County of San Diego Auditor and Controller

OFFICE OF AUDITS & ADVISORY SERVICES

GENERAL IT COMPUTING CONTROLS – SHERIFF

FINAL REPORT

Chief of Audits: Juan R. Perez
Audit Manager: Lynne Prizzia, CISA, CRISC
Senior Auditor: Christopher Ellis, CISA, CISSP
Auditor II: Rani Gorgis, CPA

Report No. A17-002

May • 2018

Intentionally Left Blank

County of San Diego

TRACY M. SANDOVAL
DEPUTY CHIEF ADMINISTRATIVE OFFICER/
AUDITOR AND CONTROLLER

AUDITOR AND CONTROLLER
OFFICE OF AUDITS & ADVISORY SERVICES
5530 OVERLAND AVENUE, SUITE 330, SAN DIEGO, CA 92123-1261
Phone: (858) 495-5991

JUAN R. PEREZ
CHIEF OF AUDITS

May 22, 2018

TO: William D. Gore, Sheriff
Office of the Sheriff

FROM: Juan R. Perez
Chief of Audits

FINAL REPORT: GENERAL IT COMPUTING CONTROLS

Enclosed is our report on the General IT Computing Controls. We have reviewed your response to our recommendations and have attached it to the audit report.

The actions taken and/or planned, in general, are responsive to the recommendations in the report. As required under Board of Supervisors Policy B-44, we respectfully request that you provide quarterly status reports on the implementation progress of the recommendations. You or your designee will receive email notifications when these quarterly updates are due, and these notifications will continue until all actions have been implemented.

If you have any questions, please contact me at (858) 495-5661.

JUAN R. PEREZ
Chief of Audits

AUD:CJE:nb

Enclosure

c: Ronald Lane, Deputy Chief Administrative Officer, Public Safety Group
Tracy M. Sandoval, Deputy Chief Administrative Officer/Auditor and Controller
Rosemarie Degracia, Group Finance Director, Public Safety Group

INTRODUCTION

Audit Objective

The Office of Audits & Advisory Services (OAAS) completed an audit of the Sheriff's Department General IT Computing Controls. The objective of the audit was to assess the design and operating effectiveness of the general computer controls that relate to the IT environment in which application systems are developed, maintained, and operated.

Background

The Sheriff's Department is the chief law enforcement agency in the County of San Diego, covering over 4,200 square miles. The Sheriff, elected by the residents of San Diego County, is the chief executive of the department. The department is comprised of seven detention facilities as well as seven patrol stations, seven patrol substations, a crime laboratory, and an array of support operations necessary to provide full law enforcement coverage for the County of San Diego. The department's approximately 4,300 employees provide general law enforcement, detention, and court security services, as well as regional investigative support and tactical emergency response. Law enforcement services are provided to 928,000 county residents, including those in nine contract cities. The department is responsible for booking and releasing inmates, ensuring court appearances, and providing necessary daily care for about 5,100 inmates per day. The Sheriff's detention facilities conduct approximately 82,500 unduplicated inmate bookings annually. Services provided to the San Diego Superior Court include weapons screening and courtroom security. The department also serves as the County's levying and enforcement agency for execution, service and return of all writs, warrants and temporary restraining orders.[1]

The Sheriff's Data Services Division maintains an extranet known as SDLaw that was developed in-house, and is used by State, Federal and local law and justice agencies in the County. The SDLaw extranet is a private law and justice web-based system. Many important applications run on the Sheriff's extranet including eJIMS, which is a portal into the Sheriff's Jail Information Management System (JIMS), and eWarrants among others. eJIMS provides real time information on inmates including bookings, arrests, charges, mug shots, court appearances, charge dispositions, release dates and types, and the current location of the inmate. Authorized personnel can view booking history and personal data on the inmate. The eWarrants application provides a high speed, near-real time search for warrants, and restraining orders in the San Diego County Officer Notification System (ONS). eWarrants gives users the ability to search for warrants based on name and number or location, such as a street address. This allows local police departments to plan and execute warrant sweeps.

Due to the highly sensitive nature of the Criminal Justice Information (CJI) contained and accessible through the extranet, the Sheriff must comply with the Criminal Justice Information Services (CJIS) Security Policy

[1] "Public Safety Group Adopted Operational Plan Fiscal Years 2016–17 And 2017–18"

developed by the U.S. Department of Justice (DOJ).

The CJIS Security Policy provides appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity with access to, or who operate in support of, criminal justice services and information. The Policy is presented at both strategic and tactical levels and is periodically updated to reflect the security requirements of evolving business models.[2]

The Sheriff's IT environment includes approximately: 100 work sites, 3,500 workstations, 400 servers, 600 mobile data computers within patrol cars, 1,800 iPhones, 6 computer rooms (small datacenters), and 2 datacenters (Primary & Backup).

Audit Scope & Limitations

The scope of the audit covered FY 2016-17 to current and included an assessment of the design and operating effectiveness of the general computer controls that relate to the IT environment in which application systems are developed, maintained, and operated.

This audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing prescribed by the Institute of Internal Auditors as required by California Government Code, Section 1236.

