THE UNIVERSITY OF TEXAS SYSTEM AUDIT OFFICE

Cybersecurity Training Compliance Audit
Fiscal Year 2021

SUMMARY

BACKGROUND

House Bill 3834 of the 86th Legislative Session added two sections to Chapter 2054 of the Texas Government Code (TGC) requiring that "certain state and local government employees and state contractors complete a cybersecurity training program certified by the [Texas] Department of Information Resources [(DIR)]."

1. §2054.5191 requires that any state employee using a computer to perform at least 25% of his or her duties and any elected or appointed officer of the state entity complete a certified training program annually, completion be verified, and an "internal review […] to ensure compliance" be performed "periodically."

2. §2054.5192 requires that any contractor granted access to "a state computer system or database" complete a certified training program during the term of the contract and again during any renewal period, the training requirement is included in contract terms, and the state entity's "person who oversees contract management" periodically review contracts for compliance and report completion to DIR.

Both rules became effective June 14, 2019.

OBJECTIVE

Determine if The University of Texas (UT) System Administration complies with the employee and contractor cybersecurity training, monitoring and reporting requirements of TGC §2054.5191 and §2054.5192.

CONCLUSION

The processes in place to identify and monitor employee training completion are generally effective but information reported to DIR in June 2021 was not accurate at the time of reporting. For contractors, periodic review of contracts is needed to improve identification, monitoring and reporting of contractors required to complete cybersecurity training.

OBSERVATIONS

1 **Medium**	Verification of the accuracy and completeness of information sources used for ongoing monitoring of employee training completion and annual compliance certification to DIR will improve reporting accuracy and compliance with the provisions of TGC §2054.5191.
2 **Medium**	Because not all contractor system access requires assignment of System Administration network credentials which require training prior to assignment, monitoring of contractor training attestation based on contract expectations at contract execution and renewal is necessary to ensure accurate reporting and full compliance with the provisions of TGC §2054.5192.

OBSERVATION 1

MEDIUM

Compliance with Employee Training Requirement
TGC §2054.5191

Verification of the accuracy and completeness of information sources used for ongoing monitoring of employee training completion and annual compliance certification to DIR will improve reporting accuracy and compliance with the provisions of TGC §2054.5191.

System Administration employees who use computers for at least 25% of their duties are required to complete cybersecurity training annually. In practice, System Administration requires all employees to complete this training. At the time of the audit, four employees (1% out of 494 identified during testing) had not done so. Three were hired or re-hired after the annual training program was delivered to employees in January and February 2021 and were employed longer than the 30-day grace period during which all compliance training is to be completed. We informed the Office of Talent and Innovation (OTI) to follow-up with these employees to ensure they complete the required training.

While nearly all employees received training, System Administration incorrectly reported 100% compliance with the employee training requirement to DIR in June 2021. The correct percentage for reporting purposes was 90-99%. The process to determine compliance for reporting to DIR relied on a report generated by the learning management system that is used to deliver and track employee training, with no additional validation to confirm accuracy. The report included only records from the annual January and February training effort, and new employees (including rehires) subject to initial compliance training requirements were not considered. In addition, an apparent error in the query used to create the report resulted in the exclusion of at least one employee who had not completed the training requirement.

MANAGEMENT ACTION PLAN

SkillSoft will transition to an upgraded product offering (late 2021), Precipio, which will offer more reliable reporting and data integration capabilities. Until implementation of the upgraded product occurs, OTI will manually review individual new hire assignments.

By the end of the first quarter of fiscal year 2022, OTI and the Information Security Office (ISO) will partner with System Audit to transfer knowledge of a cross-reference data validation process to ensure accuracy and compliance.

To ensure completion of compliance training, OTI has identified the following measures to be implemented immediately:

- Transition of oversight to Talent Management Specialist;
- Use of PeopleSoft “GRP-action” emails as initial identifier for compliance tracking; and
- Implementation of an updated review schedule at 15 days and 30 days after hire.

Anticipated Implementation Date: December 31, 2021.

