County of San Diego

Auditor and Controller

OFFICE OF AUDITS & ADVISORY SERVICES

WORKSITE & SYSTEMS ACCESS, SAFETY, AND SECURITY CONTROLS

FINAL REPORT

Chief of Audits: Juan R. Perez
Audit Manager: Laura R. Flores, CIA, CFE, CGAP
Senior Auditor: Ronald Cosey, CGAP

Report No. A19-010

November • 2020

Intentionally Left Blank

County of San Diego

TRACY DRAGER
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

November 2, 2020

TO: Brian Albright, Director
Department of Parks and Recreation

FROM: Juan R. Perez
Chief of Audits

FINAL REPORT: WORKSITE & SYSTEMS ACCESS, SAFETY, AND SECURITY CONTROLS AUDIT

Enclosed is our report on the Worksite & Systems Access, Safety, and Security Controls Audit. As there are no findings and recommendations in the report pertaining to your department, no audit response is required.

Thank you for the courteousness and cooperation extended to the Office of Audits & Advisory Services during the course of the audit.

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

JUAN R. PEREZ
Chief of Audits

AUD:RC:nb

Enclosure

c: Sarah Aghassi, Deputy Chief Administrative Officer, Land Use and Environment Group
Tracy Drager, Auditor and Controller
Renee Loewer, Group Finance Director, Land Use and Environment Group

County of San Diego

TRACY DRAGER
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

November 2, 2020

TO: Dr. Luke Bergmann, Director
Health and Human Services Agency – Behavioral Health Services

FROM: Juan R. Perez
Chief of Audits

FINAL REPORT: WORKSITE & SYSTEMS ACCESS, SAFETY, AND SECURITY CONTROLS AUDIT

Enclosed is our report on the Worksite & Systems Access, Safety, and Security Controls Audit. 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:RC:nb

Enclosure

c: Dean Arabatzis, Acting Director and General Manager, Health and Human Services Agency
Tracy Drager, Auditor and Controller
Andrew Pease, Acting Chief Operating Officer, Health and Human Services Agency
Amy Thompson, Acting Group Finance Director, Health and Human Services Agency

County of San Diego

TRACY DRAGER
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

November 2, 2020

TO: Marko Medved, Director
Department of General Services

FROM: Juan R. Perez
Chief of Audits

FINAL REPORT: WORKSITE & SYSTEMS ACCESS, SAFETY, AND SECURITY CONTROLS AUDIT

Enclosed is our report on the Worksite & Systems Access, Safety, and Security Controls Audit. 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:RC:nb

Enclosure

c: Ebony Shelton, Deputy Chief Administrative Officer/Chief Financial Officer
Tracy Drager, Auditor and Controller
Rissa Japlit, Assistant Group Finance Director, Finance and General Government Group

County of San Diego

TRACY DRAGER
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

November 2, 2020

TO: Jeff Toney, Director
Office of Emergency Services

FROM: Juan R. Perez
Chief of Audits

FINAL REPORT: WORKSITE & SYSTEMS ACCESS, SAFETY, AND SECURITY CONTROLS AUDIT

Enclosed is our report on the Worksite & Systems Access, Safety, and Security Controls Audit. 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:RC:nb

Enclosure

c: Holly Porter, Deputy Chief Administrative Officer, Public Safety Group
Tracy Drager, Auditor and Controller
Rosemarie Degracia, Group Finance Director, Public Safety Group
Karina Galvan, Assistant Group Finance Director, Public Safety Group

INTRODUCTION

Audit Objective

The Office of Audits & Advisory Services (OAAS) completed an audit of Worksite & Systems Access, Safety and Security Controls. The objective of the audit was to evaluate the process in place to prevent unauthorized access for non-permanent employees and third-party vendor personnel, and to ensure the safety and security of County facilities.

Background

The County of San Diego (County) Administrative Manual (Admin Manual) Item No. 0040-06 requires that all permanent, temporary, and seasonal employees, volunteers, and contractors be issued and display a County identification/access card (ID card) while on duty. These cards are used to access County facilities and/or as identification. The Department of General Services (DGS), Office of Security Services issues ID cards through the CardAccess 3000 application (CardAccess). While some departments have been given access to this application to manage their employees' ID cards, DGS is still responsible for issuing the cards. The Probation Department, District Attorney, and the Sheriff's Department also issue ID cards on the same system, but under their own control and purview.

