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

ITEM: 2.3
(ID # 30469)
MEETING DATE:
Tuesday, June 02, 2026

FROM : AUDITOR CONTROLLER

SUBJECT: Auditor-Controller: Internal Audit Report 2026-311 Riverside County Registrar Of Voters, Follow-up Audit, [District: All]; [$0]

RECOMMENDED MOTION: That the Board of Supervisors:

1. Receive and file Internal Audit Report 2026-311 Riverside County Registrar of Voters, Follow-up Audit.

ACTION:Consent

Ben J. Benoit
Ben J. Benoit, COUNTY AUDITOR-CONTROLLER 5/20/2026

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:	June 2, 2026
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	

C.E.O. RECOMMENDATION: Approve

BACKGROUND:

Summary

We completed a follow-up audit of the Riverside County Registrar of Voters. Our audit was limited to reviewing actions taken as of January 29, 2026, to correct findings noted in our original audit report 2025-013 dated August 26, 2025. The original audit report contained ten recommendations, all of which required implementation to help correct the reported findings.

Based on the results of our audit, we found that of the ten recommendations, all were implemented.

For an in depth understanding of the original audit report, please refer to Internal Audit Report 2025-013 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.

SUPPLEMENTAL:

Additional Fiscal Information:

Not applicable.

ATTACHMENTS:

A: Riverside County Auditor-Controller - Internal Audit Report 2026-311 Riverside County Registrar of Voters, Follow-up Audit

Office of Ben J. Benoit

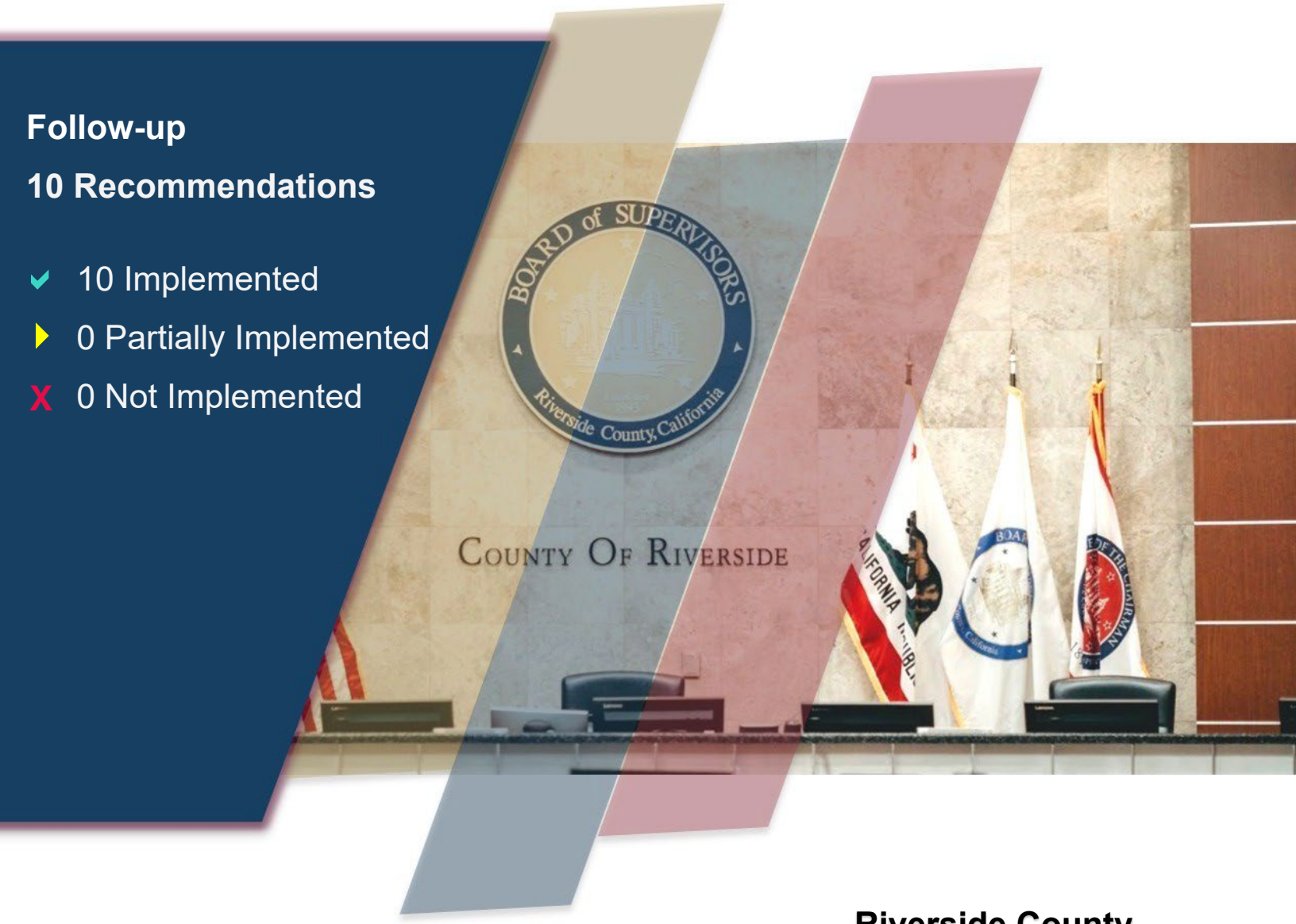
Riverside County Auditor-Controller

Internal Audit Report 2026-311

Follow-up

10 Recommendations

- ✔ 10 Implemented
- ▶ 0 Partially Implemented
- X 0 Not Implemented



Riverside County Registrar of Voters, Follow-up Audit

June 2, 2026

COUNTY OF RIVERSIDE
OFFICE OF THE AUDITOR-CONTROLLER
BEN J. BENOIT
AUDITOR-CONTROLLER
TANYA S. HARRIS, DPA, CPA | JON JENSEN, CPP
ASSISTANT AUDITOR-CONTROLLER

