An Audit Report on

Confidential Data Management at the Office of the Comptroller of Public Accounts

Lisa R. Collier, CPA, CFE, CIDA
State Auditor

The Office of the Comptroller of Public Accounts (Office) implemented data loss prevention and certain other processes and controls to secure its confidential data. However, it should strengthen those processes and controls to help prevent unauthorized disclosure of its confidential data.

This audit was conducted in accordance with Texas Government Code, Section 321.0132.

LOW

DATA LOSS PREVENTION

The Office used a data loss prevention system and laptop/tablet disk encryption to help prevent the exposure of confidential data.

Chapter 1 | p. 4

To minimize security risks, auditors communicated details about the other audit findings separately to the Office in writing.

PRIORITY One finding was rated Priority because of issues that could critically affect the Office's ability to effectively administer its information security function. Immediate action should be taken to reduce the risk.

HIGH One finding was rated High because the issues could substantially affect the Office's information security function.

MEDIUM Two findings were rated Medium, indicating moderate risk.

For more information about this audit, contact Audit Manager James Timberlake or State Auditor Lisa Collier at 512-936-9500.

February 2023 | Report No. **23-019**

Note on Confidential Findings

A separate report references confidential information. Pursuant to Standard 9.61 of the U.S. Government Accountability Office's *Government Auditing Standards*, certain information was omitted from this report because that information was deemed to present potential risks related to public safety, security, or the disclosure of private or confidential data. 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.

Auditors made recommendations in the confidential report to address the issues identified during this audit. The Office agreed with the recommendations.

Ratings Definitions

Auditors used professional judgment and rated the audit findings identified in this report. The issue ratings identified for each chapter were determined based on the degree of risk or effect of the findings in relation to the audit objective(s).

PRIORITY: Issues identified present risks or effects that if not addressed could ***critically affect*** the audited entity's ability to effectively administer the program(s)/function(s) audited. Immediate action is required to address the noted concern(s) and reduce risks to the audited entity.

HIGH: Issues identified present risks or effects that if not addressed could ***substantially affect*** the audited entity's ability to effectively administer the program(s)/function(s) audited. Prompt action is essential to address the noted concern(s) and reduce risks to the audited entity.

MEDIUM: Issues identified present risks or effects that if not addressed could ***moderately affect*** the audited entity's ability to effectively administer the program(s)/function(s) audited. Action is needed to address the noted concern(s) and reduce risks to a more desirable level.

LOW: The audit identified strengths that support the audited entity's ability to administer the program(s)/function(s) audited or the issues identified do not present significant risks ***or*** effects that would negatively affect the audited entity's ability to effectively administer the program(s)/function(s) audited.

For more on the methodology for issue ratings, see Report Ratings on page 8.

LOW

Chapter 1
Data Loss Prevention

The Office established adequate data loss prevention controls.

Data Loss Prevention. The Office's data loss prevention (DLP) system blocked the transmission of emails with certain unencrypted confidential data from leaving its email system. The DLP system generated alerts when the system rules were violated, and the Office followed its policies and procedures when it responded to those alerts. Additionally, the Office tested certain rules each month to help verify that the DLP system properly alerted the Office to rule violations.

Encryption. The Office complied with applicable requirements to encrypt confidential data stored on portable computing devices. The Office encrypted the hard drives of its portable devices (laptops and tablets) using a method that exceeded the requirements in the Department of Information Resources' *Security Control Standards Catalog*.

Appendix

Objective, Scope, and Methodology

Objective

The objective of this audit was to determine whether the Office of the Comptroller of Public Accounts (Office) implemented information system security standards and related controls to help ensure that confidential data in the agency's possession is secure.

Scope

The scope of this audit covered certain Office-wide general controls and certain system controls related to specific Office systems that contained some form of confidential data from September 1, 2021, to October 31, 2022. The scope also included a review of significant internal control components related to securing the Office's confidential data.

The following members of the State Auditor's staff performed the audit:

- Michael Yokie, CISA (Project Manager)
- Cody Bogan, CFE (Assistant Project Manager)
- Bria Freeland
- Allison Fries, CFE
- Alexander Grunstein, CFE, CFCS, CCII
- Alex Lukose, MBA
- Robert G. Kiker, CFE, CGAP (Quality Control Reviewer)
- James Timberlake, CIA, CFE (Audit Manager)

Methodology

We conducted this performance audit from July 2022 through February 2023 in accordance with generally accepted government auditing standards. Those 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 findings and conclusions based on our audit objectives. In addition, during the audit, matters not required to be reported in accordance with Government Auditing Standards were communicated to Office management for consideration.