According to DGS Policy No. 3.1.6.4, anyone performing duties under an existing service contract must be acceptable to the County, including all contract employees and others who might have access to County facilities without the supervision of a County employee. Contractors and associated staff must complete and pass a security screening by the Sheriff's Department (Background Division), California Department of Justice and Federal Bureau of Investigations before being issued an ID card permitting independent entry into County facilities.

County Admin Manual Item No. 0400-03 establishes requirements for managing access to information systems, including desktop and cloud-based applications. A desktop application runs stand alone on a desktop or laptop computer and can only be accessed at the computer where it is installed. In contrast, a cloud-based application is a piece of software that lives in and operates from the "cloud"; a server that is located remotely. All a user needs to access a cloud-based application is an internet browser, which is why these applications are accessible from any desktop, laptop, tablet, smartphone, or internet enabled device. The County Technology Office maintains a catalog of the cloud-based applications that are being used by each County department.

In December 2015, the Chief Administrative Officer authorized a comprehensive review of security protocols at all County owned and occupied facilities. The purpose of this review was to enhance security at County facilities with the ultimate goal of protecting County workers, County property, and the public who utilize County facilities. The Security Initiative that emerged involves prevention, deterrence, and mitigation. The Security Initiative is governed by Admin Manual Item No. 0050-02-

09, County Security Policy, which established oversight responsibility to the Office of Emergency Services (OES).

Audit Scope & Limitations

The scope of the audit included a review of physical access to all County facilities for permanent, temporary and seasonal employees, volunteers and contractors; security clearance for third-party access and authorization of employee access to County facilities, information systems access to cloud-based applications; emergency safety maintenance requests for Fiscal Years 2017-18 and 2018-19; and the County's Security Initiative.

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:

- Reviewed policies and procedures and related control activities over employee and contractor access to cloud-based information system applications.
- Reviewed policies and procedures and related control activities over employee and contractor physical access to County facilities.
- Obtained a report of terminated employees from PeopleSoft and compared it to a report of employees with enabled ID cards from CardAccess by employee number.
- On a sample basis, conducted the following:
    - Compared contractor's rosters with a list of contract employees' enabled ID cards from CardAccess.
    - Inspected the security screening packages of contract employees.
    - Tested temporary and contract employees' ID card expiration dates.
    - Evaluated the reasonableness of emergency maintenance requests and reviewed the associated efforts of maintaining the service level.
- Reviewed the process design of the County Security Initiative.

AUDIT RESULTS

Summary

Within the scope of the audit, we identified the following areas for improvement: (i) preventing physical access for permanent/non-

permanent employees and third-party vendor personnel that terminate employment or no longer work at a County facility; (ii) removing information systems access to applications for permanent/non-permanent employees and third-party vendor personnel that terminate employment or no longer work at a County facility; and (iii) designing complete processes to ensure compliance with the County Security Policy. We listed our observations and suggestions for improvements in the findings and related recommendations below.

Finding I: Systems Access Had Not Been Removed for Employees That Terminated Employment

We conducted a review of employees' access to cloud-based applications software. Our testing was conducted on the following sample:

Table 1. Departments and Applications Selected for Testing

Department	Application	Description
General Services	Tririga10	Real estate and facilities management
	CardAccess 3000	Physical access management
Office of Emergency Services	WebEOC	Crisis coordination system
	BlueJeans	Emergency communication system
Behavioral Health Services	Cerner Electronic Health Records	Health records management
Parks and Recreation	ArtStreet	Park registration system

Our review revealed the following:

Department of General Services (DGS)

Of 80 employees with administrative access to CardAccess, DGS had not removed access for 4 users, because respective departments that use CardAccess to manage ID cards for their department are not consistently notifying the System's Administrator when the administrative users terminate employment.

Of the 769 employees with user access to the Tririga10 application, DGS had not removed access for 5 terminated employees. The 5 employees were deceased.

Tririga has an automated workflow that interfaces with PeopleSoft to identify terminated employees and remove their access. Terminated employees' job status descriptions include: "Terminated", "Retired", and "Deceased". The workflow has a script that reads the job status in PeopleSoft for all active users in Tririga. The script in the workflow removes any user's access with a "Terminated" or "Retired" job status in PeopleSoft. However, the script does not include "Deceased" job status as an indicator for access removal. Therefore, any users with a "Deceased" job status in PeopleSoft retained their access to the Tririga10 application.