June 2, 2026

Art Tinoco
Registrar of Voters
Riverside County Registrar of Voters
2724 Gateway Dr.
Riverside, CA 92507

Subject: **Internal Audit Report 2026-311: Riverside County Registrar of Voters, Follow-up Audit**

Dear Mr. Tinoco:

We completed the follow-up audit of Riverside County Registrar of Voters. Our audit was limited to reviewing actions taken as of January 29, 2026, to help correct the findings noted in our original audit report 2025-013 dated August 26, 2025.

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, all were implemented.

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 2025-013 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
Don Kent, Chief Finance Officer
Grand Jury

Table of Contents

Physical Access Control Management

Finding 1: Badge Access System Limitations

"County of Riverside Information Security Standard Revision 2.0, Section 4.16.4, Personnel Termination, states, 'County Departments and IT Administrators shall upon termination of individual employment: disable system access; terminate or revoke any authenticators and credentials associated with the individual; and notify personnel as appropriate.' Additionally, County of Riverside Information Security Standard Revision 2.0, Section 4.3.3, Content of Audit Records, states, 'IT Administrators shall ensure that the system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.'

The department's badge access system is unable to provide deactivation dates due to limited reporting capabilities. As a result, we were unable to verify whether badge access to Registrar-occupied facilities was deactivated timely following employee separation or transfer from the department. In addition to these system limitations, Registrar does not have a manual process for tracking badge deactivations outside the system. Without the ability to track badge deactivation dates, the department cannot effectively verify or enforce timely revocation of physical access to Registrar-occupied facilities. This increases the risk of unauthorized access, which may lead to exposure of sensitive information or disruption of critical operations."

Recommendation 1.1

"Transition to the badge access system managed by Riverside County Information Technology to support more effective tracking, review, and timely deactivation of badge access. This ensures departmental technology remains within the county's centralized IT framework, promoting consistency and mitigating the risk of systems operating without proper oversight or integration."

Current Status 1.1: Implemented

Recommendation 1.2

"Develop and implement a process to manually track badge deactivations for systems that do not support the reporting of deactivation dates."

Current Status 1.2: Implemented

Recommendation 1.3

"Revise Registrar's Policy H-16, [Badge] System Access Rights, to include verbiage requiring that badge access be disabled within 24 hours of an employee's separation or transfer from the department, and to include documented approval for all deactivations."

Current Status 1.3: Implemented

Finding 2: Access Rights

"Standard Practice Manual 1001, Internal Control, states, 'Duties are divided or segregated so that no one person has complete control over a key function or activity.' Additionally, County of Riverside Information Security Standard Revision 2.0, Section 4.1.5, Separation of Duties, states, Document separation of duties of individuals,' and 'define system access authorizations to support separation of duties.'

Three employees have unrestricted access to a shared spreadsheet used to track badge additions and removals for temporary employees. This spreadsheet is maintained outside of the department's badge access system, and the number of temporary employees tracked in it increases during election periods when more temporary staff are onboarded. The department has not established appropriate access controls or segregation of duties for the shared spreadsheet, allowing multiple users to modify its contents without restriction. Without appropriate access controls and segregation of duties, unrestricted access to the shared badge tracking spreadsheet increases the risk of unauthorized modifications, data integrity issues, and undetected errors or malicious changes, potentially leading to inaccurate badge access records and security vulnerabilities."

Recommendation 2

"Implement access controls and segregation of duties for the shared badge tracking spreadsheet to ensure only authorized personnel can make changes and establish an audit trail to maintain the integrity of the records."

Current Status 2: Implemented

Finding 3: Monitoring Badge Activity Logs

"County of Riverside Information Security Standard Revision 2.0, Section 4.16.4, *Personnel Termination*, states, 'County Departments and IT Administrators shall upon termination of individual employment: disable system access; terminate or revoke any authenticators and credentials associated with the individual; and notify personnel as appropriate.' Additionally, NIST SP 800-53, Rev. 5, PE-2, *Physical Access Authorizations,* states, Review the access list

detailing authorized facility access by individuals' and 'remove individuals from the facility access list when access is no longer required.'

Registrar can generate badge access logs that track badge usage within department-maintained facilities. However, documentation demonstrating a formal review and approval process for these logs - particularly for critical areas and sensitive operational periods - is not maintained. As a result, we could not determine whether badge access logs are regularly reviewed and approved. The department does not have a process in place to perform or document such reviews. Regular monitoring of badge activity, especially in areas housing critical systems and sensitive information, and during restricted or non-standard timeframes, enables the department to identify suspicious behavior and respond proactively to potential security threats. Consistent review of access data also strengthens the department's ability to investigate incidents by offering clearer insight into access patterns and anomalies. In the event of a security issue, this information supports quicker, more effective responses and helps establish accountability by identifying individuals involved."

