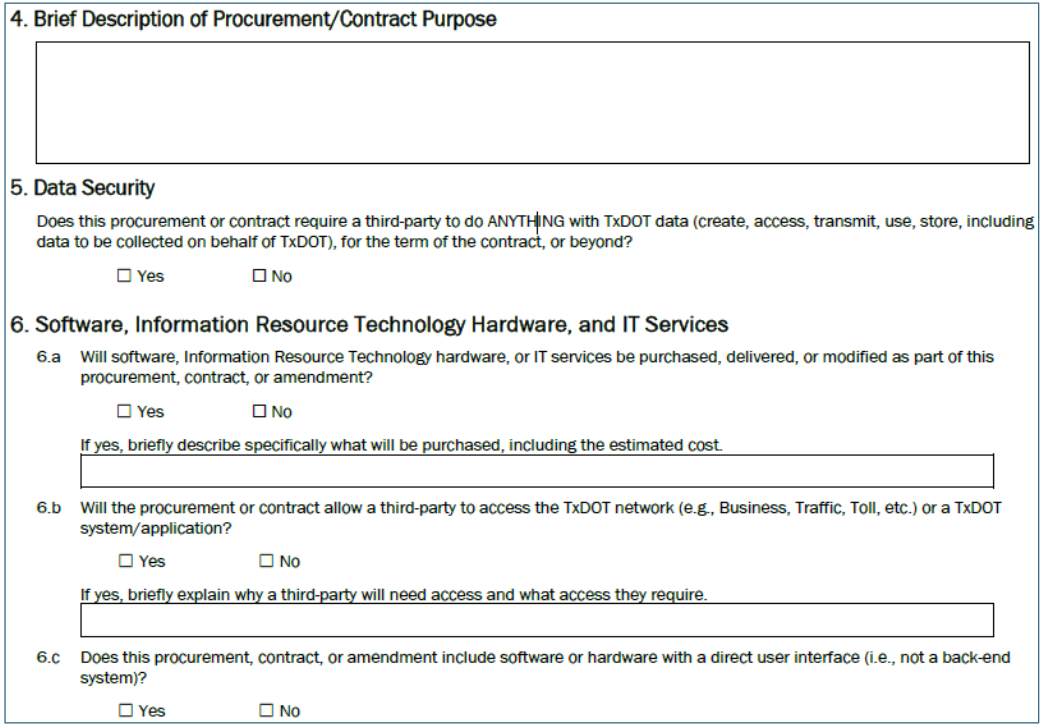
6.c Does this procurement, contract, or amendment include software or hardware with a direct user interface (i.e., not a back-end system)?

☐ Yes ☐ No

ITD Intake Form

6.b. Does the procurement or contract allow a third-party to access the TxDOT network or a TxDOT system or application?

6.c. Does the procurement, contract, or amendment include software or hardware with a direct user interface?



4. Brief Description of Procurement/Contract Purpose

5. Data Security

Does this procurement or contract require a third-party to do ANYTHING with TxDOT data (create, access, transmit, use, store, including data to be collected on behalf of TxDOT), for the term of the contract, or beyond?

☐ Yes ☐ No

6. Software, Information Resource Technology Hardware, and IT Services

6.a Will software, Information Resource Technology hardware, or IT services be purchased, delivered, or modified as part of this procurement, contract, or amendment?

☐ Yes ☐ No

If yes, briefly describe specifically what will be purchased, including the estimated cost.

6.b Will the procurement or contract allow a third-party to access the TxDOT network (e.g., Business, Traffic, Toll, etc.) or a TxDOT system/application?

☐ Yes ☐ No

If yes, briefly explain why a third-party will need access and what access they require.

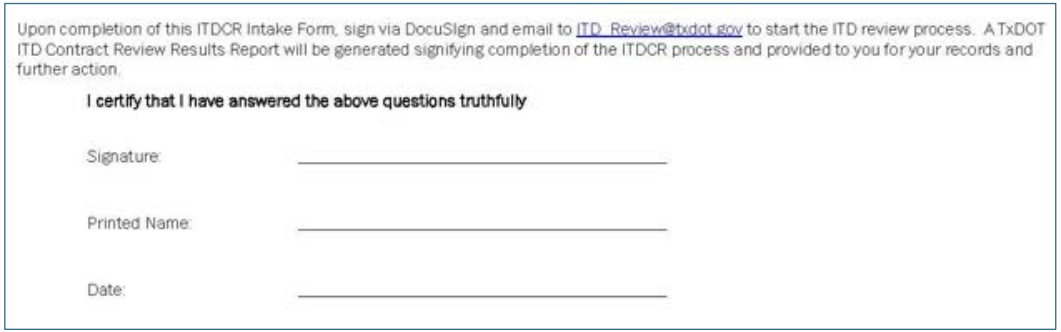
6.c Does this procurement, contract, or amendment include software or hardware with a direct user interface (i.e., not a back-end system)?

