



Doing Business with TxDOT

Cybersecurity Considerations



- 1 Prohibited Technologies
- 2 Information Technology Division (ITD) Contract Review Process
- 3 TxDOT Security Questionnaire
- 4 Information Resources and Security Requirements (Attachment I)
- 5 TX-RAMP



Governor Abbott, in January 2023, directed Texas agencies to implement a policy to prohibit the use of certain technologies from being used for agency business.

The prohibition covers several key areas:

1. Prohibition on downloading or installing prohibited technologies on TxDOT issued devices.
2. Prohibition on purchasing and/or using prohibited technologies to conduct TxDOT business, including technologies on personal devices used for TxDOT business.
3. Requirement to conduct certain TxDOT business in a secure location free of prohibited technologies.

The intent of the prohibition is to prevent Texas business that could pose a threat to the United States from being accessed or compromised by foreign nations.



The official TxDOT list is available at [Prohibited Technologies List \(txdot.gov\)](https://www.txdot.gov/prohibited-technologies-list)

Software / Applications

- Alipay
- CamScanner
- Kaspersky Security & VPN
- SHAREit
- TikTok
- WeChat
- WeChat Play
- WPS Office

Developers

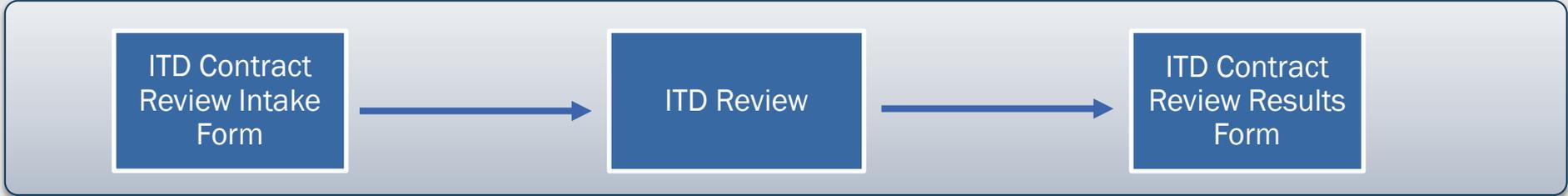
- Alipay (Hangzhou)
- ByteDance LTD
- INTSIG Information Co., Ltd
- Kaspersky Lab Switzerland GmbH
- Kingsoft Office Software Corporation
- SHAREit Technologies Co. Ltd
- Tencent Holdings
- TikTok Ltd.
- WeChat

Hardware / Equipment Manufacturers

- Dahua Technology Company
- Huawei Technologies Company
- Hangzhou Hikvision Digital Technology Company
- Hytera Communications Corporation
- SZ DJI Technology Company
- ZTE Corporation

Includes any subsidiary or affiliates of an entity listed above. Contact Information Security for clarification.

List is derived from [DIR Prohibited Technologies Guidance](#)



Process:

- ITD Contract Review Intake Form Part A completed
- ITDCR admin reviews and determines if a Part B is needed
- If needed ITDCR Intake Form Part B is required.

Participate in Review:

- Information Security
- Accessibility
- Data Center Services Liaison
- Finance

Review takes 3-4 weeks

Identifies requirements:

- TxDOT Security Questionnaire (TSQ)
- ITD Terms and Conditions (Attachment I)
- TX-RAMP
- Texas Data Center Exemption
- Hardware Requirements
- Accessibility Requirements
- SOC 1 requirements

Questions about the overall ITDCR Process can be emailed to the ITD Contract Review team at ITD_Review@txdot.gov.



Identifies use of TxDOT data.

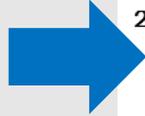


5. Data Security

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

Requestor Identifies if this is an amendment



2. Data Security Additional Questions

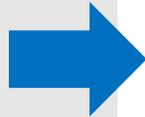
2.a If this is an amendment, do data types change or are added?

