SUBMITTAL TO THE BOARD OF SUPERVISORS
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

ITEM: 2.15
(ID # 28533)
MEETING DATE:
Tuesday, August 26, 2025

FROM : AUDITOR CONTROLLER

SUBJECT: AUDITOR-CONTROLLER: Internal Audit Report 2025-0321 Riverside County Sheriff-Coroner Department, Follow up Audit, [District: All], [$0]

RECOMMENDED MOTION: That the Board of Supervisors:

1. Receive and file Internal Audit Report 2025-321: Riverside County Sheriff-Coroner Department, Follow-up Audit

ACTION:Consent

Ben J. Benoit, COUNTY AUDITOR-CONTROLLER 8/7/2025

MINUTES OF THE BOARD OF SUPERVISORS

On motion of Supervisor Medina, seconded by Supervisor Gutierrez and duly carried by unanimous vote, IT WAS ORDERED that the above matter is received and filed as recommended.

Ayes:	Medina, Spiegel, Washington, Perez and Gutierrez
Nays:	None
Absent:	None
Date:	August 26, 2025
xc:	Auditor

Kimberly A. Rector
Clerk of the Board
By: _____ Deputy

SUBMITTAL TO THE BOARD OF SUPERVISORS COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

FINANCIAL DATA	Current Fiscal Year:	Next Fiscal Year:	Total Cost:	Ongoing Cost
COST	$ 0.0	$ 0.0	$ 0.0	$ 0.0
NET COUNTY COST	$ 0.0	$ 0.0	$ 0.0	$ 0.0
SOURCE OF FUNDS: N/A			Budget Adjustment: No	
			For Fiscal Year: n/a	

BACKGROUND:

Summary

We completed a follow-up audit of the Riverside County Sheriff-Coroner Department. Our audit was limited to reviewing actions taken as of March 24, 2025, to correct findings noted in our original audit report 2024-019 dated December 3, 2024. The original audit report contained 10 recommendations, all of which required implementation to help correct the reported findings.

Based on the results of our audit, we found that of the 10 recommendations:

- 4 of the recommendations were implemented.
- 1 of the recommendations were partially implemented.
- 4 of the recommendations were not implemented.
- 1 of the recommendations no longer applicable

For an in-depth understanding of the original audit, please refer to Internal Audit Report 2024-019 included as an attachment to this follow-up audit report, or it can also be found at https://auditorcontroller.org/divisions/internal-audit/reports.

Impact on Residents and Businesses

Provide an assessment of internal controls over the audited areas.

Additional Fiscal Information

Not applicable

ATTACHMENT.

Riverside County Auditor-Controller - Internal Audit Report 2025-321: Riverside County Sheriff-Coroner Department, Follow-up Audit

Office of Ben J. Benoit

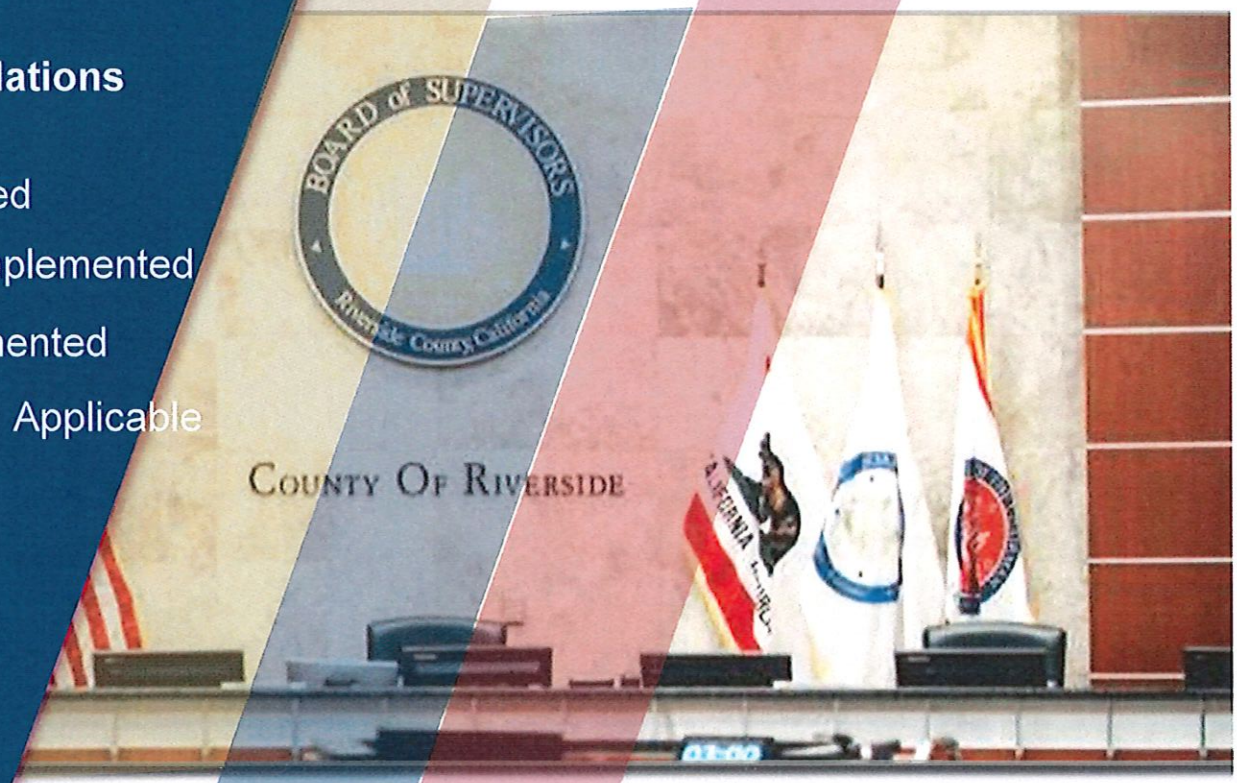
Riverside County Auditor-Controller

Internal Audit Report 2025-321

Follow-up

10 Recommendations

- ✔ 4 Implemented
- ▶ 1 Partially Implemented
- X 4 Not Implemented
- ↯ 1 No Longer Applicable



Riverside County Sheriff-Coroner Department, Follow-up Audit

August 26, 2025

August 26, 2025

Sheriff Bianco
Sheriff-Coroner
Riverside County Sheriff-Coroner Department
4095 Lemon St, 2nd Floor
Riverside, CA 92501

Subject: **Internal Audit Report 2025-321: Riverside County Sheriff-Coroner Department, Follow-up Audit**

Dear Sheriff Bianco:

We completed the follow-up audit of the Riverside County Sheriff-Coroner Department. Our audit was limited to reviewing actions taken as of March 24, 2025, to help correct the findings noted in our original audit report 2024-019 dated December 3, 2024.

We conducted our audit in accordance with the International Standards for the Professional Practice of Internal Auditing. These standards require that we plan and perform the audit to obtain reasonable assurance that our objective, as described in the preceding paragraph, is achieved. Additionally, the standards require that we conduct the audit to provide sufficient, reliable, and relevant evidence to achieve the audit objectives. We believe the audit provides a reasonable basis for our conclusion.

The original audit report contained 10 recommendations, all of which required implementation to help correct the reported findings. Based on the results of our audit, we found that of the 10 recommendations:

- 4 of the recommendations were implemented.
- 1 of the recommendations was partially implemented.
- 4 of the recommendations were not implemented.
- 1 of the recommendations no longer applicable.

Internal Audit Report 2025-321: Riverside County Sheriff-Coroner Department, Follow-up Audit

A summary of the conditions from the original audit and the results of our review on the status of the implementation of the recommendations are provided in this report. For an in-depth understanding of the original audit, please refer to Internal Audit Report 2024-019 included as "Attachment A" of this audit report along with your department status letter as "Attachment B." You can also find the original audit report at https://auditorcontroller.org/ divisions/internal-audit/reports.

We thank you and your staff for the help and cooperation. The assistance provided contributed significantly to the successful completion of this audit.

Ben J. Benoit
Riverside County Auditor-Controller

By: René Casillas, CPA, CRMA
Deputy Auditor-Controller

cc: Board of Supervisors
Jeff A. Van Wagenen, County Executive Officer
Juan Perez, Chief Operating Officer
Michelle Paradise, Assistant Chief Executive Officer
Grand Jury

Table of Contents

Vulnerability Management

Finding 1: Badge Access Controls

"County of Riverside Facilities Security Specification v1.2, Section 7.1.1, *Physical Security*, states, 'County facilities are only accessible to authorized individuals with properly coded key cards, authorized keys or access authorization, and access to the premises is by official identification only.' Additionally, National Institute of Standards and Technology's[1] (NIST) Special Publication (SP) 800-12, *An Introduction to Information Security*, Section 10.16, *Personnel Security*, states, Organizations ensure that organizational information and systems are protected during and after personnel actions such as terminations or transfers.'

As of the fieldwork date, April 26, 2024, we identified the following in our review of badge access controls:

- Seven out of 961 employees separated from the department did not have badges deactivated timely. Of the seven badges not deactivated timely, all of them were still active.