Recommendation 3.1

"Develop and implement a process to periodically monitor and review badge activity-focusing on critical areas and sensitive operational timeframes - and document the results to identify anomalies or potential unauthorized access."

Current Status 3.1: Implemented

Recommendation 3.2

"Revise Registrar's Policy H-16, *[Badge] System Access Rights,* to incorporate procedures for periodic monitoring and review of badge activity in critical areas and during sensitive operational timeframes to detect anomalies or suspicious behavior."

Current Status 3.2: Implemented

Application Controls

Finding 4: Timely Terminations of System Access

"Registrar's Policy H-15, *Timely Termination of System Access Rights*, states, 'The Registrar of Voters will create and approve Employee Termination Tickets via the RCIT [service management system] in a timely manner to ensure disabling of accounts for departed employees within 24 hours of their departure.' Additionally, County of Riverside Information Security Standard Revision 2.0, Section 4.16.4, *Personnel Termination,* states, 'County Departments and IT Administrators shall upon termination of individual employment: disable system access; terminate or revoke any authenticators and credentials associated with the individual; and notify personnel as appropriate.'

Six out of eight (75%) employees who separated from the department and had access to the election management system did not have their access revoked timely. As of April 29, 2025, one of these accounts remained active, despite the employee having separated from the department on September 29, 2023. On average, it took 37 days to deactivate access following separation, with the longest delay being 76 days and the shortest being 2 days. Requests to deactivate election management system accounts were not submitted within 24 hours of employee separation or transfer from the department. Additionally, the department indicated that certain accounts are intentionally kept active to preserve access to critical historical information that is otherwise unavailable. Not promptly disabling access to the department's election management system after employee separation or transfer increases the risk of unauthorized access and reduces assurance over system integrity. Timely deactivation helps ensure that only current personnel have access, supporting sound access control practices and promoting confidence in the department's security protocols."

Recommendation 4.1

"Ensure deactivation requests for election management system accounts are submitted within 24 hours of employee separation or transfer from the department."

Current Status 4.1: Implemented

Recommendation 4.2

"Collaborate with Riverside County Information Technology to establish and implement a process to archive or transfer critical historical information from user accounts prior to employee separation, allowing accounts to be deactivated timely."

Current Status 4.2: Implemented

Finding 5: Downtime Procedures for Business Continuity

"NIST SP 800-53, Rev. 5, Section 3.6, *Contingency Planning,* CP-1, *Policies and Procedures,* states, 'Develop, document, and disseminate ... a contingency planning policy that: Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance... [and] includes procedures to facilitate implementation of the contingency planning policy and associated controls.' Additionally, Standard Practice Manual 1001, *Internal Control,* states that, to maintain an effective system of internal control, 'Well-documented policies and procedures are established and maintained to promote employee understanding of job duties, provide day-to-day guidance to staff and help ensure continuity during employee absences or turnover.'

The Registrar has not developed written procedures for continuing operations in the event the election management system becomes unavailable due to downtime or an emergency. While the department has a *Continuity of Operations and Continuity of Government Plan* that addresses critical functions, recovery priorities, leadership succession, and emergency coordination, it does not include specific manual procedures for operating without the system. In such cases, the department relies on general State guidance and informal support from neighboring counties. Without written procedures for continuing operations during election management system downtime or emergencies, there is an increased risk of delays or inconsistencies in carrying out certain election functions. While general State guidance and support from neighboring counties may provide some assistance, formally documented processes can help promote clearer roles, more timely responses, and continuity of operations that are specific and unique to department processes and expectations."

Recommendation 5.1

"Develop detailed, written procedures that outline how critical election functions will be carried out in the event the election management system becomes unavailable. These should include manual workarounds, communication protocols, and clearly defined roles and responsibilities."