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)

Requestor Identifies the estimated data classification



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
	<input type="checkbox"/> Incoming to TxDOT <input type="checkbox"/> Outgoing from TxDOT
	<input type="checkbox"/> Incoming to TxDOT <input type="checkbox"/> Outgoing from TxDOT
	<input type="checkbox"/> Incoming to TxDOT <input type="checkbox"/> Outgoing from TxDOT

Requestor identifies connecting TxDOT systems



The list of TxDOT registered systems/business applications is available here: [System Inventory](#).



CONFIDENTIAL when completed per Texas Government Code 552.139



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.	

The PEPS Procurement Engineer (PcE) sends the TSQ to the selected provider prior to negotiations.



The PcE must send the data classification, baseline, and security overlay to the provider.

The provider should answer “yes” only if the provider is currently in compliance or will be in compliance and verified as such prior to the start date of the contract.

Any “no” answer requires that the provider include an overview of the remediation plan to comply with security requirements, including an estimated timeline and completion date.



The PcE must check the TSQ to make sure Section 1 matches the ITDCR Results Form.

- 1.6 – Security Baseline (Low, Moderate, High)
- 1.7 – Security Overlay (N/A, Sensitive, Privacy, PCI, CJIS)
- 1.8 – Data Classification (Public, Sensitive, Confidential, Regulated)
- 1.9 – TX-RAMP (TX-RAMP Level 1, TX-RAMP Level 2, N/A)

If the TSQ indicates the firm is in compliance (all answers in 2, 3, and 4, as applicable, are “yes” or “n/a”), the PcE is not required to submit to ITD for review.

If the TSQ is noncompliant (“no” answers), the PcE must review the remediation proposed for any “no” answer. If it is clear and has a reasonable date, the PcE will submit the TSQ to ITD for review. If the response is incomplete or unclear, the PcE must meet with the provider to obtain a complete response.

TSQ Deviation Request Form

The TxDOTNow form replaces the old email form

If the TSQ is noncompliant (any “NO”), submit a Third-Party Security Deviation Request to Information Security via TxDOTNow

The form is completed by the PEPS Procurement Engineer, not the provider.

Third Party Security Deviation

Request a security deviation for a third party.



Deviations are required for when a risk is identified for a third party, such as a "no" response in a TxDOT Security Questionnaire (TSQ). Deviations must be approved by appropriate TxDOT leadership prior to contract execution.

* Person to contact for questions ?	Date needed by
<input type="text"/>	<input type="text" value="MM/DD/YYYY HH:mm:ss"/>
* Third Party Name ?	* ITD Contract Review (ITDCR) Number ?
<input type="text"/>	<input type="text" value="Format should be ITDCR-####"/>
* Business Justification, ?	* Business impact ?
<input type="text"/>	<input type="text"/>
Compensating Control and Mitigating Factors ?	
<input type="text"/>	
Additional description or information ?	
<input type="text"/>	



2.24 – moved from asking if the respondent “will” be TX-RAMP ready to “are they”

2.25 – added a question on prohibited technology compliance

2.24	<p>Is the Respondent/Vendor providing TxDOT a cloud computing service certified through the Texas Risk and Authorization Management Program (TX-RAMP)? (TxDOT Control PM-01)</p> <p>If service is DIR TX-RAMP Certified, select Yes</p> <ul style="list-style-type: none">• TX-RAMP Level 1 (N/A if awarded/renewed before January 1, 2024)• TX-RAMP Level 2 <p>If <u>service</u> has a TX-RAMP Provisional Certification, select No – TX-RAMP Provisional Certification. Further approval by the TxDOT Information Security will be required.</p> <p>If service is not TX-RAMP Certified, Select No</p> <p>If service does not require TX-RAMP Certification, select N/A</p>	<p><input type="checkbox"/> <u>Yes</u> – DIR TX-RAMP Certified</p> <p><input type="checkbox"/> <u>No</u> – TX-RAMP Provisional Certification</p> <p><input type="checkbox"/> <u>No</u></p> <p><input type="checkbox"/> <u>N/A</u></p>
<p>If <u>Yes</u>, 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.</p>		<p>Planned Remediation Date: Click or tap here to enter text.</p>
2.25	<p>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? https://dir.texas.gov/information-security/prohibited-technologies (TxDOT Control SR-06)</p>	<p><input type="checkbox"/> <u>Yes</u></p> <p><input type="checkbox"/> <u>No</u></p>
<p>If No, please provide explanation, plans to remediate, and any compensating controls or mitigating factors: Click or tap here to enter text. Click or tap here to enter text.</p>		<p>Planned Remediation Date: Click or tap here to enter text.</p>