- Sixteen employees had duplicate badges assigned to them.

- One hundred thirty-one generic badges (badges that do not have personnel assigned to them) were active.

The department's current policies and procedures are not standardized department-wide and do not include a process to deactivate badge access on the day of an employee's separation or transfer from the department. Sheriff Department's individual stations, jails, and facilities have different processes over managing badge access so that there is not one standardized practice throughout the department. Additionally, Sheriff Department does not have written, formal policies and procedure that guide personnel to monitor and track duplicate or generic access badges. Allowing badges to remain active after an employee has separated or transferred from the department exposes the department to risk where unauthorized individuals will continue to have physical access into sensitive areas within the department. This can lead to unauthorized individuals accessing county facilities and poses a threat to county assets and existing county personnel. The existence of duplicate badges enables individuals to access restricted areas without proper authorization, leading to potential theft, data breaches, or other malicious

[1] NIST is a federal agency within the US Department of Commerce whose standards and guidelines on security and privacy are considered authoritative references in designing and implementing security measures, including access control policies. Their standards are critical for ensuring the integrity, confidentiality, and availability of information systems, making them a reputable source for guiding security practices.

activities. Generic badges do not tie actions to specific individuals, making it difficult to hold personnel accountable for security breaches or unauthorized access."

Recommendation 1.1

"Disable badge access within 24 hours of an employee's separation or transfer from the department."

Current Status 1.1: Not Implemented

At time of fieldwork we noted that badge access remained active for 14 out of 117 employees (11%) who had separated from the department.

Management's Response

"The Sheriff's Office is working to implement an Access Card Policy that will reinforce and align with our existing End of Service (EOS) policy. The EOS policy has already been updated to ensure that badge access along with all other forms of system access-is disabled by the next business day. This change has been fully implemented and is currently enforced as part of our standardized EOS workflow. The upcoming Access Card Policy will formalize the practice and ensure continued alignment with security and audit requirements."

Recommendation 1.2

"Develop a standardized process to review, approve, monitor, and disable duplicate badges and generic access badges."

Current Status 1.2: Not Implemented

After review, it was determined that a standardized process to review, approve, monitor, and disable duplicate and generic access badges had not been developed. We noted the following:

- Fifty-one employees were assigned duplicate badges.
- One hundred and three generic badges remained active without being assigned to specific personnel.

Management's Response

"The Sheriff's Office is in the process of implementing an Access Card Policy to standardize requirements for the review, approval, monitoring and disabling duplicate and generic access badges."

Recommendation 1.3

"Develop standardized policies and procedures over disabling badge access within 24 hours of an employee's separation or transfer from the department."

Current Status 1.3: Implemented

Recommendation 1.4

"Develop standardized policies and procedures over managing the administration and disabling of duplicate badges and generic access badges, as well as establishing criteria for their creation and usage."

Current Status 1.4 Not Implemented

Based on our inquiries and walkthroughs with department personnel standardized policies and procedures have not been developed.

Management's Response

"The Sheriff's Office is in the process of implementing an Access Card Policy to standardize requirements for managing the administration and disabling of duplicate badges and generic access badges, as well as establishing criteria for their creation and usage."

Finding 2: Timely Termination of System Access Rights

"County of Riverside Information Security Standard Revision 2.0, Section 4.16.4, *Personnel Termination,* states, 'County Departments and IT Administrators shall disable system access and retrieve all security-related organizational system-related property upon termination of individual employment.'

Active Directory and non-Active Directory access rights were not terminated in a timely manner (within 24 hours). We identified the following:

- One hundred sixty-four out of 780 former employees (21%) did not have their Active Directory account termination requests created and approved in a timely manner. The average time elapsed between employee separation and ticket approval was 64 days, with the longest taking 504 days for approval and the shortest taking 4 days.

- For the system applications not linked to Active Directory, we were unable to determine whether access rights were terminated in a timely manner as the department does not track the date and time in which a separated employee's access was disabled. Additionally, for all five system applications selected for testing, separated employees continued to have access as of the fieldwork date. See Table A below for a summary of the results:

Table A: Results Summary – System Applications Not Linked to Active Directory

System	Observations
A	Of the 149 employees with access to System A enabled, one employee (<1%) separated from the department continued to have access to System A as of the fieldwork date.
B	Of the 3,244 employees with access to System B enabled, 35 employees (1%) separated from the department continued to have access to System B as of the fieldwork date.
C	Of the 1,639 employees with access to System C enabled, 156 employees (9%) separated from the department continued to have access to System C as of the fieldwork date.
D	Of the 3,429 employees with access to System D enabled, 20 employees (<1%) separated from the department continued to have access to System D as of the fieldwork date.
E	Of the 1,223 employees with access to System E enabled, 3 employees (<1%) separated from the department continued to have access to System E as of the fieldwork date.

Sheriff Department employees did not have their Active Directory account termination requests created and approved timely upon separation from the department. Additionally, the department's current policies and procedures do not include a process for identifying the system applications needing to be disabled upon an employee separating or transferring from the department. Allowing user accounts to remain open after employment has ended exposes the department to risk where information maintained in the department can be continuously accessed by individuals who no longer have a right or need to know. Depending on the sensitivity

of the information maintained by department systems, it can create administrative issues and have a financial impact if held liable."

Recommendation 2.1

"Disable all user system accounts within 24 hours of an employee's separation from the department to remain compliant with County of Riverside Information Security Standard Revision 2.0, Section 4.16.4, *Personnel Termination.*"

Current Status 2.1: Not Implemented

Active Directory and non-Active Directory access rights were not terminated in a timely manner (within 24 hours). Based on our review, we identified the following:

- Sixty-three out of 117 (53%) former employees did not have their Active Directory account termination requests processed in a timely manner. The average time elapsed between employee separation and ticket approval was 6 days, with the longest taking 55 days for approval and the shortest taking 3 days.

- Separated employees continued to have access to non-active directory applications as of the fieldwork date. See Table A below for a summary of the results:

System	Observations
A	Of the 74 employees with access to System A enabled, one employee (<1%) separated from the department continued to have access to System A as of the fieldwork date.
B	Of the 9 employees with access to System B enabled, 5 employees (66%) separated from the department continued to have access to System B as of the fieldwork date.

Management's Response

"In response to the recommendation to "disable all user system accounts within 24 hours of an employee's separation from the department to remain compliant with County of Riverside Information Security Standard Revision 2.0, Section 4.16.4, Personnel Termination," this matter has been reviewed with the Auditor and the department revised the End of Service (EOS) Policy accordingly. "

Recommendation 2.2

"Update policies and procedures to ensure the disabling of all user system accounts are requested and approved within 24 hours of an employee's separation or transfer from the department."

Current Status 2.2: Implemented

Finding 3: Vulnerability Remediation Tracking

"County of Riverside Information Security Standard Revision v2.0, Section 4.17.4, *Vulnerability Scanning,* states, 'remediate legitimate vulnerabilities per an organizational assessment of risk… share information obtained from the vulnerability scanning process and control assessments with stakeholders and IT Administrators to help eliminate similar vulnerabilities…'

Remediation progress for unresolved system vulnerabilities need to be tracked and documented to ensure remediation steps available for vulnerabilities do not remain unresolved. Additionally, we noted multiple vulnerabilities during the audit period that were outstanding with no documented evidence of remediation progress. See Table B below for the number of total system vulnerabilities by severity as of the fieldwork date, April 26, 2024:

Table B: Number of Total System Vulnerabilities by Severity

Vulnerability Severity	Number of Vulnerabilities	Remediation Response Timeline [2]
Critical	3,858	7 Days
High	6,856	14 Days
Medium	606	30 Days

Sheriff Department does not have a process in place to track remediation progress for unresolved vulnerabilities. The absence of tracking the remediation progress impedes the department's ability to closely monitor the implementation status and quickly mitigate any risks posed by the system vulnerabilities."

[2] County of Riverside Information Security Standard Revision v2.0, Section 4.20.2, *Flaw Remediation*, establishes timelines for which security-relevant software and firmware updates are to be installed upon vulnerability identification.

Recommendation 3

"Develop procedures to ensure remediation progress for unresolved vulnerabilities is adequately documented, tracked, assigned to personnel, and monitored."

Current Status 3: Implemented

Finding 4: Server Upgrades

"NIST SP 800-40, *Procedures for Handling Security Patches*, states, "Timely patching is critical to maintain the operational availability, confidentiality, and integrity of information technology (IT) systems."

Nine of Sheriff Department's 89 system servers (10%) have not been upgraded to the available supported versions. Additionally, the department is relying on outdated server operating systems without having an Extended Security Update agreement with the respective suppliers. An Extended Security Update agreement is needed to acquire server updates after an operating system has rolled out. The department does not have a process in place to track remediation progress for unresolved vulnerabilities, such as using outdated system servers, and there are potential deployment errors that may affect the department applications when updating to the latest version. Outdated system servers may cause stability issues and contain known security vulnerabilities that individuals can exploit to gain unauthorized access to the applications running on those servers. This can lead to data breaches, loss of sensitive information, and potential legal and financial consequences."