Current Status 5.1: Implemented

Recommendation 5.2

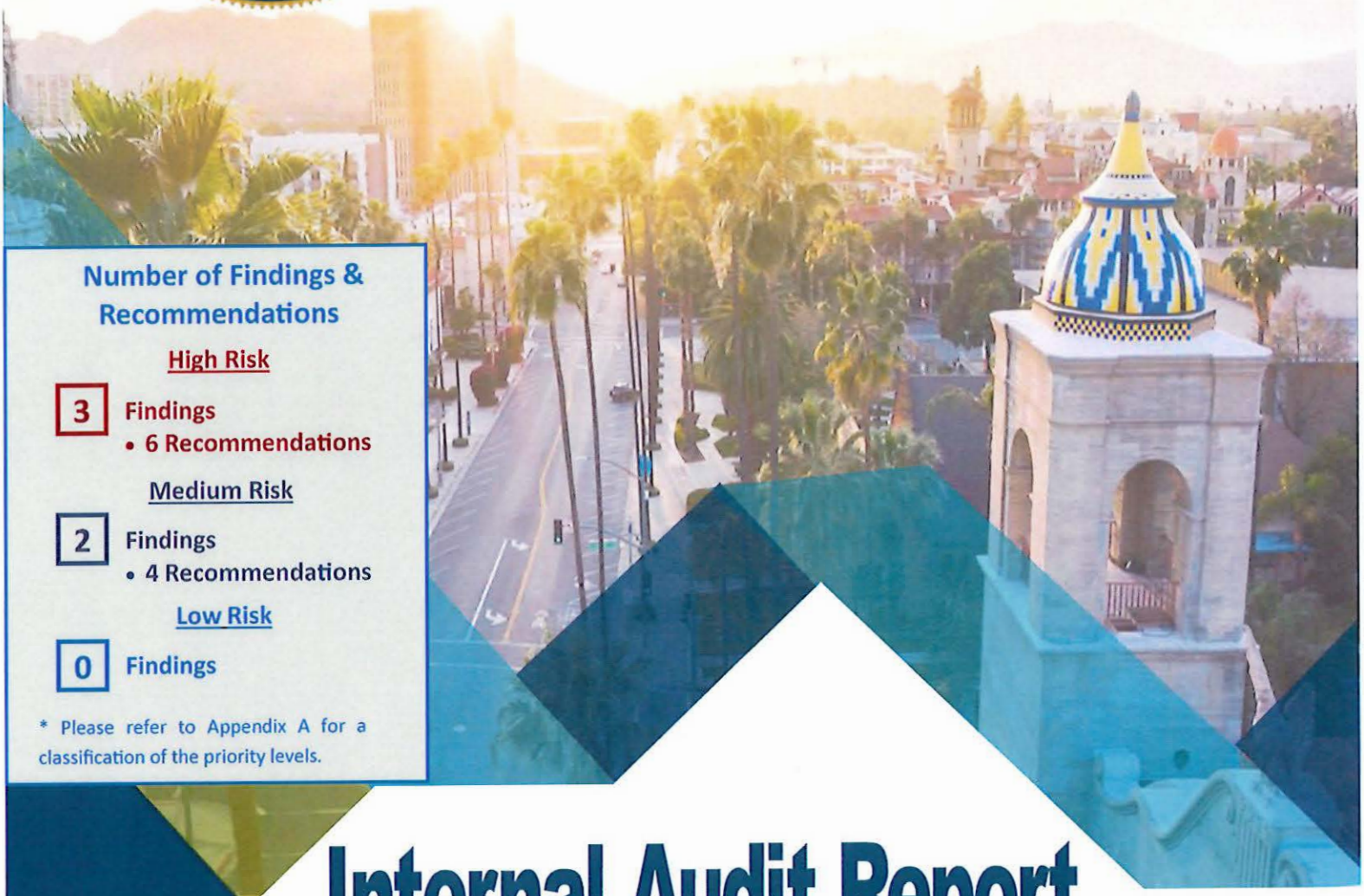
"Periodically test the election management system downtime procedures through tabletop exercises or simulations and document the results to identify improvement areas and support staff preparedness."

Current Status 5.2: Implemented

Attachment A

Office of Ben J. Benoit

Riverside County Auditor-Controller



Number of Findings & Recommendations

High Risk

3 Findings
- 6 Recommendations

Medium Risk

2 Findings
- 4 Recommendations

Low Risk

0 Findings

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

Internal Audit Report

2025-013

Riverside County Registrar of Voters Audit

August 26, 2025

COUNTY OF RIVERSIDE
OFFICE OF THE AUDITOR-CONTROLLER

BEN J. BENOIT, AUDITOR-CONTROLLER
TANYA S. HARRIS, DPA, CPA,
ASSISTANT AUDITOR-CONTROLLER

August 26, 2025

Art Tinoco
Registrar of Voters
Riverside County Registrar of Voters
2724 Gateway Dr.
Riverside, CA 92507

Subject: **Internal Audit Report 2025-013: Riverside County Registrar of Voters Audit**

Dear Mr. Tinoco:

In accordance with Board of Supervisors Resolution 83-338, we audited the Riverside County Registrar of Voters to provide management and the Board of Supervisors with an independent assessment of internal controls over physical access control management and application controls.

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 2025-013: Riverside County Registrar of Voters 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
Juan Perez, Chief Operating Officer
Grand Jury

Table of Contents

Executive Summary

Overview

The Registrar of Voters (Registrar) is responsible for providing equal access for all eligible citizens in Riverside County to participate in the democratic process. The Registrar is also entrusted with protecting the integrity of votes and maintaining transparent, accurate, and fair elections for federal, state, and local offices.

Registrar has an adopted budget of $26.5 million for FY 2024/25 and 54 adopted positions. *County of Riverside, Fiscal Year 2024/25 Adopted Budget Volume I, 319-322.*

Audit Objective

Our objective is to provide management and the Board of Supervisors with an independent assessment of the adequacy and effectiveness of internal controls over physical access control management and application controls. 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 February 3, 2025, through May 22, 2025, for operations from July 1, 2022, through May 5, 2025.