☐ Yes ☐ No

ITD Intake Form

Sign the form and include your printed name and date.

You will email this form and a copy of the contract documents to ITD at ITD_Review@TxDOT.gov and to the PEPS_COE_Process@TxDOT.gov box.



Upon completion of this ITDCR Intake Form, sign via DocuSign and email to ITD_Review@txdot.gov to start the ITD review process. A TxDOT ITD Contract Review Results Report will be generated signifying completion of the ITDCR process and provided to you for your records and further action.

I certify that I have answered the above questions truthfully

Signature: _____

Printed Name: _____

Date: _____

ITD Intake Form Part B

Question 2, focuses on the data and the classification of the data; whether the date is public, sensitive, confidential, or regulated.

PEPS in working with ITD has developed reference matrix for the classification of the data.

2. Data Security Additional Questions

2.a If this is an amendment, do data types change or are added?

☐ Yes ☐ No (Skip to Question 4)

2.b What is the estimated highest data classification category (see TxDOT Data Classification Policy) of TxDOT data involved?

- ☐ **Public** (ex: agency publications such as news releases or informational brochures; public web postings or brochures; description of TxDOT's divisions or district organizations)
- ☐ **Sensitive** (ex: agency operational information, personnel records, internal communications, internal organizational charts, contact lists with business phone numbers or business email addresses; legal information, employment agreements, separation agreements, nondisclosure agreements (NDAs), intellectual property, or contracts; financial information about the agency's accounting such as balance sheets, purchase orders, contracts, or budget information)
- ☐ **Confidential** (ex: Social Security numbers, home addresses, dates of birth or death, health-related information)
- ☐ **Regulated** (ex: payment card information, including account numbers, cardholder names, expiration dates; personal information from State Motor Vehicle Records)

2.c Name of the TxDOT system or business application that TxDOT data is coming from or going to (check all that apply, add/remove rows as needed)?

Name of TxDOT System/Business Application	Direction of TxDOT Data
	☐ Incoming to TxDOT ☐ Outgoing from TxDOT
	☐ Incoming to TxDOT ☐ Outgoing from TxDOT
	☐ Incoming to TxDOT ☐ Outgoing from TxDOT

The list of TxDOT registered systems/business applications is available here: System Inventory.

Standard Scope IR and Security Requirements

PEPS, ITD, and CSD have coordinated to develop language for the scope to specify the requirements that need to be followed to meet the security requirements for the data.

This paragraph is included in all of the contract scopes

This information is important for the consultant, since it answers questions on the TxDOT Security Questionnaire (TSQ)

1.XX Information Resources and Security Requirements

[Engineer, Architect, Surveyor] (as "Contractor") shall perform its work in accordance with Attachment I, Information Resources and Security Requirements. A Contractor-Related Entity might create, access, transmit, store, or use <Public | Sensitive | Confidential | Regulated> TxDOT data in a Contractor-Related Entity Environment. Contractor shall ensure that Contractor-Related Entity Environments comply with the TxDOT <Low | Moderate | High> Security Baseline <with the <Sensitive, Privacy, PCI, CJIS> Overlay; remove if no Overlays apply>.

Standard Scope IR and Security Requirements

Based on evaluations of the standard scope templates, PEPS and ITD have agreed upon the data classification, security baseline and overlays for the standard scope types.

This is available to all of the TxDOT staff.

Discipline	Type of Provider	Data Classification	Security Baseline	Overlay
Bridge Inspection	Engineer	Confidential	Moderate baseline	n/a
CEI	Engineer	Sensitive	Low baseline	Sensitive
Materials Engineering	Engineer	Public	Low baseline	n/a
PS&E	Engineer	Public	Low baseline	n/a
Schem/Env/PS&E	Engineer	Public	Low baseline	n/a
Survey	Surveyor	Public	Low baseline	n/a
Traffic Engineering	Engineer	Public	Low baseline	n/a
Utility Engineering	Engineer	Public	Low baseline	n/a

ITD Contract Review Process

Takes up to 4 weeks to complete depending on complexity of the procurement

Involves Multiple IT Teams Including

- Data Center Services
- Information Security
- Accessibility
- Data Privacy

Output provides key IT components and requirements for the procurement including whether a TxDOT Security Questionnaire (TSQ) or TX-RAMP is required

TxDOT Security Questionnaire

TxDOT Security Questionnaire

01

TxDOT's mechanism to determine a third party's ability to meet TxDOT security control requirements (new 2054.138 requirement).

02

A set of Yes/No questions for third parties to complete at time of selection.

03

Answering "No" to certain questions in sections 2-4 require TxDOT CISO review prior to award

TxDOT Security Questionnaire (continued)

Comprised of 4 sections depending on security baseline:

Section	Who Must Complete	# of Questions
1- General	All Respondents	12
2 – Low Baseline	All Respondents	24
3 – Moderate Baseline	Only if Moderate Baseline	29
4 – Privacy Overlay	Only if Privacy Overlay	8

Section 1 is informational only, not used to determine compliance.