Recommendation 4

"Develop a process to ensure Sheriff Department's system servers are upgraded timely once a new, supported version becomes available"

Current Status 4: Partially Implemented

Based on our review, we identified nine servers were outdated. The respective servers are in the process of decommissioning and migrating to supported platforms. Sheriff is obtaining vendor RFQs and finalizing a security update agreement to ensure continued support beyond the operating system's end-of-life.

Management's Response

"The Sheriff's Office has reviewed the nine servers identified outdated. The Technical Services Bureau is actively working to fully implement compliance by decommissioning servers, upgrading servers, schedule migrations to new servers, and procure new equipment. The department is committed to ensuring all systems are transitioned to supported platforms and that appropriate security agreements are in place to maintain compliance and operational continuity. "

Finding 5: Identifying and Prioritizing System Applications

"NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Section CP-2, *Contingency Planning*, states, 'Organizations identify critical system assets so that additional controls can be employed (beyond the controls routinely implemented) to help ensure that organizational mission and business functions can continue to be conducted during contingency operations. The identification of critical information assets also facilitates the prioritization of organizational resources.'

Sheriff Department needs to identify critical system applications and assign risk ratings to identify business dependencies that address resource prioritization and optimize patch management. The department does not have a process in place to assign risk ratings to critical and non-critical system applications for business dependencies relating to contingency planning. Not identifying critical system applications and assigning risk ratings can create operational challenges such as prioritization conflicts, security concerns, and delays in decision-making when system applications require major repairs and downtime.

On May 10, 2024, Sheriff Department identified and updated their listing of critical system applications to address the condition above and communicated their efforts to improve the adequacy and effectiveness of their internal controls. Specifically, the department assigned risk ratings and prioritized critical system applications to enhance patch management, security features, and functionality. In the follow-up audit, we will verify whether the department maintains and updates their critical system application listing to reflect all running applications."

Recommendation 5

"Develop policies and procedures to establish the frequency in which the department's listing of critical system applications is updated."

Current Status 5: Implemented

Finding 6: Memorandum of Understanding

"NIST SP 800-47, *Managing the Security of Information Exchanges*, states, 'To address information security requirements for system interconnections, an interconnection security agreement (ISA) that specifies the security requirements expected for the impact level of the information being exchanged for all participating systems is recommended. ISAs are often coupled with Memoranda of Understanding/Agreement (MOU/A).'

Sheriff Department currently relies on Riverside County Information Technology (Information Technology) for various services, including network architecture, network security, phishing training, vendor enterprise agreement, cyber insurance coverage, and vulnerability reports. However, there has not been an established Memorandum of Understanding between Sheriff Department and Information Technology. Not having an established Memorandum of Understanding creates responsibility gaps and disrupts formalized communication and procedural clarity regarding the transmission and acknowledgment from Sheriff Department and Information Technology. As such, Sheriff Department does not regularly receive vulnerability reports to assess their existing vulnerabilities. The existing informal communication channels do not ensure that critical security information reaches the intended recipients timely and reliably."

Recommendation 6

"Establish a formal Memorandum of Understanding with Information Technology that addresses roles, responsibilities, and expectations."

Current Status 6: No longer applicable

According to RCIT, due to the rapid changes in technology, a Memorandum of Understanding can impose limitations on the department. In contrast, non-managed departments retain the flexibility to utilize RCIT services as needed, without being obligated to adopt RCIT-specific solutions. This enables departments to pursue more immediate and specialized solutions that align more closely with their operational needs.

Attachment A

Office of Ben J. Benoit
Riverside County Auditor-Controller

Number of Findings & Recommendations

High Risk

4 Findings
- 8 Recommendations

Medium Risk

0 Findings

Low Risk

2 Findings
- 2 Recommendations

* Please refer to Appendix A for a classification of the priority levels.

Internal Audit Report

2024-019

Riverside County Sheriff-Coroner Department Audit

December 3, 2024

COUNTY OF RIVERSIDE
OFFICE OF THE AUDITOR-CONTROLLER

Ben J. Benoit, Auditor-Controller
Tanya S. Harris, DPA, CPA, Assistant Auditor-Controller

4080 Lemon Street, 11th Floor
P.O. Box 1326
Riverside, CA 92502-1326
951-955-3800

December 3, 2024

Sheriff Bianco
Sheriff-Coroner
Riverside County Sheriff-Coroner Department
4095 Lemon St, 2nd Floor
Riverside, CA 92501

Subject: **Internal Audit Report 2024-019: Riverside County Sheriff-Coroner Department Audit**

Dear Sheriff Bianco:

In accordance with Board of Supervisors Resolution 83-338, we audited the Riverside County Sheriff-Coroner Department to provide management and the Board of Supervisors with an independent assessment of internal controls over vulnerability management and encumbrances.

We conducted our audit in accordance with the International Standards for the Professional Practice of Internal Auditing. These standards require that we plan and perform the audit to obtain sufficient, reliable, relevant and useful information to provide reasonable assurance that our objective as described above is achieved. An internal audit includes the systematic analysis of information to evaluate and improve the effectiveness of internal controls. We believe this audit provides a reasonable basis for our conclusion.

Internal controls are processes designed to provide management reasonable assurance of achieving efficiency of operations, compliance with laws and regulations, and reliability of financial and non-financial information. Management is responsible for establishing and maintaining adequate internal controls. Our responsibility is to evaluate the internal controls.

Our conclusion and details of our audit are documented in the body of this audit report.

Internal Audit Report 2024-019: Riverside County Sheriff-Coroner Department Audit

As requested, in accordance with paragraph III.C of the Board of Supervisors Resolution 83-338, management responded to each reported condition and recommendation contained in our report. Management's responses are included in the report. We will follow-up to verify that management implemented the corrective actions.

We thank you and your staff for the help and cooperation. The assistance provided contributed significantly to the successful completion of this audit.

Ben J. Benoit
Riverside County Auditor-Controller

By: René Casillas, CPA, CRMA
Deputy Auditor-Controller

cc: Board of Supervisors
Jeff A. Van Wagenen, Jr., County Executive Officer
Dave Rogers, Chief Administrative Officer
Juan Perez, Chief Operating Officer
Grand Jury

Table of Contents

Executive Summary

Overview

Riverside County Sheriff-Coroner Department (Sheriff Department) is responsible for providing "24/7 uniformed response to calls for service from the public in the unincorporated county areas," as well as "operate a countywide jail system that serves all local agencies, provide court security and service of court processes and orders and to perform Coroner – Public Administrator functions pursuant to California law."

Sheriff has an adopted budget of $1.09 billion for FY 2024-25 and 5,341 adopted positions. County of Riverside, *Fiscal Year 2024-25 Adopted Budget Volume 1, 257*.

Audit Objective

Our objective is to provide management and the Board of Supervisors with an independent assessment about the adequacy and effectiveness of internal controls over vulnerability management and encumbrances. Internal controls are processes designed to provide management reasonable assurance of achieving efficiency of operations, compliance with laws and regulations, and reliability of financial and non-financial information. Reasonable assurance recognizes internal controls have inherent limitations, including cost, mistakes, and intentional efforts to bypass internal controls.

Audit Scope and Methodology

We conducted the audit from January 24, 2024, through May 8, 2024, for operations from July 1, 2022, through April 2, 2024. Following a risk-based approach, our scope included the following:

- Vulnerability Management
- Encumbrances

AUDIT HIGHLIGHTS

- Monitoring employee badge issuance and deactivation can be implemented to safeguard the department's assets.
- Separated employee user accounts need to be deactivated timely (within 24 hours).
- Unresolved system vulnerabilities need to be tracked and monitored.
- Server operating systems need to be upgraded to the available supported versions.
- Critical system applications need to be identified and assigned risk ratings.
- A Memorandum of Understanding needs to be established between Sheriff Department and Riverside County Information Technology.

Audit Conclusion

Based on the results of our audit, internal controls over encumbrances are functioning as designed to help Sheriff Department achieve its business process objectives. However, we identified improvement opportunities for internal controls over vulnerability management that can help provide reasonable assurance that the department's objectives relating to this area will be achieved. Specifically, the improvement opportunities are as follows: Monitor employee badge issuance and deactivation to safeguard the department's assets; deactivate employee user accounts timely upon separation or transfer from the department; upgrade the server operating systems to the available supported versions; identify critical system applications and assign risk ratings[1]; establish a Memorandum of Understanding with Riverside County Information Technology.

Upon discussing the condition above relating to the identification of critical system applications[1] with management on May 10, 2024, Sheriff Department proceeded to resolve this condition and communicated their efforts to improve the adequacy and effectiveness of their internal controls over maintaining their critical system application listing. We would like to extend our appreciation to the department for being receptive to our evaluation and proactive in implementing the recommendations associated with this area.

[1] Please see Finding 5 (page 15) for a description of the department's resolution efforts relating to the identification of critical system applications.