Using a risk-based approach, our scope included the following:

- Physical Access Control Management
- Application Controls

AUDIT HIGHLIGHTS

- Badge deactivation dates need to be documented and tracked independently of the current badge access system.
- Access controls and segregation of duties need to be established over badge tracking spreadsheets.
- Badge activity logs need to be periodically monitored and reviewed for anomalies or suspicious activity.
- Separated employee access rights to the election management system need to be deactivated timely.
- Written procedures need to be developed for continuing operations in the event the election management system becomes unavailable.

Audit Conclusion

Based on the results of our audit, we have identified improvement opportunities for internal controls over physical access control management and application controls that can help provide reasonable assurance that the department's objectives relating to these areas will be achieved. Specifically, the improvement opportunities are as follows: Badge deactivation dates need to be documented and tracked independently of the current badge access system, access controls and segregation of duties need to be established over badge tracking spreadsheets, badge activity logs need to be periodically monitored and reviewed for anomalies or suspicious activity, separated employee access rights to the election management system need to be deactivated timely, and written procedures need to be developed for continuing operations in the event the election management system becomes unavailable.

Physical Access Control Management

Background

Access control management is a crucial component of information security that involves the establishment, maintenance, and enforcement of policies and procedures to manage access to information systems, resources, and physical facilities within an organization. Access control management plays a vital role in safeguarding sensitive data, maintaining the integrity of systems, and protecting against unauthorized access or breaches. Access extends to physical access control, ensuring that only authorized personnel can enter secure areas or buildings. It is essential for protecting physical assets and sensitive information stored in physical locations.

Badge access controls serve as a fundamental component in establishing and maintaining a secure physical environment within the organization. Badge access controls are essential for regulating and monitoring entry and exit points, aligning with the overarching objective of fortifying the organization's security infrastructure. The utilization of identification badges or electronic access cards contributes to the establishment of robust internal controls, ensuring that access permissions are intricately configured in adherence to organizational security policies and regulatory standards. By objectively assessing the design and functionality of the badge access system, the department can identify any potential vulnerabilities or inefficiencies and determine enhancements that bolster the organization's overall physical security measures.

Below, we detail some examples of instances where lapses in security measures have occurred:

- Aurora, Illinois – Henry Pratt Company Shooting (2019): A terminated employee returned to their former job and opened fire, killing five coworkers and injuring several police officers. The employee had reportedly been fired for disciplinary reasons earlier that day.[1]

- Arlington, Virginia – Reagan National Airport (2013): A former contractor used an unreturned Security Identification Display Area (SIDA) security badge to slip into restricted airport areas, leading to his arrest on trespassing and burglary charges.[2]

- Multnomah County, Oregon (2019): A county employee was dismissed from their job but briefly continued to have access to county records where they were able to obtain the names and social security numbers of 40 clients.[3]

---

[1] "Aurora, Illinois, Gunman Who Fatally Shot 5 Vowed to Kill All His Co-Workers If He Was Fired." NBCNews.com, NBCUniversal News Group, 29 Apr. 2019.

[2] "Security Badge Breach at Reagan National Airport." NBCWashington.com, NBCUniversal News Group, 24 Apr. 2013.

[3] "Press Release: Multnomah County Reports Security Breach after Employee Termination" | Multnomah County. Multnomah County, 2 July 2019.

These incidents highlight the critical importance of access control policies. Ensuring badges are promptly deactivated and collected after termination, and continuously monitoring access permissions is essential to prevent such tragedies and maintain security.

Objective

To verify the existence and adequacy of internal controls over Registrar's physical access control management processes.

Audit Methodology

To accomplish these objectives, we:

- Conducted interviews with key personnel to gain an understanding of the department's physical access control management processes.

- Obtained and reviewed relevant policies and procedures related to physical access control management, including Riverside County Information Security Standard Revision 2.0 and Registrar's Policy H-16, *[Badge] System Access Rights*.

- Obtained listings of all badge access systems used by the department.

- Obtained and reviewed listings of active and separated employees, as well as employee time-off records during the audit period.

- Obtained and reviewed reports of active, deactivated, and temporary badges.

- Verified whether badge access for separated employees was disabled within 24 hours and supported by sufficient documentation.

- Verified whether badge activity occurred during weekends, holidays, time off, or outside of normal working hours.

- Verified whether any employees had access rights exceeding those of peers in similar roles.

- Verified whether controls over temporary badges were adequate and supported by proper documentation and approvals.

- Verified whether lost or stolen badges were reported and deactivated in a timely manner, and whether issuance of replacements was properly documented.

- Verified whether badge access points were secure, properly maintained, and fully operational.

Finding 1: Badge Access System Limitations	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 upon termination of individual employment: disable system access; terminate or revoke any authenticators and credentials associated with the individual; and notify personnel as appropriate." Additionally, County of Riverside Information Security Standard Revision 2.0, Section 4.3.3, *Content of Audit Records*, states, "IT Administrators shall ensure that the system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event."

The department's badge access system is unable to provide deactivation dates due to limited reporting capabilities. As a result, we were unable to verify whether badge access to Registrar-occupied facilities was deactivated timely following employee separation or transfer from the department. In addition to these system limitations, Registrar does not have a manual process for tracking badge deactivations outside the system. Without the ability to track badge deactivation dates, the department cannot effectively verify or enforce timely revocation of physical access to Registrar-occupied facilities. This increases the risk of unauthorized access, which may lead to exposure of sensitive information or disruption of critical operations.

