COUNTY OF SACRAMENTO

DEPARTMENT OF FINANCE - AUDITOR-CONTROLLER DIVISION – INTERNAL AUDIT UNIT

INTERNAL AUDIT REPORT

DEPARTMENT OF TECHNOLOGY

INFORMATION TECHNOLOGY SECURITY

JULY 1, 2020 TO OCTOBER 7, 2021

SACRAMENTO COUNTY

Audit Committee Submittal Date: 03/18/2022

SUMMARY

Background

The Department of Technology (DTech) provides central information technology (IT) and telecommunications service for Sacramento County employees, departments and regional partners. DTech is responsible for the County-wide area network that connects all County departments; operates the County Voice over IP Telephone system; supports the County's human resources and financial systems, property tax system, geographical information system and criminal justice information system; operates the County communications center and data center; and manages the public safety Sacramento Regional Radio Communications System, the County's web portals and e-government program.

The Sacramento Countywide Risk Assessment Study assessed DTech's IT security as a high risk area for the Sacramento County operation. Accordingly, we conducted this performance audit to evaluate DTech's IT Security Controls.

Audit Objective

The objectives of the audit are to identify and assess key processes and controls related to IT security and evaluate whether procedures and controls are in place.

Summary

There were two exceptions noted after reviewing the IT security controls. The findings noted were for server access and system access.

Department of Finance
Ben Lamera
Director

Auditor-Controller Division
Joyce Renison
Assistant Auditor-Controller

County of Sacramento

February 25, 2022

Rami Zakaria, Chief Information Officer
Sacramento County Department of Technology
799 G Street
Sacramento, CA 95814

The Sacramento County Department of Technology (DTech) Information Technology (IT) security was identified by the Countywide Risk Assessment as a high risk area. Accordingly, we audited DTech's controls over IT Security to verify whether there is proper IT security control protocols and contingency plan in case of data breach or loss.

We conducted this performance audit 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 objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Our audit was conducted to assess and identify DTech's key processes and controls for Countywide IT Security and design tests to verify that key controls are in place.

Management is responsible for the design, implementation and maintenance of effective internal controls to ensure compliance with federal and state regulatory requirements. Management is also responsible for maintaining effective and efficient internal controls to safeguard County assets, networks and data.

The scope of our audit included DTech IT security controls from July 1, 2020 to October 7, 2021.

We conducted a survey of the internal control environment and identified key controls related to Countywide IT Security in the following areas:

- Management oversight: We reviewed the policies relating to security risk, training, vendors and network inventory with DTech and noted they have policies in place. We also tested whether County employees signed the security and awareness document. We also selected two vendor contracts for review for reasonableness.

- Security Design: We reviewed IT security risk analysis performed by DTech, the security penetration test reports in June 2020 and May 2021 and related findings and recommendations and whether DTech had addressed the security penetration test findings and recommendations. We reviewed the list of IT assets and had DTech verify each IT asset had a department responsible for it and a replacement value as part of DTech's IT security contingency plan. We reviewed DTech's draft Information Technology Security Manual (ITSM) Control Family 3.6 Contingency Planning policy prepared by DTech and confirmed whether the policies were in place.

- Logical Security: We verified with DTech that the network connection has been classified as trusted per the National Institute of Standards and Technology (NIST). We obtained and reviewed a copy of the County Network's demilitarized zone (DMZ) architecture and confirmed with DTech that it was appropriate per the NIST standards. We had DTech confirm that services accessed from outside connections are classified into appropriate trust zones and segmented appropriately and protocols for both inward and outward services have been identified. We had DTech verify all physical access points to the information assets have been identified.

- Hardened System: We reviewed access roles and category schemes with DTech. We randomly reviewed ten employees' IT access and checked whether their access corresponded with their assigned roles. We also reviewed whether the access privileges granted to employees are restrictive enough and follow the principle of least privilege.

- Segregation of Duties: We reviewed the perimeter security strategy and the access control policy with DTech and confirmed the policy was in place.

- Intrusion Detection: We confirmed with DTech that it has host-based and network-based intrusion detection schemes in place. We reviewed DTech's Contingency plan including security incident response plan, post-incident report, draft ITSM Control Family 3.6 Contingency Planning policy and draft system and integrity policy. We noted that DTech followed its own protocol to respond to a security breach occurred in June 2021.