Vulnerability Management

Background

Vulnerability management is a proactive approach focused on identifying, assessing, tracking, and mitigating system vulnerabilities. It involves discovering and prioritizing vulnerabilities, tracking common exposed vulnerabilities, scanning systems for applicable vulnerabilities, assessing associated risks, assigning responsibility, and recommending remediation strategies. Effective patch management involves integrating applications and servers for regular updates to address known vulnerabilities and improve system stability. This requires timely application of tested patches to mitigate exploitation risks by cyber threat actors.

Incident response is critical, involving constant monitoring of malicious codes and attempted breaches by cyber threat actors exploiting system vulnerabilities. This process strategically neutralizes threats by blocking them or quarantining infected files or applications, acting as a detective control, while vulnerability assessment and patch management serve as preventive controls. Preventive controls are prioritized to minimize the frequency of repetitive threats.

Sheriff Department enhances physical security through secured badge access cards, controlling and monitoring entry and exit within its facilities. Badge access facilitates enforcement of access controls, tracks personnel movement, mitigates unauthorized entry risk, and safeguards sensitive assets and information.

Active Directory is a directory service used to manage permissions and network resource access. When an employee separates from the department, Sheriff Department's Human Resources division creates a help desk ticket to request removal of the employee's access rights. After approval, the department's Technical Service Bureau is notified to disable the Active Directory account and other access points. Help desk tickets include tasks such as disabling email accounts, reclaiming software licenses, and retrieving issued equipment. Tickets remain open until all tasks are completed, ensuring comprehensive deactivation of the departed employee's access.

Objective

To verify the existence and adequacy of internal controls over Sheriff Department's vulnerability management processes.

Audit Methodology

To accomplish these objectives, we:

- Obtained an understanding of County of Riverside Information Security Standard Revision 2.0.

- Interviewed key personnel and reviewed Sheriff Department's procedures over vulnerability management.

- Verified whether adequate segregation of duties are in place relating to vulnerability management.

- Obtained a listing of all active badges within Sheriff Department and verified whether the badges were deactivated timely upon employee separation from the department.

- Obtained a report from the department that details the ticket creation and approval dates for disabling employee access to Active Directory.

- Verified whether requests to disable Active Directory were created and approved by department personnel within 24 hours of an employee's separation or transfer from the department.

- Obtained a listing of all critical systems used by Sheriff Department and judgmentally selected a sample of systems not linked to Active Directory (System A, System B, System C, System D, and System E).

- Verified whether access rights to the selected system applications above were disabled within 24 hours of an employee's separation or transfer from the department.

- Obtained the department's vulnerability management plan and verified the existence of adequate insurance coverage, vulnerability assessments, patch management processes, and incident response plans.

- Obtained the department's vulnerability assessment report and verified whether vulnerabilities are tracked and resolved timely.

- Obtained the department's incident response report and verified whether threats are neutralized timely.

- Obtained a listing of department applications and verified whether an adequate patch management system is used and applications are assigned risk ratings.

Finding 1: Badge Access Controls	Priority Level: 1[2]

County of Riverside Facilities Security Specification v1.2, Section 7.1.1, *Physical Security*, states, "County facilities are only accessible to authorized individuals with properly coded key cards, authorized keys or access authorization, and access to the premises is by official identification only." Additionally, National Institute of Standards and Technology's[3] (NIST) Special Publication (SP) 800-12, *An Introduction to Information Security*, Section 10.16, *Personnel Security*, states, "Organizations ensure that organizational information and systems are protected during and after personnel actions such as terminations or transfers."

As of the fieldwork date, April 26, 2024, we identified the following in our review of badge access controls:

- Seven out of 961 employees separated from the department did not have badges deactivated timely. Of the seven badges not deactivated timely, all of them were still active.

- Sixteen employees had duplicate badges assigned to them.

- One hundred thirty-one generic badges (badges that do not have personnel assigned to them) were active.

The department's current policies and procedures are not standardized department-wide and do not include a process to deactivate badge access on the day of an employee's separation or transfer from the department. Sheriff Department's individual stations, jails, and facilities have different processes over managing badge access so that there is not one standardized practice throughout the department. Additionally, Sheriff Department does not have written, formal policies and procedure that guide personnel to monitor and track duplicate or generic access badges. Allowing badges to remain active after an employee has separated or transferred from the department exposes the department to risk where unauthorized individuals will continue to have physical access into sensitive areas within the department. This can lead to unauthorized individuals accessing county facilities and poses a threat to county assets and existing county personnel. The existence of duplicate badges enables individuals to access restricted areas without proper authorization, leading to potential theft, data breaches, or other malicious activities. Generic badges do not tie actions to specific individuals, making it difficult to hold personnel accountable for security breaches or unauthorized access.

[2] Please see Appendix A (page 16) for a description of the finding priority level classifications.

[3] NIST is a federal agency within the US Department of Commerce whose standards and guidelines on security and privacy are considered authoritative references in designing and implementing security measures, including access control policies. Their standards are critical for ensuring the integrity, confidentiality, and availability of information systems, making them a reputable source for guiding security practices.

Recommendation 1.1

Disable badge access within 24 hours of an employee's separation or transfer from the department.

Management's Response

"**Concur.** Current Sheriff policy requires all separating employees to return all issued equipment to either the assigned station/bureau, Uniform Services, and/or Sheriff's Admin on their final working day—this includes the employee ID card, which is also programmed for door access. Periodic human error may occur, whereas cards may become lost or personnel responsible for deactivation may occasionally fail to render an unused card deactivated—this is likely why there is such a small number of errant cards. Policies related to employee ID card access has been modified to assure proper deactivation of access is addressed and recorded.

Note: Due to the various and disparate door access control systems used throughout the department, the door access control systems are not tied to the agency Active Directory (AD); however, Sheriff's Project Management Office (PMO) is actively seeking an enterprise system to replace the system and access points at all Sheriff's facilities."

Actual/Estimated Date of Corrective Action

"Policy modifications estimated to be implemented by November 2024. It is anticipated this project of this magnitude will encompass about two years to implement."

Recommendation 1.2

Develop a standardized process to review, approve, monitor, and disable duplicate badges and generic access badges.

Management's Response

"**Concur.** Sheriff shall adopt a written policy detailing a process for staff to periodic review, approve, monitor, and disable duplicate badges and generic access badges. The policy should incorporate additional safeguards, to include the centralized management of badges, and adopt measures to ensure that only authorized personnel have access to sensitive areas within the department, thereby maintaining a higher level of security and control. Policy changes with the existing system limitations in place should occur until an enterprise replacement solution is fully implemented."

Actual/Estimated Date of Corrective Action

"It is anticipated the creation of policy should be completed in 3 months; November 2024."

Recommendation 1.3

Develop standardized policies and procedures over disabling badge access within 24 hours of an employee's separation or transfer from the department.

Management's Response

"**Concur.** See response in Recommendation 1.2 (above)."

Actual/Estimated Date of Corrective Action

"It is anticipated the creation of policy should be completed in 3 months; November 2024."

Recommendation 1.4

Develop standardized policies and procedures over managing the administration and disabling of duplicate badges and generic access badges, as well as establishing criteria for their creation and usage.

Management's Response

"**Concur.** See response in Recommendation 1.2 (above)."

Actual/Estimated Date of Corrective Action

"It is anticipated the creation of policy should be completed in 3 months; November 2024."

Finding 2: Timely Termination of System Access Rights	Priority Level: 1[4]

County of Riverside Information Security Standard Revision 2.0, Section 4.16.4, *Personnel Termination,* states, "County Departments and IT Administrators shall disable system access and retrieve all security-related organizational system-related property upon termination of individual employment."

[4] Please see Appendix A (page 16) for a description of the finding priority level classifications.

Active Directory and non-Active Directory access rights were not terminated in a timely manner (within 24 hours). We identified the following:

- One hundred sixty-four out of 780 former employees (21%) did not have their Active Directory account termination requests created and approved in a timely manner. The average time elapsed between employee separation and ticket approval was 64 days, with the longest taking 504 days for approval and the shortest taking 4 days.

- For the system applications not linked to Active Directory, we were unable to determine whether access rights were terminated in a timely manner as the department does not track the date and time in which a separated employee's access was disabled. Additionally, for all five system applications selected for testing, separated employees continued to have access as of the fieldwork date. See Table A below for a summary of the results:

Table A: Results Summary – System Applications Not Linked to Active Directory

System	Observations
A	Of the 149 employees with access to System A enabled, one employee (<1%) separated from the department continued to have access to System A as of the fieldwork date.
B	Of the 3,244 employees with access to System B enabled, 35 employees (1%) separated from the department continued to have access to System B as of the fieldwork date.
C	Of the 1,639 employees with access to System C enabled, 156 employees (9%) separated from the department continued to have access to System C as of the fieldwork date.
D	Of the 3,429 employees with access to System D enabled, 20 employees (<1%) separated from the department continued to have access to System D as of the fieldwork date.
E	Of the 1,223 employees with access to System E enabled, 3 employees (<1%) separated from the department continued to have access to System E as of the fieldwork date.

