Texas Water Development Board

Review of Select Cybersecurity Processes
Phase I: Data Classification

Project #2021.06
August 2022

Executive Summary

We reviewed processes and controls over the agency's data classification activities for fiscal year 2021. The primary objective of the review was to determine whether the agency's data classification processes ensure that electronic data is identified and classified in accordance with state and federal information security standards and guidance, internal policies and procedures, and relevant laws, rules, and regulations.

Overall, our review found that controls have been established to provide assurance that the agency's data is classified in accordance with requirements and guidance. Specifically:

- The agency has developed and implemented a data classification policy that defines four categories for classifying information and specifies that the data owner is responsible for data classification.

- New employee orientation training broadly covered all information technology security policies, including the data classification policy, and annual security awareness training often included modules that address data classification.

- An initial classification of data was performed through Information Technology's project delivery framework for the development of new applications.

- The Information Security Officer participated in security discussions for enhancements to legacy applications and facilitated data classification at certain stages of systems development and enhancements.

However, certain processes should be developed and implemented, or strengthened in some instances, to further ensure that:

- Additional guidance and targeted training specifically for information owners is provided and covers the agency's data classification policy and four data classification categories to ensure they are familiar with their related responsibilities.

- Data is periodically classified by the information owners, specific types of data - including PII - are identified, and updates to classification categories are documented, as needed.

Specific details regarding the second observation, noted within the Detailed Results section of this report, were omitted and communicated separately to the Board and management in writing, in accordance with government auditing standards and Texas Government Code.

Background

The Texas Administrative Code (TAC) Chapter 202[1] requires state agencies to define all information classification categories, except for the Confidential Information category, and establish controls for each. TAC 202[2] also requires information owners to classify information under their authority in accordance with the agency's established information classification categories.

Data classification is the process of categorizing data according to its type, sensitivity, and value to the agency if altered, stolen, or destroyed. Classifying data helps the agency:

- Understand the value of its data,
- Determine whether the data is at risk,
- Implement controls to mitigate risk of exposure, and
- Comply with applicable information security standards and guidance, and relevant laws, rules, or regulations.

According to the Department of Information Resources (DIR) Data Classification Guide[3], classifying data allows state agencies to make more efficient security decisions because it identifies and communicates the minimum level of protection required for any piece of data, as well as the individuals who may view that data.

While Texas Administrative Code defines confidential information[4], it does not explicitly define any additional classification categories. Therefore, to address a need for clarification and standardization, DIR's Data Classification Guide establishes a baseline data classification scheme that can be adopted and modified by state agencies. The classification scheme is based on Texas rules and law, as well as relevant federal standards and includes the following four classification categories:

Classification Category	Description
Public	Information that is freely and without reservation made available to the public.
Sensitive	Information that could be subject to release under an open records request but should be controlled to protect third parties.
Confidential	Information that typically is excepted from the Public Information Act.
Regulated	Information that is controlled by a federal regulation or other third-party agreement.

The agency's Information Technology (IT) Division's Data Classification Policy defines four classification categories for agency data, consistent with DIR's data classification scheme, and

[1] 1 TAC 202.24(b)(1)
[2] 1 TAC 202.22(a)(1)(A)
[3] DIR Data Classification Guide, Version 1.1
[4] 1 TAC 202.1(7)

references Texas Government Code, Chapter 552, Public Information Act, as it relates to protecting the data from unauthorized disclosure or public release. The Director for Information Technology is responsible for implementing and revising the policy. Per the policy, the data owner, in consultation with the agency's General Counsel, Information Security Officer (ISO), and Coordinator for Records Management, is responsible for data classification.

Additionally, Senate Bill 475, Sec. 2054.137(a) requires each state agency with more than 150 full-time employees to designate a full-time employee of the agency to serve as a data management officer which the agency has established. Sec. 2054.161 requires a state agency, on initiation of an information resources technology project, including an application development project and any information resources projects described in Subchapter G (Project Management Practices), to classify the data produced from or used in the project and determine appropriate data security and applicable retention requirements under Section 441.185 (Record Retention Schedules) for each classification.

Objectives, Scope, and Methodology

Objective

The objectives of the audit were to determine whether the agency's data classification processes and controls ensure that electronic data is identified and classified in accordance with state and federal information security standards and guidance, internal policies and procedures, and relevant laws, rules, and regulations.

Scope and Methodology

The scope of the audit covered fiscal year 2021 (September 1, 2020, to August 31, 2021), as well as any other related time periods.

The methodology for the audit consisted of a review of the following information:

- Texas Government Code, Chapter 552.
- Texas Government Code, Chapter 2054.
- Title 1, Texas Administrative Code, Chapter 202.
- DIR's Data Classification Guide.
- DIR's Security Control Standards Catalog.
- DIR's Cybersecurity Framework Control Objectives and Definitions.
- Agency Information Technology Policies and Procedures.
- Application inventory data.
- Application data maintained in the systems.

Tests and procedures included the following:

- Interviewed management and staff.
- Reviewed applicable statutes, rules, laws, and requirements.

- Reviewed agency policies and procedures, templates, forms, and related reports.
- Reviewed supporting documentation related to data classification.
- Interviewed information owners.
- Tested a sample of applications identified on the application inventory spreadsheet.
- Examined documentation to determine whether controls were operating as designed.

This engagement was conducted in accordance with *Generally Accepted Government Auditing Standards* and the *International Standards for the Professional Practice of Internal Auditing*. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our observations and conclusions based on our audit objectives.