Office of Emergency Services (OES)
Of the 604 County employees with user access to the WebEOC application, OES had not removed access for 11 terminated employees.

Respective departments that use the WebEOC application are not consistently notifying the System's Administrator when employees terminate employment.

Behavioral Health Services (BHS)
Of the 561 County employees with user access to the Cerner application, BHS had not removed access for 3 terminated employees.

BHS terminates user access to Cerner after 90 days of inactivity. However, 1 of the 3 terminated employees still had access beyond 90 days of termination. The 90-day mark had not come yet for the other 2 terminated employees. A Cerner user can maintain his/her access if the user signs-in into the account and is active after termination.

All County information systems access must be promptly terminated at the time that a user ceases to provide services to the County or when a user's employment status or duties change in accordance with County Admin Manual Item 0400-03, Computer Accounts - Management and Use. Otherwise, the risk of unauthorized use of information and access to the department's information systems is increased.

Recommendation: DGS Management should:

1. Develop a formal process to ensure that respective departments inform the System's Administrator of CardAccess when their administrative users terminate employment.

2. Revise the Tririga10 application workflow script to read the "employees termination date" in the PeopleSoft file instead of the "job status description" to identify terminated employees and remove their access.

OES Management should:

1. Review user access periodically and disable access for users that no longer require access to the application based on their responsibilities.

2. Consider enabling the control in WebEOC that removes user's access after a period of inactivity.

BHS Management should:

1. Review user access quarterly and disable access for users that no longer require access to the Cerner application based on their responsibilities.

Finding II: **Terminated Employees Had Enabled ID Cards**

We reviewed employees' physical access to County facilities and found the following:

Our comparison of terminated employees from Peoplesoft with employees that had enabled ID cards from CardAccess identified 1,251 terminated employees with enabled ID cards; 1,215 of them were regular employees and 36 were temporary employees.

When an employee transfers to another County department, the receiving department requests a new ID card in advance to ensure it is ready for use on the first day of work. The employee also needs to keep the ID card assigned by the department that he/she is transferring from until the last day of work at that department. According to DGS Office of Security Services' staff, an expiration date should be entered in the CardAccess system for these cards, so they can be deactivated after the employees' last day in the department. However, DGS staff has not consistently entered an expiration date in the system as there is no formal policy as a directive.

As a result, the ID cards from departments employees have transferred from are still enabled in the system, which increases the risk that unauthorized individuals may continue to access worksite facilities after leaving departments and terminating employment with the County.

The Department of Human Resources Policy No. 302 – Separation Event Process, requires departments to notify DGS, Office of Security Services of a status change on or before the last day of work in the current job, and return the ID card within five days of the separation event. Furthermore, each department is responsible for the collection of ID cards from all employees who leave County service or have a change in department, in accordance with Admin Manual Item 0040-06, County Identification Card Program.

Recommendation: DGS, Office of Security Services Management should:

1. Develop and implement written procedures that outline requirements to enter an expiration date in the CardAccess system for ID cards that are being temporarily used until employees' new cards are activated.

2. Communicate these procedures to staff responsible for managing ID cards and periodically monitor for compliance.

Finding III: **ID Cards of Terminated Contract Employees Were Not Deactivated**

We reviewed the adequacy of physical access to County facilities for contract employees. Our sample focused on janitorial contracts due to the large number of employees with access to County facilities. We selected a judgmental sample of 2 out of 38 janitorial contractors to include T&T Janitorial and Nova Commercial.

Of the 222 T&T Janitorial employees with enabled ID cards, 3 had terminated employment with the contractor. Another 53 staff members had enabled ID cards but were not listed on the contractor's roster of employees that work at County facilities. A representative for the contractor stated that the 53 staff members were in their reserve pool to work at County facilities.

Additionally, 214 of the 453 Nova Commercial employees with enabled ID cards had terminated employment with the contractor. Another 63 staff members had enabled ID cards but were not listed on the contractor's roster of employees that work at County facilities.