Sheriff Department employees did not have their Active Directory account termination requests created and approved timely upon separation from the department. Additionally, the department's current policies and procedures do not include a process for identifying the system applications needing to be disabled upon an employee separating or transferring from the department. Allowing user accounts to remain open after employment has ended exposes the department to risk where information maintained in the department can be continuously

accessed by individuals who no longer have a right or need to know. Depending on the sensitivity of the information maintained by department systems, it can create administrative issues and have a financial impact if held liable.

Recommendation 2.1

Disable all user system accounts within 24 hours of an employee's separation from the department to remain compliant with County of Riverside Information Security Standard Revision 2.0, Section 4.16.4, *Personnel Termination*.

Management's Response

"**Concur.** Sheriff currently employs an "End of Service" process (EOS) to identify, list, track, monitor, and deactivate access to all agency systems upon separation from the department, either immediately for contentious separations or within 24 hours following non-contentious separations. This process has been in place for many years and is considered a routine task for Sheriff's IT personnel. Deactivation occurs at the Active Directory (AD) level, as well as software license deactivation for enterprise systems. Current EOS process will be reviewed and modified to confirm the proper deactivation of all system applications access is addressed and properly documented."

Actual/Estimated Date of Corrective Action

"November 2024."

Recommendation 2.2

Update policies and procedures to ensure the disabling of all user system accounts are requested and approved within 24 hours of an employee's separation or transfer from the department.

Management's Response

"**Concur.** Sheriff will ensure a written policy exists for this process—see response to Recommendation 1.2."

Actual/Estimated Date of Corrective Action

"It is anticipated the creation of policy should be completed in 3 months; November 2024."

Finding 3: Vulnerability Remediation Tracking	Priority Level: 1[5]

County of Riverside Information Security Standard Revision v2.0, Section 4.17.4, *Vulnerability Scanning,* states, "remediate legitimate vulnerabilities per an organizational assessment of risk… share information obtained from the vulnerability scanning process and control assessments with stakeholders and IT Administrators to help eliminate similar vulnerabilities…"

Remediation progress for unresolved system vulnerabilities need to be tracked and documented to ensure remediation steps available for vulnerabilities do not remain unresolved. Additionally, we noted multiple vulnerabilities during the audit period that were outstanding with no documented evidence of remediation progress. See Table B below for the number of total system vulnerabilities by severity as of the fieldwork date, April 26, 2024:

Table B: Number of Total System Vulnerabilities by Severity

Vulnerability Severity	Number of Vulnerabilities	Remediation Response Timeline [6]
Critical	3,858	7 Days
High	6,856	14 Days
Medium	606	30 Days

Sheriff Department does not have a process in place to track remediation progress for unresolved vulnerabilities. The absence of tracking the remediation progress impedes the department's ability to closely monitor the implementation status and quickly mitigate any risks posed by the system vulnerabilities.

Recommendation 3

Develop procedures to ensure remediation progress for unresolved vulnerabilities is adequately documented, tracked, assigned to personnel, and monitored.

Management's Response

"**Concur.** Sheriff's Technical Services Bureau (TSB) currently have staff responsible for monitoring, managing, and—in some cases—rejecting software patches after testing patch functionality following a release. Due to the varied and occasional specialized/custom nature of some agency applications, some commercial Operating System (OS) patches may render the

[5] Please see Appendix A (page 16) for a description of the finding priority level classifications.

[6] County of Riverside Information Security Standard Revision v2.0, Section 4.20.2, *Flaw Remediation*, establishes timelines for which security-relevant software and firmware updates are to be installed upon vulnerability identification.

impacted utility/service disabled—these threats are typically mitigated via network isolation. Sheriff's TSB will develop written protocols to maintain tracking of the remediation of potential system vulnerabilities based on their severity. This approach will enable close monitoring of the implementation status and progress, ensuring effective mitigation of any associated risks."

Actual/Estimated Date of Corrective Action

"It is anticipated the documentation of bureau protocol should be completed in 3 months; November 2024."

Finding 4: Server Upgrades	Priority Level: 1[7]

NIST SP 800-40, *Procedures for Handling Security Patches*, states, **"**Timely patching is critical to maintain the operational availability, confidentiality, and integrity of information technology (IT) systems."

Nine of Sheriff Department's 89 system servers (10%) have not been upgraded to the available supported versions. Additionally, the department is relying on outdated server operating systems without having an Extended Security Update agreement with the respective suppliers. An Extended Security Update agreement is needed to acquire server updates after an operating system has rolled out. The department does not have a process in place to track remediation progress for unresolved vulnerabilities, such as using outdated system servers, and there are potential deployment errors that may affect the department applications when updating to the latest version. Outdated system servers may cause stability issues and contain known security vulnerabilities that individuals can exploit to gain unauthorized access to the applications running on those servers. This can lead to data breaches, loss of sensitive information, and potential legal and financial consequences.

Recommendation 4

Develop a process to ensure Sheriff Department's system servers are upgraded timely once a new, supported version becomes available.

Management's Response

"**Concur.** Sheriff's Technical Services Bureau (TSB) will conduct thorough research and develop a comprehensive process to establish and maintain a regular schedule for evaluating, verifying, and updating the operating systems of server infrastructure. This process will ensure that all servers are consistently up to date and fully supported, receiving all necessary critical updates and patches to maintain optimal security and performance."

Actual/Estimated Date of Corrective Action

"It is anticipated the documentation of bureau protocol should be completed in 3 months; November 2024."

Finding 5: Identifying and Prioritizing System Applications	Priority Level: 3[7]

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Section CP-2, *Contingency Planning*, states, "Organizations identify critical system assets so that additional controls can be employed (beyond the controls routinely implemented) to help ensure that organizational mission and business functions can continue to be conducted during contingency operations. The identification of critical information assets also facilitates the prioritization of organizational resources."

Sheriff Department needs to identify critical system applications and assign risk ratings to identify business dependencies that address resource prioritization and optimize patch management. The department does not have a process in place to assign risk ratings to critical and non-critical system applications for business dependencies relating to contingency planning. Not identifying critical system applications and assigning risk ratings can create operational challenges such as prioritization conflicts, security concerns, and delays in decision-making when system applications require major repairs and downtime.

On May 10, 2024, Sheriff Department identified and updated their listing of critical system applications to address the condition above and communicated their efforts to improve the adequacy and effectiveness of their internal controls. Specifically, the department assigned risk ratings and prioritized critical system applications to enhance patch management, security features, and functionality. In the follow-up audit, we will verify whether the department maintains and updates their critical system application listing to reflect all running applications.

Recommendation 5

Develop policies and procedures to establish the frequency in which the department's listing of critical system applications is updated.

Management's Response

"**Concur.** Sheriff's Technical Services Bureau (TSB) will develop a process to regularly evaluate and categorize critical system applications. This will include verifying update status and completion to ensure all necessary critical updates and patches are applied for optimal security and performance."

[7] Please see Appendix A (page 16) for a description of the finding priority level classifications.

Actual/Estimated Date of Corrective Action

"It is anticipated the documentation of bureau protocol should be completed in 3 months; November 2024."

Finding 6: Memorandum of Understanding	Priority Level: 3[7]

NIST SP 800-47, *Managing the Security of Information Exchanges*, states, "To address information security requirements for system interconnections, an interconnection security agreement (ISA) that specifies the security requirements expected for the impact level of the information being exchanged for all participating systems is recommended. ISAs are often coupled with Memoranda of Understanding/Agreement (MOU/A)."

Sheriff Department currently relies on Riverside County Information Technology (Information Technology) for various services, including network architecture, network security, phishing training, vendor enterprise agreement, cyber insurance coverage, and vulnerability reports. However, there has not been an established Memorandum of Understanding between Sheriff Department and Information Technology. Not having an established Memorandum of Understanding creates responsibility gaps and disrupts formalized communication and procedural clarity regarding the transmission and acknowledgment from Sheriff Department and Information Technology. As such, Sheriff Department does not regularly receive vulnerability reports to assess their existing vulnerabilities. The existing informal communication channels do not ensure that critical security information reaches the intended recipients timely and reliably.

Recommendation 6

Establish a formal Memorandum of Understanding with Information Technology that addresses roles, responsibilities, and expectations.

Management's Response

"**Concur.** Sheriff's Technical Services Bureau (TSB) shall develop and establish a comprehensive Memorandum of Understanding (MOU) between the Sheriff's Technical Services Bureau and Riverside County Information Technology (RCIT). This MOU will clearly define IT-specific roles, system requirements, security protocols, and reporting standards to ensure effective collaboration and seamless service integration."

Actual/Estimated Date of Corrective Action

"It is anticipated the documentation of bureau protocol should be completed in 6 months; February 2025."

Encumbrances

Background

The Auditor-Controller's Office's *2024 Year-End Manual*, Chapter 6, *Encumbrances (Governmental Funds)*, states that encumbrances are commitments that exist at fiscal-year end related to unfulfilled contracts for goods and services. If a department waits until the next fiscal year when the commitments are fulfilled to record the related expenditures, sufficient appropriations to satisfy the payments may not be available. As such, to use budgeted appropriations from the fiscal year in which the commitment was established, Board of Supervisor approval must be obtained to increase the appropriation. A county-established "Schedule K" form is used during the year-end accrual process when requesting an increase in appropriations due to an established encumbrance. The Schedule K consists of purchase orders that have rolled over and are $5,000 or greater and must have a status of *dispatched* or *pending approval*. Blanket purchase orders covering multiple deliveries during the year do not qualify for encumbrance.