The audit team consisted of:

Michelle Cooper, CGAP, CFE, CICA
Nicky Carter, CICA
Nicole Campbell, CIA, CISA

Detailed Results

We reviewed processes and controls over the agency's data classification activities. The review focused on fiscal year 2021, and any related time periods. The primary objective of the review was to determine whether the agency's data classification processes ensure that electronic data is identified and classified in accordance with state and federal information security standards and guidance, internal policies and procedures, and relevant laws, rules, and regulations.

Overall, our review found that controls have been established to provide assurance that the agency's data classified in accordance with the requirements.

However, we found that certain processes and controls over the agency's data classification activities should be developed and implemented, or strengthened in some instances, to further ensure compliance with requirements. Specifically, we noted the following:

1. **Information owners were not familiar with the agency's data classification policy and their related requirements.**

   Title 1, Texas Administrative Code, Chapter 202, Section 202.24(b)(1), requires state agencies to define information classification categories, with the exception of the Confidential Information category, and establish controls for each. Additionally, Title 1, Texas Administrative Code, Chapter 202, Section 202.22(a)(1)(A) requires owners to classify information under their authority in accordance with the agency's established information classification categories.

   Our review noted that the agency has established and implemented a data classification policy, that defines four categories for classifying information,[5] and those four categories are consistent with those established by DIR's Data Classification Guide.[6]

   The agency's new employee orientation and related training broadly covers all information technology security policies, including the data classification policy. And all employees, contractors, interns, and volunteers who have access to a TWDB application or system, are required to also complete TWDB's annual security awareness training, in accordance with Texas Government Code 2054.5191. This annual training varies, but often includes modules that address data classification.

   We interviewed a total of 11 information owners throughout various Offices within the agency to determine whether they were:

   (a) Aware that they were listed as the information owner of the application, and
   (b) Familiar with the agency's data classification policy and their related responsibilities.

[5] IT Security Policies, Data Classification Policy, September 2019
[6] DIR Data Classification Guide, Version 1.1

Our review found that despite the training efforts noted above, all 11 information owners stated that they were not familiar with the agency's data classification policy, or the four classification categories.

We also noted that four (37%) of the 11 information owners were not aware that they were listed as the designated owner for their respective application(s), and two (11%) stated that they inherited ownership and were not the subject matter experts for the application(s).

It is necessary for information owners to be familiar with the agency's data classification policy, as well as related rules and guidance, and informed on the significance of their roles as it relates to classifying and protecting the agency's data, so that they can effectively fulfill their related responsibilities.

Recommendation

Additional guidance and targeted training specifically for information owners should be provided and should cover the agency's data classification policy and four data classification categories to ensure they are familiar with their related responsibilities.

Managements Response: *IT leadership agrees with the recommendation. We have determined that the information owner is the same as the data owner and will implement processes to ensure data owners receive annual training on the agency's data classification policy, to include the four data classification categories. The data owners reside in the business areas and their responsibilities related to the data classification policy will be integrated into the agency's Data Governance program and processes.*

Responsible Party: *Ashok Durairajan, Data Officer / Angela Gower, Information Security Officer*
Implementation Date: *08/31/2023*

2. A standardized process does not exist to ensure agency data is periodically classified, specific types of data including PII are identified, and updates to classification categories are documented as needed.

We assessed the agency's process for identifying and classifying data, including PII, as well as updating and documenting classification categories.

We noted that while certain procedures and controls have been implemented, a standardized process should be developed to ensure data is periodically classified, specific types of data including PII are identified, and updates to classification categories are documented, as needed.

To minimize security risk, details regarding this observation were communicated separately to the Board and management in writing.

Pursuant to Standard 9.61 of the U.S. Government Accountability Office's *Generally Accepted Government Auditing Standards*, certain information was omitted from this report because of

its confidential and sensitive nature. Under the provisions of Texas Government Code, Section 552.139, the omitted information is also exempt from the requirements of the Texas Public Information Act.

Recommendation

A standardized process should be developed and implemented to ensure data is periodically classified, specific types of data including PII are identified, and updates to classification categories are documented, as needed.

Managements Response: *IT leadership agrees with the recommendation. Through the Data Governance program, a process will be implemented that ensures data classifications are reviewed/updated annually. This process and any applicable data classification updates will be documented.*

Responsible Party: *Ashok Durairajan, Data Officer / Angela Gower, Information Security Officer*
Implementation Date: *08/31/2023*

Closing

We would like to express our appreciation to all of the management and personnel for their cooperation and assistance provided to the internal audit staff during this review. For questions or additional information concerning this report, please contact Nicole Campbell at (512) 463-7978.

Report Distribution

Internal Distribution

Board's Office
Brooke T. Paup, Chairwoman
Patrick Lopez, Chief of Staff to Chairwoman Paup
George B. Peyton V, Board Member
Adrianne Evans, Chief of Staff to Board Member Peyton

Executive Administrator's Office
Jeff Walker, Executive Administrator
Amanda Lavin, Assistant Executive Administrator

Program Area
Edna Jackson, Deputy Executive Administrator, Operations and Administration

External Distribution

Legislative Budget Board
audit@lbb.state.tx.us

Governor's Office of Budget, Planning, and Policy
budgetandpolicyreports@gov.texas.gov

State Auditor's Office
iacoordinator@sao.state.tx.us