Methodology

OAAS performed the audit using the following methods:

- Interviewed Sheriff Data Services Division management and staff regarding IT environment and controls.
- Reviewed CJIS Security Policy.
- Reviewed department policies and procedures in regards to security, incident response, logical and physical access, and change management.
- Evaluated the internal IT control structure against Control Objectives for Information and Related Technologies (COBIT) and the CJIS Security Policy.
- On a sample basis, reviewed physical access to Sheriff's facilities, logical access to the SDLaw extranet, data encryption, security logging and monitoring, and digital media disposal.

[2] "Criminal Justice Information Services (CJIS) Security Policy"; CJIS Information Security Officer; 2017

Audit Results

Summary

Within the scope of the audit, the adequacy of the design and operating effectiveness of the general computer controls that relate to the IT environment in which application systems are developed, maintained, and operated were generally effective. Several opportunities for improvement were identified including lack of periodic reviews for badge reader access, and CJI at rest passphrase length below the minimum character limit required by CJIS Security Policy.

Finding I: **Periodic Review & Badge Access Oversight Needs Improvement**

OAAS determined that periodic reviews of badge readers that give personnel access to the Sheriff's Data Center, IT offices, and equipment rooms are not currently being performed by the Sheriff's Data Services Division. OAAS identified one (1) of 30 sampled workers that should no longer have access to Sheriff's facilities. The individual was a special agent from the FBI that had been given access to Sheriff's facilities for an investigation. When the access was no longer needed it remained active until OAAS identified it during audit testing.

The County's Facilities Management issues badges, and manages access to badge readers for the Sheriff and all County departments. They follow an off-boarding process to remove workers' badge access when they are separated from the County or change departments. Facilities Management relies on department contacts to notify them if a worker has separated or needs a change in their access. In this case, it appears that no one notified Facilities Management after the worker's assignment had been completed and access was no longer needed.

The CJIS Security Policy 5.9.1.2 Physical Access Authorizations states, "The agency shall develop and keep current a list of personnel with authorized access to the physically secure location." Failure to periodically review physical access to facilities may lead to inappropriate access and non-compliance with CJIS Security Policy.

Recommendation: The Sheriff should perform periodic reviews of workers with physical access to Sheriff's facilities in order to detect unauthorized access.

Finding II: **CJI At Rest Minimum Passphrase Length Needs Improvement**

The Sheriff encrypts their removable data drives (external hard drives, flash/thumb drives, etc.) using BitLocker. During the encryption testing for CJI at rest, OAAS determined the passphrase minimum length within BitLocker is set to eight characters, rather than ten as required by CJIS Security Policy 5.10.1.2.2 Encryption for CJI at Rest.

Using a passphrase minimum length of eight characters, rather than the required ten, makes the passphrase more vulnerable to brute force attacks, and increases the risk of a data breach of the CJI. Additionally, the Sheriff is out of compliance with CJIS Security Policy in regards to encryption for CJI at rest.

The passphrase minimum length is set to eight characters by default in most encryption software including BitLocker. It appears this was never updated to be in alignment with the CJIS Security Policy requirement during the initial setup.

Recommendation: The Sheriff should change the CJI at rest minimum passphrase length of eight characters to be in alignment with the CJIS Security Policy requirement of ten characters.

DEPARTMENT'S RESPONSE
(OFFICE OF THE SHERIFF)

COUNTY OF SAN DIEGO

INTER-DEPARTMENTAL CORRESPONDENCE

May 14, 2018

TO: Juan R. Perez
Chief of Audits

FROM: William D. Gore, Sheriff
Office of the Sheriff

DEPARTMENT RESPONSE TO AUDIT RECOMMENDATIONS: GENERAL IT COMPUTING CONTROLS

Finding I: Periodic Review & Badge Access Oversight Needs Improvement

OAAS Recommendation: OAAS determined that periodic reviews of badge readers that give personnel access to the Sheriff's Data Center, IT offices, and equipment rooms are not currently being performed by the Sheriff's Data Services Division.

Action Plan: The Sheriff's Data Services Division agrees with the OAAS recommendation that Sheriff's personnel should perform periodic reviews of workers physical access to Sheriff's facilities in order to detect unauthorized access. The Sheriff's Data Services Division will work with San Diego County General Services Electronic Security Group to enable Sheriff's staff to have access to badge reader servers to review personnel access settings.

Planned Completion Date: July 31, 2018

Contact Information for Implementation: Keith Fernandez, Supervising IT Engineer

Finding II: CJI at Rest Minimum Passphrase Length Needs Improvement

OAAS Recommendation: The Sheriff should change the CJI at rest minimum passphrase length of eight characters to be in alignment with the CJIS Security Policy requirement of ten characters.

Action Plan: The Sheriff's Data Services Division agrees with the OAAS recommendation that Sheriff's personnel should increase the passphrase length from eight characters to ten characters to be in alignment with CJIS Security Policy requirements. This change will be put in place through policy changes controlled by the Sheriff's Data Services Division.

Planned Completion Date: July 31, 2018

Contact Information for Implementation: Keith Fernandez, Supervising IT Engineer

If you have any questions, please contact Ashish Kakkad, Chief Information Officer at (858) 692-9089.

William D. Gore, Sheriff

WG/db