Recommendation 1.1

Transition to the badge access system managed by Riverside County Information Technology to support more effective tracking, review, and timely deactivation of badge access. This ensures departmental technology remains within the county's centralized IT framework, promoting consistency and mitigating the risk of systems operating without proper oversight or integration.

Management's Response:

"**Concur.** The department will be transitioning to a badge access system managed by Riverside County Information Technology (RCIT)."

Actual/Estimated Date of Corrective Action: "June 30, 2026 (*Subject to contingent funding and partnership with the Riverside County Assessor-County Clerk-Recorder's Department, who share building access*)."

[4] Please see Appendix A (page 17) for a description of the finding priority level classifications.

Recommendation 1.2

Develop and implement a process to manually track badge deactivations for systems that do not support the reporting of deactivation dates.

Management's Response:

"**Concur.** The department will implement a manual process for tracking badge deactivation, until the new RCIT badge system is fully implemented. Once the RCIT badge system is operational this manual process will be discontinued."

Actual/Estimated Date of Corrective Action: "July 28, 2025"

Recommendation 1.3

Revise Registrar's Policy H-16, *[Badge] System Access Rights,* to include verbiage requiring that badge access be disabled within 24 hours of an employee's separation or transfer from the department, and to include documented approval for all deactivations.

Management's Response:

"**Concur.** The department will revise Policy H-16 to include verbiage requiring badge access be disabled within 24 hours of an employee's separation or transfer. All deactivations will require documented approval."

Actual/Estimated Date of Corrective Action: "July 28, 2025"

Finding 2: Access Rights	Priority Level: 1[5]

Standard Practice Manual 1001, *Internal Control*, states, "Duties are divided or segregated so that no one person has complete control over a key function or activity." Additionally, County of Riverside Information Security Standard Revision 2.0, Section 4.1.5, *Separation of Duties*, states, "Document separation of duties of individuals," and "define system access authorizations to support separation of duties."

Three employees have unrestricted access to a shared spreadsheet used to track badge additions and removals for temporary employees. This spreadsheet is maintained outside of the department's badge access system, and the number of temporary employees tracked in it

[5] Please see Appendix A (page 17) for a description of the finding priority level classifications.

increases during election periods when more temporary staff are onboarded. The department has not established appropriate access controls or segregation of duties for the shared spreadsheet, allowing multiple users to modify its contents without restriction. Without appropriate access controls and segregation of duties, unrestricted access to the shared badge tracking spreadsheet increases the risk of unauthorized modifications, data integrity issues, and undetected errors or malicious changes, potentially leading to inaccurate badge access records and security vulnerabilities.

Recommendation 2

Implement access controls and segregation of duties for the shared badge tracking spreadsheet to ensure only authorized personnel can make changes and establish an audit trail to maintain the integrity of the records.

Management's Response:

"**Partially Concur.** Previously, the Registrar of Voters managed a shared spreadsheet, which was accessed solely by three administrative staff members and maintained an audit trail via Excel tracking. To enhance this process the ROV will implement access controls and segregation of duties for the shared badged tracking spreadsheet to ensure only authorized personnel can make changes and to establish an audit trail maintaining the integrity of the records."

Actual/Estimated Date of Corrective Action: "July 28, 2025"

Finding 3: Monitoring Badge Activity Logs — Priority Level: 2[6]

County of Riverside Information Security Standard Revision 2.0, Section 4.16.4, *Personnel Termination*, states, "County Departments and IT Administrators shall upon termination of individual employment: disable system access; terminate or revoke any authenticators and credentials associated with the individual; and notify personnel as appropriate." Additionally, NIST SP 800-53, Rev. 5, PE-2, *Physical Access Authorizations*, states, "Review the access list detailing authorized facility access by individuals" and "remove individuals from the facility access list when access is no longer required."

Registrar can generate badge access logs that track badge usage within department-maintained facilities. However, documentation demonstrating a formal review and approval process for these logs – particularly for critical areas and sensitive operational periods – is not maintained. As a result, we could not determine whether badge access logs are regularly reviewed and approved. The department does not have a process in place to perform or document such reviews. Regular

[6] Please see Appendix A (page 17) for a description of the finding priority level classifications.

monitoring of badge activity, especially in areas housing critical systems and sensitive information, and during restricted or non-standard timeframes, enables the department to identify suspicious behavior and respond proactively to potential security threats. Consistent review of access data also strengthens the department's ability to investigate incidents by offering clearer insight into access patterns and anomalies. In the event of a security issue, this information supports quicker, more effective responses and helps establish accountability by identifying individuals involved.

Recommendation 3.1

Develop and implement a process to periodically monitor and review badge activity – focusing on critical areas and sensitive operational timeframes – and document the results to identify anomalies or potential unauthorized access.

Management's Response:

"**Partially Concur.** The department currently has a process in effect to periodically review badge activity. To enhance this process, the ROV will incorporate additional monitoring measures and provide more detailed tracking of badge activity."