According to the contract, contractors have the responsibility for collecting ID cards and returning them to the County when a contract ends or an employee leaves employment. In addition, the contract provides that the County may assess contractors a $100 fee for any ID cards not returned. However, the Contracting Officer's Representatives (COR) were not monitoring their contracts for this particular provision.

As a result, there is an increased risk that unauthorized individuals no longer working for County contractors continue to have access to County facilities or falsely use ID cards to identify themselves as County workers.

Recommendation: DGS Management should ensure that the assigned COR develops a contract monitoring plan that includes activities to enforce all contract provisions, including collection of ID cards and assessing penalty fees when necessary.

Finding IV: **Background Check Documentation for Contract Employees Was Not Always Maintained**

DGS Policy and Procedures No. 3.1.6.4 Contract Service Provider Security Requirements, Section B states the following:

> "Background checks are required for all contract employees before access will be permitted to County facilities/property ... ID badges will only be issued to applicants successfully completing the background investigation process".

We selected a judgmental sample of 25 contract employees to determine whether a background check was performed. The Office of Security Services did not maintain background check documentation for 5 of the 25 contract employees tested, as such we were unable to obtain reasonable assurance that a background check was performed for these employees.

Further, we noted that DGS Contract Service Provider Security Requirements do not address how staff should maintain background check files. If these documents are not properly safeguarded, it increases the risk that unauthorized personnel may obtain inadvertent or illicit access to confidential information.

Recommendation: DGS Management should:

1. Revise the Contract Service Provider Security Requirements Policy to include requirements to properly maintain and safeguard contract employee background check files.

2. Communicate policy changes to staff responsible for managing contract employees' access to County facilities.

Finding V: **ID Cards' Expiration Date for Temporary County Employees and Contract Employees Not Properly Recorded**

Admin Manual Item No. 0040-06, County Identification Access Card Program states the following:

> "Temporary and seasonal employees, contractors and volunteers, will be issued temporary ID cards that have a definite expiration date included on the Identification/Access Card Registration Form".

We selected a judgmental sample of contract employees' ID cards to determine whether an expiration date was recorded in the system. Our test found the following:

Of the 1,480 contract employees tested, 6 had ID cards with no expiration date in the system.

Further, we selected a judgmental sample of 30 County employees to determine whether their ID cards were properly authorized. From our sample of 30 County employees, 6 were temporary employees. Therefore, we reviewed their records to ensure an expiration date was recorded in the system.

While we noted that 3 of the 6 temporary employees had no expiration date listed on the ID Card Registration Form received by the Office of Security Services, an expiration date was entered into the CardAccess system. According to DGS staff, if no expiration date for ID cards of temporary employees is received, it is their practice to enter an expiration date of four years from the date of issuance.

The Office of Security Services has no formalized procedures that provide direction to their staff when the authorizer department does not include an expiration date for temporary employees on the ID Card Registration Form.

Lack of an expiration date on contract employees' or County temporary employees' ID cards, increases the risk that unauthorized individuals no longer working for the County or County contractors continue to have access to County facilities or falsely use ID cards to identify themselves as County workers.

Recommendation: DGS, Office of Security Office Management should:

1. Reject all Identification/Access Card Registration Forms that are not completed in accordance with Admin Manual Item No. 0040-06.

2. Consider automating the ID Card Registration Forms to require the authorizer to include an expiration date if the "Temporary" box for temporary employees is checked on the form.

Finding VI: **Documentation Was Not Always Maintained for the Authorization to Issue ID Cards**

Admin Manual Item No. 0040-06, County Identification Access Card Program requires that the ID Card Registration Form should be signed by each department authorizer before an ID card can be processed by DGS, Office of Security Services.

We selected a judgmental sample of 30 employees whose ID cards were issued between January 2018 to August 2019 and tested whether proper authorization was given before the ID card was issued. Our test revealed that 10 of the 30 employees tested had no ID Card Registration Form on file, because the Office of Security Services did not always obtain and maintain the form. As a result, we were unable to substantiate proper approval.

Recommendation: DGS, Office of Security Management should retrain its staff on the procedures for processing ID cards and the importance of maintaining documentation.