- Security Assessments: We reviewed the 2020 and 2021 security penetration reports and noted that the findings have been addressed. We reviewed how the results are communicated to management and staff and how it gets incorporated into a change plan. We also reviewed the penetration test process and outline document and confirmed that a process is in place.

However, we did not perform specific tests to identify any weaknesses and vulnerabilities of the IT security system as DTech has contracted outside vendors to perform such tests in 2020 and 2021. Accordingly, the audit is not designed to identify any weaknesses and vulnerabilities of DTech's IT security system.

Based on our audit, there were two exceptions noted related to Countywide IT Security. See ATT I, *Findings and Recommendations.*

DTech's response to the findings identified during our engagement are described in ATT I, Current Findings and Recommendations. We did not perform procedures to validate DTech's responses to the findings and accordingly, we do not express an opinion on the responses to the findings.

This report is intended solely for the information and use of the Sacramento County Board of Supervisors, those charged with governance, Sacramento County Audit Committee, Sacramento County Executive, and DTech's management, and should not be used for any other purpose. It is not intended to be, and should not be, used by anyone other than these specified parties. However, this report is a matter of public record and its distribution is not limited.

Sincerely,

BEN LAMERA
DIRECTOR OF FINANCE

By: Hong Lun (Andy) Yu, CPA
Audit Manager

ATT I: *Findings and Recommendations*

ATT I

County of Sacramento
Sacramento County Department of Technology
Information Technology Security
Findings and Recommendations

FINDINGS AND RECOMMENDATIONS

1. Server Access

Condition
County information system users can access privileged functions on servers utilizing non-privileged accounts and access to these privileged functions are not adequately logged.

Criteria
Non-privileged users should be prevented from executing privileged functions and the execution of privileged functions should be logged to conform to the National Institute of Standards and Technology (NIST) Cybersecurity Framework for the access control category and to comply with the draft Information Technology Security Manual (ITSM) Control Family: Access Control County policy sections AC-6(9) and AC-6(10).

Effect
Controlling and monitoring privileged access and actions reduces the exploitable threat surface and allows for detection and tracking of unauthorized actions. Additionally, it facilitates the principle of least privilege, which states that users, programs, and processes should only have the necessary privileges to complete their tasks.

Recommendation
We recommend Department of Technology (DTech) approve a written policy that requires information system users to log all privileged actions and access activity to a centralized solution. We also recommend that DTech utilize privileged access management systems or equivalencies to manage, monitor and audit these actions.

Management's Response
The Department of Technology has completed the development of the Information Technology Security Manual, which is supported by the County Information Security Policy #3000. Sections AC-6(9) and AC-6(10) of this manual require County information systems to log privileged actions and access activity. Furthermore, DTech has operationalized the utilization of a Privileged Access Management system from BeyondTrust and a security and event information management (SIEM) system from Splunk. An account and systems analysis will be conducted to ensure adequate coverage of these controls to bring non-compliant accounts and systems into

compliance. Additionally, associated standards and procedures will be developed to ensure proper onboarding of server access.

2. Timely Removal of Departed Employees

Condition

Of the ten samples tested, we noted one instance where an employee who had departed was not removed from the system within a week of departure and still had access to County email and intranet. Currently this is a manual process where a manager has to actively inform DTech to remove the departed employee from the system.

Criteria

Per ITSM Control Family 3.1 Access Control: Account Management, DTech should be notified within 24 hours if an employee is terminated or transferred or within one week when an account is no longer required or system usage or need-to-know changes need to be made.

Effect

Not removing or changing former employee's access in a timely manner allows an opportunity to steal or compromise data or cause damage to the organization.

Recommendation

We recommend DTech create an automated process where they receive a notification anytime there is a change to prevent anyone from being overlooked.

Management's Response

The Department of Technology has completed the development of the Information Technology Security Manual, which is supported by the County Information Security Policy #3000. Sections AC-2 of the manual require the timely management of accounts when an employee is terminated or transferred. Associated standards and procedures will be developed to ensure proper account management under these conditions. Additionally, technical solutions will be evaluated to allow for the automation of these actions.