Actual/Estimated Date of Corrective Action: "July 28, 2025"

Auditor's Comment

During our audit fieldwork, the department was unable to provide documentation demonstrating a formal process to periodically review badge activity. As a result, we could not verify whether such reviews were being performed or whether they occurred consistently. In the follow-up audit, we will verify whether the department has developed and implemented a documented review process that outlines the frequency, scope, and responsible personnel for monitoring badge activity in critical areas and during sensitive timeframes.

Recommendation 3.2

Revise Registrar's Policy H-16, *[Badge] System Access Rights*, to incorporate procedures for periodic monitoring and review of badge activity in critical areas and during sensitive operational timeframes to detect anomalies or suspicious behavior.

Management's Response:

"**Concur.** The department will revise Policy H-16, *[Badge] System Access Rights*, to include procedures for periodic monitoring and review of badge activity in critical areas and during sensitive operational timeframes."

Actual/Estimated Date of Corrective Action: "July 28, 2025"

Application Controls

Background

Application controls are automated and manual safeguards embedded within software applications that are used to initiate, process, record, and report transactions. These controls are designed to ensure the accuracy, completeness, validity, and authorization of data as it moves through various stages of processing. They play a critical role in supporting the reliability of financial reporting, operational efficiency, and regulatory compliance.

Application controls are typically categorized into input, processing, output, and access controls. When designed and implemented effectively, these controls help reduce the risk of errors, omissions, and unauthorized activity within business processes. This includes controls over user access – such as granting, modifying, and deactivating user accounts – to ensure that only authorized individuals can access sensitive data and system functions.

In addition to transactional and access-related controls, effective application management also involves maintaining written procedures to guide staff in the event of system downtime or disruptions. Such documentation supports continuity of operations and helps ensure that critical processes can resume with minimal interruption.

As organizations increasingly rely on automated systems to perform critical operations, the strength of application controls becomes essential to maintaining the integrity of data and ensuring consistent and reliable outcomes.

Objective

To verify the existence and adequacy of internal controls over Registrar's application controls processes.

Audit Methodology

To accomplish these objectives, we:

- Conducted interviews with key personnel to gain an understanding of the department's application controls processes and systems.

- Obtained and reviewed relevant policies and procedures, including Riverside County Information Security Standard Revision 2.0.

- Obtained a listing of critical system applications and judgmentally selected the department's election management system for testing.

- Obtained listings of active employees and those separated from the department during the audit review period.

- Obtained user access listings for the election management system and verified whether access rights for separated employees were removed timely.

- Verified whether access approvals to the election management system were properly documented and still valid.

- Verified whether adequate segregation of duties existed within the department's application controls processes.

- Verified whether manual procedures were established for use during system outages and whether data backup processes were implemented and performed regularly.

- Obtained an understanding of how sensitive information is managed, including its type, format, and applicable legal requirements.

- Reviewed written procedures to assess whether controls effectively safeguard sensitive information and ensure compliance with laws and information security standards.

Finding 4: Timely Terminations of System Access	Priority Level: 1[7]

Registrar's Policy H-15, *Timely Termination of System Access Rights*, states, "The Registrar of Voters will create and approve Employee Termination Tickets via the RCIT [service management

[7] Please see Appendix A (page 17) for a description of the finding priority level classifications.

system] in a timely manner to ensure disabling of accounts for departed employees within 24 hours of their departure." Additionally, County of Riverside Information Security Standard Revision 2.0, Section 4.16.4, *Personnel Termination,* states, "County Departments and IT Administrators shall upon termination of individual employment: disable system access; terminate or revoke any authenticators and credentials associated with the individual; and notify personnel as appropriate."

Six out of eight (75%) employees who separated from the department and had access to the election management system did not have their access revoked timely. As of April 29, 2025, one of these accounts remained active, despite the employee having separated from the department on September 29, 2023. On average, it took 37 days to deactivate access following separation, with the longest delay being 76 days and the shortest being 2 days. Requests to deactivate election management system accounts were not submitted within 24 hours of employee separation or transfer from the department. Additionally, the department indicated that certain accounts are intentionally kept active to preserve access to critical historical information that is otherwise unavailable. Not promptly disabling access to the department's election management system after employee separation or transfer increases the risk of unauthorized access and reduces assurance over system integrity. Timely deactivation helps ensure that only current personnel have access, supporting sound access control practices and promoting confidence in the department's security protocols.

Recommendation 4.1

Ensure deactivation requests for election management system accounts are submitted within 24 hours of employee separation or transfer from the department.

Management's Response:

"**Partially Concur**. The department ensures deactivation requests for Election Management System accounts are submitted within 24 hours of an employee's separation, unless continued access is needed by supervisors or executive staff to maintain operations."

Actual/Estimated Date of Corrective Action: "December 31, 2025"

Auditor's Comment

The delays noted in this finding are based on when the department submitted deactivation requests relative to the employees' separation dates. Available documentation showed that six of the eight requests were not submitted within 24 hours of separation, with delays ranging from 2 to 76 days. In the follow-up audit, we will verify whether the department is submitting

deactivation requests for election management system accounts within 24 hours of employee separation or transfer.

Recommendation 4.2

Collaborate with Riverside County Information Technology to establish and implement a process to archive or transfer critical historical information from user accounts prior to employee separation, allowing accounts to be deactivated timely.

Management's Response:

"**Concur**. To address historical data management, we will partner with RCIT to develop and implement formal procedures for archiving or securely transferring critical historical records."