Finding VII: **The Issuance of Visitor Badges Did Not Comply with County Policy**

Admin Manual Item No. 0400-06, County Identification Access Card Program requires DGS to issue temporary ID cards that have a definite expiration date for temporary, seasonal, and volunteer staff. Further, these cards should be handled in the same manner as permanent employees' cards. However, during the review of ID card authorizations, we noted that DGS issued visitors badges to a department for some of its staff instead.

In order to expedite obtaining the necessary ID cards, the department requested visitor badges, because it hires a large number of seasonal and/or volunteer staff that need access to County facilities for a short period of time.

DGS stated that the requesting department has a process in place to monitor visitor badges, however DGS had not reviewed and verified such process. Nevertheless, this process is not in compliance with County policy and may result in reduced staff accountability.

Recommendation:

1. DGS, Office of Security Services Management should determine whether departments have the need for visitor badges, and if so:

a. Recommend revising the Admin Manual Item No. 0040-06 to address the issuance of visitor badges; and,

b. Develop an internal process to issue and monitor the use of visitor badges.

Or,

2. DGS, Office of Security Services Management should:

a. Reject requests for visitor badges; and,

b. Comply with Admin Manual Item No. 0040-06 and only issue temporary ID cards that have a definite expiration date for seasonal and volunteer staff.

Finding VIII: **Additional Processes Needed to Ensure County Security Policy Is Fully Implemented**

We reviewed the County Security Initiative and found that not all the processes had been completely designed to ensure compliance with Admin Manual Item No. 0050-02-09, County Security Policy. For example, the requirement to report the progress of the Security Action Plans (SAP) had not been completely developed. OES had not determined how departments would communicate the progress (e.g., via a document, a meeting, or a systems report) of SAP's. A governance committee was created to help make these types of decisions.

We identified specific areas to consider while OES and the governance committee work out the details of all the processes with the County Security Policy and ensure that they are working as intended.

Recommendation: OES Management and the Governance Committee should consider the following areas when designing the security initiative processes:

- Revise the County Security Policy to ensure that the security of County facilities is reassessed on a 5-year cycle, if that is what the initiative intended.

- Standardize the Vulnerability Assessment format and criteria to ensure instructions to complete assessments are clear, to prevent inconsistencies.

- Clearly define the timeframe to disseminate Vulnerability Assessments to prevent delays in the development of Security Action Plans.

- Ensure confidentiality is maintained during the process of reporting the results of Vulnerability Assessments to the respective departments.

- Design and develop an IT solution that is tailored to the needs of the entire Security Initiative process, including operational functionality, proper approvals, secure storage of documentation, and reporting capabilities.

- Standardize the Security Action Plan format and ensure instructions to complete the action plans are clear to prevent inconsistencies.

- Define clear roles and responsibilities for approving the Security Action Plans and revise the County Security Policy to include clarification, if necessary.

- Consider and address any budget constraints that may impede the progress of security enhancements to facilities.

- Develop a charter for the Governance Committee to define the purpose, roles, and responsibilities of the committee.

DEPARTMENT'S RESPONSE
(BEHAVIORAL HEALTH SERVICES)

County of San Diego

NICK MACCHIONE, FACHE
AGENCY DIRECTOR

HEALTH AND HUMAN SERVICES AGENCY
BEHAVIORAL HEALTH SERVICES
3255 CAMINO DEL RIO SOUTH, MAIL STOP P-531
SAN DIEGO, CA 92108-3806
(619) 563-2700 ▪ FAX (619) 563-2705

LUKE BERGMANN, Ph.D.
DIRECTOR, BEHAVIORAL HEALTH SERVICES

October 19, 2020

TO: Juan R. Perez, Chief of Audits
Auditor and Controller

FROM: Luke Bergmann, Ph.D., Director
Behavioral Health Services

DEPARTMENT RESPONSE TO AUDIT RECOMMENDATIONS: WORKSITE AND SYSTEMS ACCESS, SAFETY, AND SECURITY CONTROLS AUDIT

Finding I: Systems Access Had Not Been Removed for Employees That Terminated Employment

- **OAAS Recommendation:** Review user access quarterly and disable access for users that no longer require access to the Cerner application based on their responsibilities.
- **Action Plan:** Behavioral Health Services (BHS) agree with the audit recommendations. BHS has implemented a process to review user access monthly and disable access for users that no longer require access to the Cerner application based on their responsibilities. The process was executed on September 2, 2020.
- **Planned Completion Date:** September 2, 2020 *(action was already executed)*
- **Contact Information for Implementation:** AnnLouise Conlow, Senior MIS Manager, Behavioral Health Services, (619) 507-6678.