The Executive Office initially reviews the request for encumbrance amounts, which are subject to availability of appropriations and Net County Cost requirements, and then recommends the classification to its appropriate fund balance (i.e., restricted, committed, assigned). Once the Board of Supervisors has approved the encumbrance amounts, a journal entry will be posted to reclassify the approved amounts. Only fund balance accounts are affected in this process, and these balances will roll forward into the new fiscal year. The fund balance reclassification will then be appropriately reflected in the new fiscal year and budgeted appropriations will be increased in the original budgeted expenditure account to satisfy the commitment.

Objective

To verify the existence and adequacy of internal controls over Sheriff Department's encumbrance process relating to Schedule K purchase orders.

Audit Methodology

To accomplish these objectives, we:

- Obtained an understanding of the Auditor-Controller's Office's *2024 Year-End Manual* relating to encumbrances and applicable department processes and procedures.

- Obtained an understanding of the roles and responsibilities of departments that are involved in the year-end encumbrance process.

- Obtained and analyzed Sheriff Department's year-end encumbrances package for the completed FY 2022-23.

- Verified the accuracy and completeness of encumbrance data reported by Sheriff Department.

- Traced year-end encumbrances reported in Sheriff Department's encumbrance data to supporting documentation and entries in the Riverside County Financial System.

- Reviewed the Schedule K, related purchase orders, and recorded transactions to identify any discrepancies or irregularities in encumbrance activity.

- Determined whether Sheriff Department encumbrance spending was limited to purposes previously approved by the Board of Supervisors and the Auditor-Controller's Office.

Finding: None Noted

Based on the results of our audit, we determined that internal controls over encumbrances provide reasonable assurance that its objectives related to this area will be achieved. Reasonable assurance recognizes internal controls have inherent limitations, including costs, mistakes, and intentional efforts to bypass internal controls.

Appendix A: Finding Priority Level Classification

Priority Level 1	Priority Level 2	Priority Level 3
These are audit findings that represent the most critical issues that require immediate attention and pose a significant risk to the department's objectives, compliance, security, financial health, or reputation. They may indicate serious control failures, non-compliance with laws or regulations, significant financial errors, or vulnerabilities with severe potential impact. Immediate corrective measures are necessary to mitigate the risks associated with these findings.	These are audit findings that are important and require timely resolution, but their impact is not as severe as Priority Level 1. They may highlight moderate control weaknesses, areas of non-compliance with internal policies and procedures, or financial discrepancies that are significant but are not critical. While they might not pose an immediate threat, they should be addressed promptly to prevent further escalation or potential negative consequences.	These are audit findings that are less critical and generally have a lower impact on the department's objectives, compliance, or operations. They may include minor control deficiencies, procedural deviations with minimal impact, or non-critical administrative errors. While they may not require immediate attention, they should still be acknowledged and addressed within a reasonable timeframe to ensure ongoing improvement and prevent potential accumulation of minor issues.
Expected Implementation Date of Recommendation* One to three months	**Expected Implementation Date of Recommendation *** Three to six months	**Expected Implementation Date of Recommendation *** Six to twelve months

* Expected completion to implement recommendation date begins after issuance of final audit report.

Attachment B

Riverside County Sheriff's Office

Chad Bianco, Sheriff-Coroner

4095 Lemon Street • Riverside • California • 92501
www.riversidesheriff.org

The following are the current status of the reported findings and planned corrective actions contained in Internal Audit Report 2024-019: Riverside County Sheriff-Coroner Department Audit.

3/24/25

Authorized Signature **Date**

Finding 1: Badge Access Controls

"County of Riverside Facilities Security Specification v1.2, Section 7.1.1, *Physical Security*, states, 'County facilities are only accessible to authorized individuals with properly coded key cards, authorized keys or access authorization, and access to the premises is by official identification only.' Additionally, National Institute of Standards and Technology's**3** (NIST) Special Publication (SP) 800-12, *An Introduction to Information Security*, Section 10.16, *Personnel Security*, states, 'Organizations ensure that organizational information and systems are protected during and after personnel actions such as terminations or transfers.'

As of the fieldwork date, April 26, 2024, we identified the following in our review of badge access controls:

- Seven out of 961 employees separated from the department did not have badges deactivated timely. Of the seven badges not deactivated timely, all of them were still active.
- Sixteen employees had duplicate badges assigned to them.
- One hundred thirty-one generic badges (badges that do not have personnel assigned to them) were active.

The department's current policies and procedures are not standardized department-wide and do not include a process to deactivate badge access on the day of an employee's separation or transfer from the department. Sheriff Department's individual stations, jails, and facilities have different processes over managing badge access so that there is not one standardized practice throughout the department. Additionally, Sheriff Department does not have written, formal policies and procedure that guide personnel to monitor and track duplicate or generic access badges. Allowing badges to remain active after an employee has separated or transferred from the department exposes the department to risk where unauthorized individuals will continue to have physical access into sensitive areas within the department. This can lead to unauthorized individuals accessing county facilities and poses a threat to county assets and existing county personnel. The existence of duplicate badges enables individuals to access restricted areas without proper authorization, leading to potential theft, data breaches, or other malicious activities.

Generic badges do not tie actions to specific individuals, making it difficult to hold personnel accountable for security breaches or unauthorized access."

Current Status

Reported Finding Corrected? [X] **Yes** [ ] **No**

Recommendation 1.1

"Disable badge access within 24 hours of an employee's separation or transfer from the department."

Management Reply

"Concur. Current Sheriff policy requires all separating employees to return all issued equipment to either the assigned station/bureau, Uniform Services, and/or Sheriff's Admin on their final working day—this includes the employee ID card, which is also programmed for door access. Periodic human error may occur, whereas cards may become lost or personnel responsible for deactivation may occasionally fail to render an unused card deactivated—this is likely why there is such a small number of errant cards. Policies related to employee ID card access has been modified to assure proper deactivation of access is addressed and recorded.

Note: Due to the various and disparate door access control systems used throughout the department, the door access control systems are not tied to the agency Active Directory (AD); however, Sheriff's Project Management Office (PMO) is actively seeking an enterprise system to replace the system and access points at all Sheriff's facilities."

Actual/Estimated Date of Corrective Action: November, 2024

Current Status

Corrective Action: [ ] **Fully Implemented** [X] **Partially Implemented** [ ] **Not Implemented**

The Sheriff's Office is conducting market research to identify a qualified cloud-based system to integrate with Active Directory. In the meantime, an End of Service email notification is generated to prompt the immediate deactivation of security key cards for impacted employees.

Recommendation 1.2

"Develop a standardized process to review, approve, monitor, and disable duplicate badges and generic access badges."

"Management Reply

"Concur. Sheriff shall adopt a written policy detailing a process for staff to periodic review, approve, monitor, and disable duplicate badges and generic access badges. The policy should incorporate additional safeguards, to include the centralized management of

badges, and adopt measures to ensure that only authorized personnel have access to sensitive areas within the department, thereby maintaining a higher level of security and control. Policy changes with the existing system limitations in place should occur until an enterprise replacement solution is fully implemented."

Actual/Estimated Date of Corrective Action: November, 2024

Current Status

Corrective Action: [X] **Fully Implemented** [ ] **Partially Implemented** [ ] **Not Implemented**

Description of the corrective action taken (or pending action and estimated date of completion for planned corrective action that is partially or not implemented).

The Sheriff's Office has implemented as of December 2024 the End of Service Policy & Procedure and it is supported by department directive 16-010 End of Service Notification email group.

Recommendation 1.3

"Develop standardized policies and procedures over disabling badge access within 24 hours of an employee's separation or transfer from the department."

Management Reply

"**Concur** See response in Recommendation 1.2 (above)."

Actual/Estimated Date of Corrective Action: November, 2024

Current Status

Corrective Action: [X] **Fully Implemented** [ ] **Partially Implemented** [ ] **Not Implemented**

Description of the corrective action taken (or pending action and estimated date of completion for planned corrective action that is partially or not implemented).

The Sheriff's Office has implemented as of December 2024 the End of Service Policy & Procedure and it is supported by department directive 16-010 End of Service Notification email group.

Recommendation 1.4

"Develop standardized policies and procedures over managing the administration and disabling of duplicate badges and generic access badges, as well as establishing criteria for their creation and usage."

Management Reply

"**Concur** See response in Recommendation 1.2 (above)."

Actual/Estimated Date of Corrective Action: November, 2024
Current Status

Corrective Action: ☐ **Fully Implemented** ☒ **Partially Implemented** ☐ **Not Implemented**

Description of the corrective action taken (or pending action and estimated date of completion for planned corrective action that is partially or not implemented).