OBSERVATION 2

MEDIUM

Compliance with Contractor Training Requirement
TGC §2054.5192

> Because not all contractor system access requires assignment of System Administration network credentials which require training prior to assignment, monitoring of contractor training attestation based on contract expectations at contract execution and renewal is necessary to ensure accurate reporting and full compliance with the provisions of TGC §2054.5192

The TGC requires contractors with access to "a state computer system or database" to complete a cybersecurity training program both during the initial contract term and during contract renewal periods. The primary control in place to ensure compliance is to verify training attestation by the contractor at the point System Administration grants network access. However, at the time of the audit, ten contractors with actively used credentials had not attested to completion of training, and two independent contractors had not re-performed training attestation upon renewal of their contracts. Four of the 12 exceptions were for accounts created after the process to require training but prior to account setup began.

The current process to ensure contractors attest to completing cybersecurity training is decentralized, relying on departments to understand and enforce contractor cybersecurity training requirements when a System Administration login account is *not* needed by the contractor to use a System Administration system or database and when a contractor with existing credentials is granted a renewal period. We compared contractor training attestations to network access credentials and found that more than half of the attestations do not correspond with a network account. This indicates that the primary control to ensure contractor compliance (i.e., ensuring contractor training at the point that network access is granted) is not reliable to ensure full compliance with the training requirement.

There is also no monitoring to ensure all applicable contractors have completed training. Although Contracts and Procurement (CnP) maintains a record of all contractor training attestations, CnP does not monitor the contracts expected to require access to a system or database occurs to ensure all contractors have completed training.

Finally, System Administration incorrectly reported 100% compliance with the contractor training requirement to DIR in June 2021. We are unable to precisely determine an accurate percentage of compliance because contracts likely to require contractor access to System Administration systems or databases are not identified and monitored for this purpose.

MANAGEMENT ACTION PLAN

Going forward, the Director or Assistant Director of CnP will periodically attend the OTIS On/Offboarding Workgroup to ensure best practices are applied related to Cybersecurity Training for contractors. Currently, this group is working to update their Network Access Control Form.

By close of fiscal year 2022, CnP will go-live with ASC Contract Management Software which will provide tracking, notifications and reporting that support accurate monitoring of contractor training attestations based on contract expectations and execution and renewal.

Anticipated Implementation Date: August 31, 2022.

METHODOLOGY

This engagement was conducted in accordance with the guidelines set forth in the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*.

SCOPE AND PROCEDURES

The scope of the audit included fiscal year 2021 training completion as reported by System Administration to DIR on June 11, 2021. Procedures included a review of applicable policies and procedures, discussion with knowledgeable and responsible staff, comparison of training records to current employees, and limited testing of contracts and contractor compliance.

We will follow up on management action plans in this report to determine their implementation status. This process will help enhance accountability and ensure that timely action is taken to address the observations.

OBSERVATION RATINGS

Priority	An issue that, if not addressed timely, has a high probability to directly impact achievement of a strategic or important operational objective of System Administration or the UT System as a whole.
High	An issue considered to have a medium to high probability of adverse effects to a significant office or business process or to System Administration as a whole.
Medium	An issue considered to have a low to medium probability of adverse effects to an office or business process or to System Administration as a whole.
Low	An issue considered to have minimal probability of adverse effects to an office or business process or to System Administration as a whole.

CRITERIA

Texas Government Code Title 10, Subtitle B, Chapter 2054, sections 2054.5191 and 2054.5192

REPORT DATE

August 31, 2021

REPORT DISTRIBUTION

To: Phil Dendy, Chief Compliance and Risk Officer
Julie Goonewardene, Chief Innovation and Human Resources Officer
Terry Hull, Associate Vice Chancellor for Finance
Scott Kelley, Ed.D., Executive Vice Chancellor for Business Affairs
Helen Mohrmann, Chief Information Security Officer

Cc: Stephanie Gil, Manager, Human Resources Business Partners
Lori McElroy, Assistant Chief Information Security Officer
Frank Reighard, Director, Contracts and Procurement
UT System Administration Internal Audit Committee
External Agencies (State Auditor, Legislative Budget Board, Governor's Office)