Contains Standard Terms and Conditions for TxDOT

Intended to work without modification – applicability of terms is based on statements from ITDCR Results Form

From:

3.8 Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment

In accordance with 2 CFR §§ 200.216 and 200.471, Contractor shall not provide services, equipment, or systems for telecommunications or video surveillance that (a) are provided or manufactured by or (b) have components provided or manufactured by any of the following business entities:

- (1) Huawei Technologies Company
- (2) ZTE Corporation
- (3) Hyatera Communications Corporation
- (4) Hangzhou Hikvision Digital Technology Company
- (5) Dahua Technology Company
- (6) Any subsidiary or affiliate of an entity listed above

To:

3.8 Prohibited Technologies

In accordance with the Texas Statewide Plan for Prohibited Technologies, Contractor shall not provide services, equipment, or systems to TxDOT determined to be a Prohibited Technology by TxDOT. A list of the entities currently determined to be Prohibited Technologies is available at:

<https://ftp.txdot.gov/pub/txdot/itd/cybersecurity/prohibited-technologies-list-cybersecurity.pdf>

TX-RAMP Certification – Process Overview

- IF the ITDCR Results Form states TX-RAMP is Required: Follow guidance provided in ITDCR Results Form:
 - If contractor and involved system have no TX-RAMP certification status, InfoSec will provide guidance in the ITDCR Results Form for contractors to obtain TX-RAMP Certification or Provisional status through DIR.
 - If a contractor already has a TX-RAMP Provisional status, InfoSec will provide guidance in the ITDCR Results Form for contractors to obtain a TX-RAMP Evaluation through TxDOT. A summary of the TX-RAMP Evaluation Process is included below:
 - Must submit a TX-RAMP Evaluation Package to Vendor Management for ISO Review before TxDOT acceptance of provisional status.
 - If the TX-RAMP Evaluation Package is complete, but indicates non-compliance, a third-party security deviation will need to be approved along with the TX-RAMP Decision.
 - Provisional status expires after 18 months from notification of award through DIR. Contractors must obtain TX-RAMP Level 1 or Level 2 certification prior to expiration.
- Average process length: TX-RAMP Evaluations take up to 30 days and can take longer if more information is needed is from the contractor.

TX-RAMP Certification – Process Inputs & Outputs

Input(s)/Process Trigger	Output(s)/Result
<ul style="list-style-type: none"> If a new contract or contract renewal As part of the ITD Contract Review, it will be determined if TX-RAMP is required. 	<ul style="list-style-type: none"> If TX-RAMP is required: Follow guidance provided within ITDCR results form If TX-RAMP is not required: No further action is needed

Security Baseline	Required TX-AMP Certification	Effective Date
Low	Level 1	1/1/2024
Moderate	Level 2	1/1/2022
High	Level 2	1/1/2022

TX-RAMP Level 1

(Required prior to any contract award or renewal that takes place after January 1, 2024)

Automatic Certification through contractor held attestations: FedRAMP Low, StateRAMP Category 1, or AZRAMP Level 2

Required for any cloud computing service
TxDOT Low Baseline

TX-RAMP Level 2

(Certification Required by January 1, 2022)

Automatic Certification through contractor held attestations: FedRAMP Moderate, StateRAMP Category 3, or AZRAMP Level 3

Required for any cloud computing service
TxDOT Moderate Baseline

Questions



Steven Pryor

Chief Information Security Officer
Texas Department of Transportation

Mobile: (512) 965-4487

Steven.Pryor@txdot.gov