LUKE BERGMANN, Ph.D., Director Digitally signed by LUKE BERGMANN, Ph.D., Director Date: 2020.10.19 16:32:12 -07'00'

LUKE BERGMANN, Ph.D., Director
Behavioral Health Services

LB:jd:bm

DEPARTMENT'S RESPONSE
(DEPARTMENT OF GENERAL SERVICES)

County of San Diego

MARKO MEDVED, PE, CEM
DIRECTOR
(858) 694-2338

DEPARTMENT OF GENERAL SERVICES
5560 OVERLAND AVENUE, SUITE 410, SAN DIEGO, CA 92123

NICOLE J. ALEJANDRE
ASSISTANT DIRECTOR
(858) 694-3885

September 9, 2020

TO: JUAN R. PEREZ, Chief of Audits
Auditor and Controller

FROM: MARKO MEDVED, PE, CEM, Director
General Services

RESPONSE TO AUDIT RECOMMENDATIONS FOR WORKSITE & SYSTEMS ACCESS, SAFETY, AND SECURITY CONTROLS REPORT

Finding I: Systems Access Had Not Been Removed for Employees That Terminated Employment

OAAS Recommendation:

1. Develop a formal process to ensure that respective departments inform the System's Administrator of Card Access when their administrative users terminate employment.

Action Plan: DGS agrees with the recommendation. An electronic form will be developed with an electronic signature that will be used by the various departments to request changes or additions to the administrative user base. DGS Security will develop a quarterly preventive maintenance task in Tririga10 that will prompt the System Administrator to reach out to the various departmental administrative users and verify the employees in the access system are current and correct.

Planned Completion Date: December 18, 2020

Contact Information for Implementation: Charles Gompf, Facility Support Manager
Ken Frederiksen, Facility Support Manager

2. Revise the Tririga10 application workflow script to read the "employees termination date" in the PeopleSoft file instead of the "job status description" to identify terminated employees and remove their access.

Action Plan: DGS partially agrees with the recommendation. DGS will work with application developer and modify the workflow to include the PeopleSoft Employee Status code of

"Deceased (D)" and terminate Tririga account access. This methodology is cost efficient and will accomplish the same objective.

Planned Completion Date: September 12, 2020

Contact Information for Implementation: Christine Wang, IT Principal Analyst

Finding II: Terminated Employees Had Enabled ID Cards

OAAS Recommendation:

1. Develop and implement written procedures that outline requirements to enter an expiration date in the Card Access system for ID cards that are being temporarily used until employees' new cards are activated.

2. Communicate these procedures to staff responsible for managing ID cards and periodically monitor for compliance.

Action Plan: DGS agrees with this recommendation. DGS Security has instituted a ten-business day expiration date for transfers or for employees that have been promoted. DGS Security staff will be trained quarterly on the procedures and the System Administrator will verify compliance.

Planned Completion Date: December 18, 2020

Contact Information for Implementation: Charles Gompf, Facility Support Manager
Ken Frederiksen, Facility Support Manager

Finding III: ID Cards of Terminated Contract Employees Were Not Deactivated

OAAS Recommendation:

1. DGS Management should ensure that the assigned COR develops a contract monitoring plan that includes activities to enforce all contract provisions, including collection of ID cards and assessing penalty fees when necessary.

Action Plan: DGS agrees with this recommendation. The COR for the Security Guard Contract currently meets monthly with the Account Manager for the Security Contractor and verifies employee lists. DGS Security will meet with DPC to craft a recommendation that the COR for each contract follows this example and meets monthly to verify employee lists and contract compliance.

Planned Completion Date: January 8, 2021

Contact Information for Implementation: Charles Gompf, Facility Support Manager
Ken Frederiksen, Facility Support Manager

Finding IV: Background Check Documentation for Contract Employees Not Always Maintained

OAAS Recommendation:

1. Revise the Contract Service Provider Security Requirements Policy to include requirements to properly maintain and safeguard contract employee background check files.