Sections 2-4 are Yes/No compliance attestation questions. Any **"No"** answers require CISO review prior to contract award.

TxDOT Security Questionnaire Common Issues

Section 1:

- Questions 1.6-1.8 (security baseline) - not completed or not aligned with TxDOT's contract requirements

Section 2-4:

- Answering "No" but not providing a clear reason why it's no, what is being done to resolve compliance, or a remediation date

General:

- Not signed

If every unsure what is being asked, reach out to TxDOT for clarification.

Example Questions from Section #2

2.1 Does the vendor have a group within the organization responsible for cybersecurity?

2.2 Are Vendor information security roles and responsibilities defined and documented in a policy formally approved by the vendor?

2.4 Is the information system, including its components patched in a timely manner as patches become available?

2.5 Will all vendor employees and subcontractors be required to sign an agreement prior to being authorized to create, access, transmit, use or store TxDOT data?

2.6 Are use accounts approved prior to provisioning, reviewed periodically, and removed when no longer necessary or the employee is terminated?

Example Questions from Section #2 (continued)

2.7 Are users assigned a unique username or unique identifier?

2.8 Are inactive accounts automatically disabled or removed after a denied period of inactivity?

2.9 Are user accounts automatically locked after a number of incorrect login attempts?

2.10 Are passwords required to be sufficiently strong such that commonly guessed passwords are not allowed, default passwords are not allowed or immediately changed upon first use, and passwords automatically expire after a period of time?

2.14 Is system data backed up periodically?

Example Questions from Section #2 (continued)

2.18 Is there an individual responsible for cybersecurity within the vendor's organization?

2.21 is a vulnerability management process in place to monitor information system vulnerabilities and ensure appropriate remediation is a timely manner?

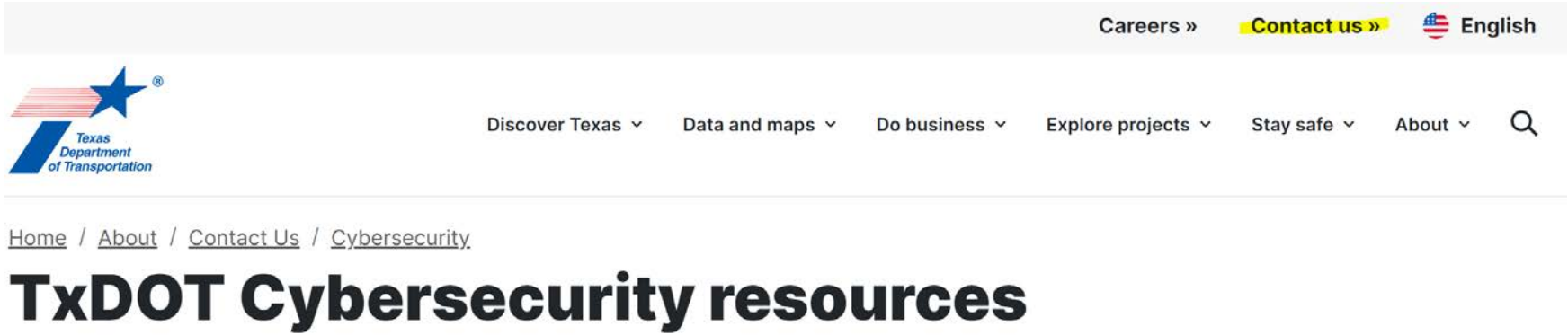
2.22 is an incident notification policy in place to notify TxDOT of a potential/suspected cyber security incident potentially involving TxDOT date?

2.23 Is a cybersecurity training and awareness program in place to increase awareness of cybersecurity and privacy threats and best practices?

Cybersecurity Resources

TxDOT Cybersecurity Resources

Go to TxDOT.gov under Contact Us to access the latest Cybersecurity resources



TxDOT/ACEC Workgroup on CyberSecurity

New workgroup focused on cybersecurity issues

Goal is to identify areas where TxDOT's cybersecurity and ITD documents could be modified to improve clarity

Areas of concern:

- Costs to smaller firms to meet Texas cybersecurity requirements
- TSQ questions are confusing and are answered "yes" without understanding

Summary

Summary

An ITD Intake Form must be approved prior to advertisement

All of the procurements will need to submit an Intake Form

ITD comments must be addressed prior to advertisement

If ITD requires a Questionnaire to be included, contact COE

ITD is responsible for the review of the provider responses to the questionnaire and will coordinate any follow-up action

Questions and Discussion

Contact Information

Dan Neal, P.E.

PEPS COE Section Director


Dan.Neal@txdot.gov


512-416-2667

Steven Pryor

Chief Information Security Officer


Steven.Pryor@txdot.gov


512-302-2008