Information Security Office
GDE-01-604

Guideline Title: Reconnection Attestations

Effective Date: 12/5/2022

Date of Last Revision: N/A

DocuSigned by:
Steven Pryor
E5B3FA5479BF4DC...

Division of Primary Responsibility: TxDOT Information Security Office

Purpose

This Reconnection Attestations Guideline describes the minimum requirements that organizations must provide the Texas Department of Transportation (TxDOT) to affirm that their operations are secure and remain compliant with TxDOT security policies. Follow these guidelines to provide TxDOT the minimum necessary details to seek reconnection and continue to access, transmit, use, or store TxDOT data.

Required Elements

Attestation must be provided on company letterhead. It must be signed by an individual on behalf of the organization who has the legal authority to attest that the summary and required additional information provided are materially true and that they accurately, completely, and justly represent the security incident. The attestation must include a statement that the organization agrees to meet the security controls provided in the *TxDOT Information Security and Privacy Controls Standards Catalog* and to periodically provide evidence that it continues to meet the required security controls.

Attestation must include a summary of the incident that specifies when the incident was first identified and when it was reported to TxDOT. The summary must also address information about:

- The incident, including incident indicators, identification, objectives. and timeline;
- The TxDOT data involved, including the types of TxDOT data, if it was encrypted at the time of the incident or why it was not encrypted, and if was commingled with other data;
- The aftermath, including if the incident was propagated to other state systems; if the incident was classified as ransomware; if it resulted in criminal violations (and if they were reported or not); if it involved the unauthorized disclosure or modification of confidential information, including Personally Identifiable Information as defined in the Texas Business and Commerce Code, §521.002(1); and if it compromised, destroyed, or altered information systems, applications, or access to such systems or applications in any way.

The Attestation must also provide a summary of how the security incident was resolved. This summary must address all recovery and resolution efforts including:

- If the source of the incident was identified and addressed;

- If other partners, subcontractors, or vendors were involved in the recovery effort and what roles they played;
- How you validated that the incident had been resolved.

Attach the following information related to the security incident:

- Updated TxDOT Security Questionnaire (TSQ)
- 3rd party forensic results of incident resolution (if available or mandated by TxDOT)

NOTE: TxDOT reserves the right to ask for additional information as details warrant.

Definitions

Personal identifying information- means information that alone or in conjunction with other information identifies an individual, including an individual's:
(A) name, social security number, date of birth, or government-issued identification number;
(B) mother's maiden name;
(C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;
(D) unique electronic identification number, address, or routing code; and
(E) telecommunication access device as defined by Section 32.51, Penal Code.
[Source: Texas Business and Commerce Code, §521.002(1)]

Security incident- An event that results in the accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, exposure, or destruction of information or information resources. [Source: 1 TAC §202.1(40)]

State-controlled data--Any and all data that is created, processed, or stored by a state agency. [Source: 1 TAC §202.1(43)]

References

Texas Government Code, Sec. 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.