The Sheriff's Office has a written procedure to record the issuing and deactivating key cards in Active Directory Security System. The system generates reports identifying duplicate badges and generic access badges. The department needs to establish a criteria for the creation of duplicates and generic badges.

Finding 2: Timely Termination of System Access Rights

"County of Riverside Information Security Standard Revision 2.0, Section 4.16.4, *Personnel Termination,* states, 'County Departments and IT Administrators shall disable system access and retrieve all security-related organizational system-related property upon termination of individual employment'

Active Directory and non-Active Directory access rights were not terminated in a timely manner (within 24 hours). We identified the following:

• One hundred sixty-four out of 780 former employees (21%) did not have their Active Directory account termination requests created and approved in a timely manner. The average time elapsed between employee separation and ticket approval was 64 days, with the longest taking 504 days for approval and the shortest taking 4 days.

• For the system applications not linked to Active Directory, we were unable to determine whether access rights were terminated in a timely manner as the department does not track the date and time in which a separated employee's access was disabled. Additionally, for all five system applications selected for testing, separated employees continued to have access as of the fieldwork date. See Table A below for a summary of the results:

System	Observations
A	Of the 149 employees with access to System A enabled, one employee (<1%) separated from the department continued to have access to System A as of the fieldwork date.
B	Of the 3,244 employees with access to System B enabled, 35 employees (1%) separated from the department continued to have access to System B as of the fieldwork date.
C	Of the 1,639 employees with access to System C enabled, 156 employees (9%) separated from the department continued to have access to System C as of the fieldwork date.
D	Of the 3,429 employees with access to System D enabled, 20 employees (<1%) separated from the department continued to have access to System D as of the fieldwork date.
E	Of the 1,223 employees with access to System E enabled, 3 employees (<1%) separated from the department continued to have access to System E as of the fieldwork date.

Sheriff Department employees did not have their Active Directory account termination requests created and approved timely upon separation from the department. Additionally, the department's current policies and procedures do not include a process for identifying the system applications needing to be disabled upon an employee separating or transferring from the department. Allowing user accounts to remain open after employment has ended exposes the department to risk where information maintained in the department can be continuously accessed by individuals who no longer have a right or need to know. Depending on the sensitivity of the information maintained by department systems, it can create administrative issues and have a financial impact if held liable."

Current Status

Reported Finding Corrected? [X] **Yes** [ ] **No**

Riverside Sheriff, Technical Services Branch (T.S.B.) has created and implemented the End of Service Policy, which ensures the timely deactivation of user accounts for former employees. Policy specifically states that all access rights are removed/disabled within 24 hours of notification.

Recommendation 2.1

"Disable all user system accounts within 24 hours of an employee's separation from the department to remain compliant with County of Riverside Information Security Standard Revision 2.0, Section 4.16.4, *Personnel Termination."*

Management Reply

"**Concur**. Sheriff currently employs an 'End of Service' process (EOS) to identify, list, track, monitor, and deactivate access to all agency systems upon separation from the department, either immediately for contentious separations or within 24 hours following non-contentious separations. This process has been in place for many years and is considered a routine task for Sheriff's IT personnel. Deactivation occurs at the Active Directory (AD) level, as well as software license deactivation for enterprise systems. Current EOS process will be reviewed and modified to confirm the proper deactivation of all system applications access is addressed and properly documented."

Actual/Estimated Date of Corrective Action: November, 2024

Current Status

Corrective Action: [X] **Fully Implemented** [ ] **Partially Implemented** [ ] **Not Implemented**

Description of the corrective action taken (or pending action and estimated date of completion for planned corrective action that is partially or not implemented).

Riverside Sheriff, Technical Services Branch (T.S.B.) has created and implemented the End of Service Policy, which ensures the timely deactivation of user accounts for former employees. Policy specifically states that all access rights are removed/disabled within 24 hours of notification.

Recommendation 2.2

"Update policies and procedures to ensure the disabling of all user system accounts are requested and approved within 24 hours of an employee's separation or transfer from the department."

Management Reply

"**Concur.** Sheriff will ensure a written policy exists for this process—see response to Recommendation 1.2."

Actual/Estimated Date of Corrective Action: November, 2024

Current Status

Corrective Action: [X] **Fully Implemented** [ ] **Partially Implemented** [ ] **Not Implemented**

Description of the corrective action taken (or pending action and estimated date of completion for planned corrective action that is partially or not implemented).

Riverside Sheriff, Technical Services Branch (T.S.B.) has created and implemented the End of Service Policy, which ensures the timely deactivation of user accounts for former employees. Policy specifically states that all access rights are removed/disabled within 24 hours of notification.

Finding 3: Vulnerability Remediation Tracking

"County of Riverside Information Security Standard Revision v2.0, Section 4.17.4, *Vulnerability Scanning,* states, 'remediate legitimate vulnerabilities per an organizational assessment of risk... share information obtained from the vulnerability scanning process and control assessments with stakeholders and IT Administrators to help eliminate similar vulnerabilities.'

Remediation progress for unresolved system vulnerabilities need to be tracked and documented to ensure remediation steps available for vulnerabilities do not remain unresolved. Additionally, we noted multiple vulnerabilities during the audit period that were outstanding with no documented evidence of remediation progress. See Table B below for the number of total system vulnerabilities by severity as of the fieldwork date, April 26, 2024:

Table B: Number of Total System Vulnerabilities by Severity

Vulnerability Severity	Number of Vulnerabilities	Remediation Response Timeline
Critical	3,858	7 Days
High	6,856	14 Days
Medium	606	30 Days

Sheriff Department does not have a process in place to track remediation progress for unresolved vulnerabilities. The absence of tracking the remediation progress impedes the department's ability to closely monitor the implementation status and quickly mitigate any risks posed by the system vulnerabilities."

Current Status

Reported Finding Corrected? [X] **Yes** [ ] **No**

Policy and Procedure has been created and implemented, Endpoint Patch Management Policy, to assure scans, assessment and remediation of endpoint vulnerabilities are properly addressed as needed.

Recommendation 3

"Develop procedures to ensure remediation progress for unresolved vulnerabilities is adequately documented, tracked, assigned to personnel, and monitored."

Management Reply

"**Concur.** Sheriff's Technical Services Bureau (TSB) currently have staff responsible for monitoring, managing, and—in some cases—rejecting software patches after testing patch functionality following a release. Due to the varied and occasional specialized/custom nature of some agency applications, some commercial Operating System (OS) patches may render the impacted utility/service disabled—these threats are typically mitigated via network isolation. Sheriff's TSB will develop written protocols to maintain tracking of the remediation of potential system vulnerabilities based on their severity. This approach will enable close monitoring of the implementation status and progress, ensuring effective mitigation of any associated risks."

Actual/Estimated Date of Corrective Action: November, 2024

Current Status

Corrective Action: [X] **Fully Implemented** [ ] **Partially Implemented** [ ] **Not Implemented**

Description of the corrective action taken (or pending action and estimated date of completion for planned corrective action that is partially or not implemented).

A Policy and Procedure, titled Endpoint Patch Management Policy, has been developed and implemented to ensure the proper scanning, assessment, and remediation of endpoint vulnerabilities as needed. Additionally, processes have been established to address these vulnerabilities in accordance with the severity matrix outlined in the policy.

Finding 4: Server Upgrades

"NIST SP 800-40, *Procedures for Handling Security Patches*, states, 'Timely patching is critical to maintain the operational availability, confidentiality, and integrity of information technology (IT) systems.'

Nine of Sheriff Department's 89 system servers (10%) have not been upgraded to the available supported versions. Additionally, the department is relying on outdated server operating systems without having an Extended Security Update agreement with the respective suppliers. An Extended Security Update agreement is needed to acquire server updates after an operating system has rolled out. The department does not have a process in place to track remediation progress for unresolved vulnerabilities, such as using outdated system servers, and there are potential deployment errors that may affect the department applications when updating to the latest version. Outdated system servers may cause stability issues and contain known security vulnerabilities that individuals can exploit to gain unauthorized access to the applications running

on those servers. This can lead to data breaches, loss of sensitive information, and potential legal and financial consequences."

Recommendation 4

"Develop a process to ensure Sheriff Department's system servers are upgraded timely once a new, supported version becomes available."

Management Reply

"**Concur.** Sheriff's Technical Services Bureau (TSB) will conduct thorough research and develop a comprehensive process to establish and maintain a regular schedule for evaluating, verifying, and updating the operating systems of server infrastructure. This process will ensure that all servers are consistently up to date and fully supported, receiving all necessary critical updates and patches to maintain optimal security and performance."

Actual/Estimated Date of Corrective Action: November, 2024

Current Status

Corrective Action: [X] **Fully Implemented** [ ] **Partially Implemented** [ ] **Not Implemented**

Description of the corrective action taken (or pending action and estimated date of completion for planned corrective action that is partially or not implemented).