2. Communicate policy changes to staff responsible for managing contract employees' access to County facilities.

Action Plan: DGS agrees with this recommendation. A revised policy regarding background checks will be devised. There are several categories of background investigations that will need to be defined as required by various departments. Some contract county employees have background checks through other agencies, these will be vetted, and a decision made as to their validity.

Planned Completion Date: January 8, 2021

Contact Information for Implementation: Charles Gompf, Facility Support Manager
Ken Frederiksen, Facility Support Manager

Finding V: ID Cards Expiration Date for Temporary County Employees and Contract Employees Not Properly Recorded

OAAS Recommendation:

1. Reject all Identification/Access Card Registration Forms that are not completed in accordance with Admin Manual Item No. 0040-06.

2. Consider automating the ID Card Registration Forms to require the authorizer to include an expiration date if the "Temporary" box for temporary employees is checked on the form.

Action Plan: DGS agrees with this recommendation. DGS will require that all Access/ID Card Registration forms have an expiration date completed. DGS will create an automated form that requires the authorizer to include an expiration date if the temporary box on the form is marked.

Planned Completion Date: January 8, 2021

Contact Information for Implementation: Charles Gompf, Facility Support Manager
Ken Frederiksen, Facility Support Manager

Finding VI: Documentation Was Not Always Maintained for the Authorization to Issue ID Cards

OAAS Recommendation: DGS, Office of Security Management should retrain its staff on the procedures for processing ID cards and the importance of maintaining documentation.

Action Plan: DGS agrees with this recommendation. DGS will provide quarterly training on the procedures for processing ID cards and the importance of maintaining documentation. DGS will create a fully electronic form with e-signature and a corresponding database that will make storage and retrieval of the ID information faster and more accurate.

Planned Completion Date: January 8, 2021

Contact Information for Implementation: Charles Gompf, Facility Support Manager
Ken Frederiksen, Facility Support Manager

Finding VII: The Issuance of Visitor Badges Did Not Comply with County Policy

OAAS Recommendation:

1. DGS, Office of Security Services Management should determine whether departments have the need for visitor badges, and if so:
a. Recommend revising the Admin Manual Item No. 0040-06 to address the issuance of visitor badges; and,
b. Develop an internal process to issue and monitor the use of visitor badges.
Or,
2. DGS, Office of Security Services Management should:
a. Reject requests for visitor badges; and,
b. Comply with Admin Manual Item No. 0040-06 and only issue temporary ID cards that have a definite expiration date for seasonal and volunteer staff.

Action Plan: DGS agrees with this recommendation. DGS will request Chief Administrative Officer approval to revise the CAO Admin Manual Item No. 0040-06 to address the issuance of visitor badges. This will include the required procedures for the departments requesting visitor badges (e.g. issuing, collecting, and maintaining accurate records.) DGS will create a process to monitor the various departments use of visitor's badges and perform periodic audits.

Planned Completion Date: February 12, 2021

Contact Information for Implementation: Charles Gompf, Facility Support Manager
Ken Frederiksen, Facility Support Manager

If you have any questions, please contact Mike Curtis, Deputy Director, at (858) 282-3919 or michael.curtis@sdcounty.ca.gov.

Sincerely,

Nicole J. Alejandre
Digitally signed by Nicole J. Alejandre
Date: 2020.09.18 16:14:50 -07'00'

NICOLE J. ALEJANDRE
Assistant Director

DEPARTMENT'S RESPONSE
(OFFICE OF EMERGENCY SERVICES)

JEFF TONEY
DIRECTOR
(858) 565-3490
FAX (858) 565-3499

County of San Diego

Office of Emergency Services
5580 Overland Ave, Suite 100, San Diego, CA 92123-1239
www.sdcounty.ca.gov/oes

STEPHEN REA
ASSISTANT DIRECTOR
(858) 565-3490
FAX (858) 565-3499

October 5, 2020

TO: Juan R. Perez
Chief of Audits

FROM: Jeff Toney, Director
Office of Emergency Services

DEPARTMENT RESPONSE TO AUDIT RECOMMENDATIONS: WORKSITE & SYSTEMS ACCESS, SAFETY, AND SECURITY CONTROLS

Finding I: Systems Access Had Not Been Removed for Employees That Terminated Employment

OAAS Recommendation 1: Review user access periodically and disable access for users that no longer require access to the application based on their responsibilities.