Addressing the Audit Objective

During the audit, we performed the following:

- Interviewed Office management and staff to gain an understanding of the controls and processes used to secure the Office's systems that process and store confidential data.
- Identified the relevant criteria:
  - Texas Administrative Code, Title 1, Chapter 202.
  - Department of Information Resources' *Security Control Standards Catalog,* Version 2.0.
  - The Office's policies and procedures.
- Tested certain Office-wide general information technology controls, including logical access, security monitoring, information technology risk assessment, and data loss prevention.
- Tested certain system-specific information technology controls over logical access, authentication, change management, and event log management.

Figure 1 shows the populations and samples selected for testing.

Figure 1

Populations and Samples Selected for Testing the Office's Systems

Description	Population	Sample Size	Sampling Methodology	Representative Determination
Data Loss Prevention (DLP) system alerts	973	25 random, 1 risk-based	Nonstatistical Random [a] and Risk-Based [b, c]	Not Representative
DLP system rules	24	5	Risk-Based [b, d]	Not Representative
Retired laptops and tablets	709	25	Nonstatistical Random [a]	Representative

[a] A nonstatistical random sample is representative. This sample design was chosen so the sample could be evaluated in the context of the population. It would be appropriate to project those test results to the population, but the accuracy of the projection cannot be measured.

[b] A risk-based sample is not representative, and it would not be appropriate to project those test results to the population.

[c] Population selected to ensure review of alerts categorized as "high" risk.

[d] Population selected to ensure review of rules that included blocking of emails.

Sources: Office systems including the ServiceNow asset management system, Symantec DLP system, and Centralized Accounting and Payroll/Personnel System.

Data Reliability and Completeness

Auditors (1) observed the Office staff extract requested data populations, (2) reviewed the code, queries, and report parameters used to extract the data, (3) analyzed the populations, including reviewing key fields for validity, reasonableness, and completeness, and (4) reviewed user access. Auditors determined that the following populations were sufficiently reliable for the purposes of the audit:

- Populations of leased laptop and tablet computers from the ServiceNow system and Office-owned laptop and tablet computers from the CAPPS system.
- Population of alerts generated by the DLP system for October 2022.

Report Ratings

In determining the ratings of audit findings, auditors considered factors such as financial impact; potential failure to meet program/function objectives; noncompliance with state statute(s), rules, regulations, and other requirements or criteria; and the inadequacy of the design and/or operating effectiveness of internal controls. In addition, evidence of potential fraud, waste, or abuse; significant control environment issues; and little to no corrective action for issues previously identified could increase the ratings for audit findings. Auditors also identified and considered other factors when appropriate.

Copies of this report have been distributed to the following:

Legislative Audit Committee

The Honorable Dan Patrick, Lieutenant Governor, Joint Chair

The Honorable Dade Phelan, Speaker of the House, Joint Chair

The Honorable Joan Huffman, Senate Finance Committee

The Honorable Robert Nichols, Member, Texas Senate

The Honorable Greg Bonnen, House Appropriations Committee

The Honorable Morgan Meyer, House Ways and Means Committee

Office of the Governor

The Honorable Greg Abbott, Governor

Office of the Comptroller of Public Accounts

The Honorable Glenn Hegar, Comptroller of Public Accounts

Ms. Lisa Craven, Deputy Comptroller, Chief Clerk, and Chief of Staff

This document is not copyrighted. Readers may make additional copies of this report as needed. In addition, most State Auditor's Office reports may be downloaded from our website: https://sao.texas.gov.

In compliance with the Americans with Disabilities Act, this document may also be requested in alternative formats. To do so, contact our report request line at (512) 936-9500 (Voice), (512) 936-9400 (FAX), 1-800-RELAY-TX (TDD), or visit the Robert E. Johnson Building, 1501 North Congress Avenue, Suite 4.224, Austin, Texas 78701.

The State Auditor's Office is an equal opportunity employer and does not discriminate on the basis of race, color, religion, sex, national origin, age, or disability in employment or in the provision of services, programs, or activities.

To report waste, fraud, or abuse in state government, visit: https://sao.fraud.texas.gov.