Sheriff T.S.B has developed and implemented the Server Patch Management Policy **to ensure that server upgrades are conducted as needed, maintaining security, performance, and compliance.**

Finding 5: Identifying and Prioritizing System Applications

"NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Section CP-2, *Contingency Planning*, states, 'Organizations identify critical system assets so that additional controls can be employed (beyond the controls routinely implemented) to help ensure that organizational mission and business functions can continue to be conducted during contingency operations. The identification of critical information assets also facilitates the prioritization of organizational resources.'

Sheriff Department needs to identify critical system applications and assign risk ratings to identify business dependencies that address resource prioritization and optimize patch management. The department does not have a process in place to assign risk ratings to critical and non-critical system applications for business dependencies relating to contingency planning. Not identifying critical system applications and assigning risk ratings can create operational challenges such as prioritization conflicts, security concerns, and delays in decision-making when system applications require major repairs and downtime.

On May 10, 2024, Sheriff Department identified and updated their listing of critical system applications to address the condition above and communicated their efforts to improve the adequacy and effectiveness of their internal controls. Specifically, the department assigned risk ratings and prioritized critical system applications to enhance patch management, security features, and functionality. In the follow-up audit, we will verify whether the department maintains and updates their critical system application listing to reflect all running applications."

Recommendation 5

"Develop policies and procedures to establish the frequency in which the department's listing of critical system applications is updated."

Management Reply

"**Concur.** Sheriff's Technical Services Bureau (TSB) will develop a process to regularly evaluate and categorize critical system applications. This will include verifying update status and completion to ensure all necessary critical updates and patches are applied for optimal security and performance."

Actual/Estimated Date of Corrective Action: November, 2024
Current Status

Corrective Action: [X] **Fully Implemented** [ ] **Partially Implemented** [ ] **Not Implemented**

Description of the corrective action taken (or pending action and estimated date of completion for planned corrective action that is partially or not implemented).

Sheriff T.S.B. has established and implemented an ongoing process to review, update, and verify the status of system applications as needed, ensuring their functionality, security, and compliance.

Finding 6: Memorandum of Understanding

"NIST SP 800-47, *Managing the Security of Information Exchanges*, states, 'To address information security requirements for system interconnections, an interconnection security agreement (ISA) that specifies the security requirements expected for the impact level of the information being exchanged for all participating systems is recommended. ISAs are often coupled with Memoranda of Understanding/Agreement (MOU/A).'

Sheriff Department currently relies on Riverside County Information Technology (Information Technology) for various services, including network architecture, network security, phishing training, vendor enterprise agreement, cyber insurance coverage, and vulnerability reports. However, there has not been an established Memorandum of Understanding between Sheriff Department and Information Technology. Not having an established Memorandum of Understanding creates responsibility gaps and disrupts formalized communication and procedural clarity regarding the transmission and acknowledgment from Sheriff Department and Information Technology. As such, Sheriff Department does not regularly receive vulnerability reports to assess their existing vulnerabilities. The existing informal communication channels do not ensure that critical security information reaches the intended recipients timely and reliably."

Recommendation 6

"Establish a formal Memorandum of Understanding with Information Technology that addresses roles, responsibilities, and expectations."

Management Reply

"**Concur.** Sheriff's Technical Services Bureau (TSB) shall develop and establish a comprehensive Memorandum of Understanding (MOU) between the Sheriff's Technical Services Bureau and

Riverside County Information Technology (RCIT). This MOU will clearly define IT-specific roles, system requirements, security protocols, and reporting standards to ensure effective collaboration and seamless service integration"

Actual/Estimated Date of Corrective Action: February, 2025

Current Status

Corrective Action: ☐ **Fully Implemented** ☐ **Partially Implemented** ☒ **Not Implemented**

Description of the corrective action taken (or pending action and estimated date of completion for planned corrective action that is partially or not implemented).

Following further research and verification with RCIT, it has been confirmed that no county departments have a valid MOU outlining IT-specific roles, system requirements, security protocols, and reporting standards. An RCIT representative will be coordinating with the auditors to provide clarification on this matter.

Riverside County Board of Supervisors
Request to Speak

Submit request to the Clerk of the Board (right of podium), Speakers are entitled to three (3) minutes, subject to Board Rules listed on the reverse side of this form. The Board may limit the public input on any item, based on the number of people requesting to speak and the business of the Board.

SPEAKER'S NAME: Roy Bleckley

Address: _____

City: _____ **Zip:** _____

Phone #: _____

Date: _____ **Agenda #** 2.10, 11, 12, 15, 16

PLEASE STATE YOUR POSITION BELOW:

Position on "Regular" (non-appealed) Agenda Item:

_____**Support** _____**Oppose** _____**Neutral**

Note: If you are here for an agenda item that is filed for "Appeal", please state separately your position on the appeal below:

_____**Support** _____**Oppose** _____**Neutral**

I give my 3 minutes to: _____

Parking validations available for speakers only – see Clerk of the Board.

(Revised: 04/23/2025)

BOARD RULES

Requests to Address Board on "Agenda" Items:
You may request to be heard on a published agenda item. Requests to be heard must be submitted to the Clerk of the Board before the scheduled meeting time.

Requests to Address Board on items that are "NOT" on the Agenda:
Notwithstanding any other provisions of these rules, member of the public shall have the right to address the Board during the mid-morning "Oral Communications" segment of the published agenda. Said purpose for address must pertain to issues which are under the direct jurisdiction of the Board of Supervisors. YOUR TIME WILL BE LIMITED TO THREE (3) MINUTES. The Board may limit the public input on any item, based on the number of people requesting to speak and the business of the Board.

Power Point Presentations/Printed Material:
Speakers who intend to conduct a formalized Power Point presentation or provide printed material must notify the Clerk of the Board's Office by 12 noon on the Monday preceding the Tuesday Board meeting, ensuring that the Clerk's Office has sufficient copies of all printed materials and at least one (1) copy of the Power Point CD. Copies of printed material given to the Clerk (by Monday noon deadline) will be provided to each Supervisor. If you have the need to use the overhead "Elmo" projector at the Board meeting, please ensure your material is clear and with proper contrast, notifying the Clerk well ahead of the meeting, of your intent to use the Elmo. Speakers are prohibited from bringing signs, placards, or posters into the hearing room.

Individual Speaker Limits:
Individual speakers are limited to a maximum of three (3) minutes. The Board may limit the public input on any item, based on the number of people requesting to speak and the business of the Board. Please step up to the podium when the Chair calls your name and begin speaking immediately. Pull the microphone to your mouth so that the Board, audience, and audio recording system hear you clearly. Once you start speaking, the "green" podium light will light. The "yellow" light will come on when you have one (1) minute remaining. When you have 30 seconds remaining, the "yellow" light will begin flash, indicating you must quickly wrap up your comments. Your time is up when the "red" light flashes. The Chair adheres to a strict three (3) minutes per speaker. ***Note: If you intend to give your time to a "Group/Organized Presentation", please state so clearly at the very bottom of the reverse side of this form.***

Group/Organized Presentations:
Group/organized presentations with more than one (1) speaker will be limited to nine (9) minutes at the Chair's discretion. The organizer of the presentation will automatically receive the first three (3) minutes, with the remaining six (6) minutes relinquished by other speakers, as requested by them on a completed "Request to Speak" form, and clearly indicated at the front bottom of the form.

Addressing the Board & Acknowledgement by Chair:
The Chair will determine what order the speakers will address the Board and will call on all speakers in pairs. The first speaker should immediately step to the podium and begin addressing the Board. The second speaker should take up a position in one of the chamber aisles to quickly step up to the podium after the preceding speaker. This is to afford an efficient and timely Board meeting, giving all attendees the opportunity to make their case. Speakers are prohibited from making personal attacks, and/or using course, crude, profane or vulgar language while speaking to the Board members, staff, the public and/or meeting participants. Such behavior, at the discretion of the Board Chair may result in removal from the Board Chambers by Sheriff Deputies.

Flores, Kate

From: Roy Bleckert <sprintcar166@gmail.com>
Sent: Monday, August 25, 2025 10:22 PM
To: Supervisor Medina - 1st District; Office of 2nd District Supervisor; District3; District 4 Supervisor V. Manuel Perez; District 5; Van Wagenen, Jeffrey; Benoit, Ben J; mtran@rivco.org; Clerk of the Board; Bianco, Chad; michaelhestrin@rivcoda.org; Sharp, Donald
Subject: AUDITS Agenda Items 2.10-20

My first observation is there seems to be a badge/access problem across multiple departments!

The non compliance of HWS in the Homeless area of compliance & documentation gaps in the 20 percentile raises BIG RED FLAGS!

These are a few of Many

- Thirteen of 57 (23%) program participant files did not have adequate supporting documentation to validate eligibility for the program.
- Fifteen of 57 (26%) program participant files and services provided were not reviewed and approved by designated individuals to ensure adequate segregation of duties.
- Fifteen of 57 (26%) program participant files and services provided did not have adequate oversight of the eligibility determination and benefits processing.

DPSS appears to be a complete dumpster fire!

Registrar of Voters not having a comprehensive plan & chain of command in case the election system shuts down is troubling !!!

--

Roy Bleckert..... 1 Rad Bad Dude !!!!!! 951 208 9967

2.10 - 2.20