Action Plan: OES agrees that system access had not been removed for employees who terminated employment with the County. WebEOC is used by the entire County as well as other jurisdictions within the region. At the time of the audit, there were over 6,000 user accounts covering 67 organizations/jurisdictions. Currently, there is no practical process or tool that allows supervisors or HR departments within these organizations to notify OES when employees leave. User lists are periodically sent to jurisdiction contacts so that they may update their user accounts.

In March 2020, OES consulted with Juvare, the developer of WebEOC. Administrative controls were implemented to disable all user accounts for users who had not logged in within the past 365 days. Active users must contact OES to unlock their account. This policy enforcement is now permanent. Further, all users who had not logged in within the past one thousand days, were deleted from WebEOC. This reduced the number of user accounts by approximately 50%. This is a manual process and will continue as a matter of practice.

Planned Completion Date: Completed and ongoing.

Contact Information for Implementation: Patty Jordan, IT Principal, (858) 565-5594

OAAS Recommendation 2: Consider enabling the control in WebEOC that removes user's access after a period of inactivity.

Action Plan: In March 2020, OES consulted with Juvare, the developer of WebEOC. Administrative controls were implemented to disable all user accounts for users who had not logged in within the past 365 days. Active users must contact OES to unlock their account. This policy enforcement is now permanent. Further, all users who had not logged in within the past one thousand days, were deleted from WebEOC. This reduced the number of user accounts by approximately 50%. This is a manual process and will continue as a matter of practice.

Planned Completion Date: Completed and ongoing.

Contact Information for Implementation: Patty Jordan, IT Principal, (858) 565-5594

Finding VIII: Additional Processes Needed to Ensure County Security Policy Is Fully Implemented

OAAS Recommendation: OES Management and the Governance Committee should consider the following areas when designing the security initiative processes:

- Revise the County Security Policy to ensure that the security of County facilities is reassessed on a 5-year cycle, if that is what the initiative intended.
- Standardize the Vulnerability Assessment format and criteria to ensure instructions to complete assessments are clear to prevent inconsistencies.
- Clearly define the timeframe to disseminate Vulnerability Assessments to prevent delays in the development of Security Action Plans.
- Ensure confidentiality is maintained during the process of reporting the results of Vulnerability Assessments to the respective departments.
- Design and develop an IT solution that is tailored to the needs of the entire Security Initiative process, including operational functionality, proper approvals, secure storage of documentation, and reporting capabilities.
- Standardize the Security Action Plan format and ensure instructions to complete the action plans are clear to prevent inconsistencies.
- Define clear roles and responsibilities for approving the Security Action Plans and revise the County Security Policy to include clarification, if necessary.
- Consider and address any budget constraints that may impede the progress of security enhancements to facilities.
- Develop a charter for the Governance Committee to define the purpose, roles, and responsibilities of the committee.

Action Plan: OES agrees that additional processes are needed to ensure the County Security Initiative is fully implemented. The County Security Initiative is an enterprise-wide initiative that is outlined in Admin Manual Item No. 0050-02-09 and is administered by the Office of Emergency Services, but compliance hinges on functions being executed by every County business group and department.

At the time of the audit, OES Management in coordination with the County Security Initiative Governance Committee were actively planning for the redesign of business processes to improve efficiency, reduce cost, and increase quality of outputs. This process will continue throughout FY20-21. The redesign will include:

- Enhanced Vulnerability Assessment Form and Security Action Plan that includes standardized criteria and clear instructions

- Clearly defined workflow timelines from initial facility identification through Security Action Plan approval
- Clearly defined roles and responsibilities for those authorized to approved Security Action Plans
- Development and implementation of an IT solution that is tailored to the needs of the entire Security Initiative process, including operational functionality, proper approvals, secure storage of documentation, and reporting capabilities
- Development a charter for the Governance Committee to define the purpose, roles, and responsibilities of the committee

Additionally, OES Management and the County Security Initiative Governance Committee will coordinate with County Executive Leadership to discuss proposed revisions to the County Security Policy.

Planned Completion Date: Process redesign completion planned for June 30, 2021. Enterprise-wide implementation will be ongoing.

Contact Information for Implementation: Julie Jeakle, Group Program Manager, (858) 715-2207

If you have any questions, please contact me at (858) 715-2201.

Jeff Toney
Director