Actual/Estimated Date of Corrective Action: "January 30, 2026"

Finding 5: Downtime Procedures for Business Continuity | **Priority Level: 2[8]**

NIST SP 800-53, Rev. 5, Section 3.6, *Contingency Planning*, CP-1, *Policies and Procedures*, states, "Develop, document, and disseminate... a contingency planning policy that: Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance... [and] includes procedures to facilitate implementation of the contingency planning policy and associated controls." Additionally, Standard Practice Manual 1001, *Internal Control*, states that, to maintain an effective system of internal control, "Well-documented policies and procedures are established and maintained to promote employee understanding of job duties, provide day-to-day guidance to staff and help ensure continuity during employee absences or turnover."

The Registrar has not developed written procedures for continuing operations in the event the election management system becomes unavailable due to downtime or an emergency. While the department has a *Continuity of Operations and Continuity of Government Plan* that addresses critical functions, recovery priorities, leadership succession, and emergency coordination, it does not include specific manual procedures for operating without the system. In such cases, the department relies on general State guidance and informal support from neighboring counties. Without written procedures for continuing operations during election management system downtime or emergencies, there is an increased risk of delays or inconsistencies in carrying out certain election functions. While general State guidance and support from neighboring counties may provide some assistance, formally documented processes can help promote clearer roles,

[8] Please see Appendix A (page 17) for a description of the finding priority level classifications.

more timely responses, and continuity of operations that are specific and unique to department processes and expectations.

Recommendation 5.1

Develop detailed, written procedures that outline how critical election functions will be carried out in the event the election management system becomes unavailable. These should include manual workarounds, communication protocols, and clearly defined roles and responsibilities.

Management's Response:

"**Partially Concur**. We maintain a reliable partnership with both our EMS vendor and the California Secretary of State (SOS). In the event of a system outage, we will follow the SOS contingency guidance to ensure uninterrupted election operations. The department will also develop comprehensive, written procedures detailing how essential election functions will be managed if the Election Management System becomes unavailable."

Actual/Estimated Date of Corrective Action: "February 27, 2026"

Recommendation 5.2

Periodically test the election management system downtime procedures through tabletop exercises or simulations and document the results to identify improvement areas and support staff preparedness.

Management's Response:

"**Partially Concur.** We conduct simulation exercises before each election to validate our processes. Our primary system of record is VoteCal, the statewide voter registration database managed by the California Secretary of State. We will continue working closely with the Secretary of State and our EMS vendor to test and validate system functionality and resilience before each election."

Actual/Estimated Date of Corrective Action: "December 31, 2025"

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.

Art Tinoco
Registrar of Voters

Registrar of Voters

RivCo VOTE
Your Voice. Every Vote. Our Future.

Matthew Ceballos
Assistant Registrar of Voters

The following are the current status of the reported findings and planned corrective actions contained in Internal Audit Report 2025-013: Riverside County Registrar of Voters Audit.

1/29/2026

Authorized Signature **Date**

Finding 1: Badge Access System Limitations

"County of Riverside Information Security Standard Revision 2.0, Section 4.16.4, Personnel Termination, states, 'County Departments and IT Administrators shall upon termination of individual employment: disable system access; terminate or revoke any authenticators and credentials associated with the individual; and notify personnel as appropriate.' Additionally, County of Riverside Information Security Standard Revision 2.0, Section 4.3.3, Content of Audit Records, states, 'IT Administrators shall ensure that the system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.'

The department's badge access system is unable to provide deactivation dates due to limited reporting capabilities. As a result, we were unable to verify whether badge access to Registrar-occupied facilities was deactivated timely following employee separation or transfer from the department. In addition to these system limitations, Registrar does not have a manual process for tracking badge deactivations outside the system. Without the ability to track badge deactivation dates, the department cannot effectively verify or enforce timely revocation of physical access to Registrar-occupied facilities. This increases the risk of unauthorized access, which may lead to exposure of sensitive information or disruption of critical operations."

Current Status

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

The department has implemented a formal manual process to track and document badge deactivation, including deactivation dates, for all employee separations and transfers. This interim control ensures timely revocation of physical access and compliance with County Information Security Standards. In parallel, the department is actively advancing implementation of the RCIT-managed badge access system, which will provide enhanced audit logging and reporting capabilities. The department anticipates timely completion.

Art Tinoco
Registrar of Voters

Registrar of Voters

RivCo VOTE
Your Voice. Every Vote. Our Future.

Matthew Ceballos
Assistant Registrar of Voters

Recommendation 1.1

"Transition to the badge access system managed by Riverside County Information Technology to support more effective tracking, review, and timely deactivation of badge access. This ensures departmental technology remains within the county's centralized IT framework, promoting consistency and mitigating the risk of systems operating without proper oversight or integration."

Management Reply

"**Concur**. The department will be transitioning to a badge access system managed by Riverside County Information Technology (RCIT)."

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 department has made measurable progress toward completion of this recommendation by securing Service Agreements with RCIT to evaluate the cost and requirements for transitioning to the RCIT-managed badge access system. The department anticipates timely completion.

Recommendation 1.2

"Develop and implement a process to manually track badge deactivations for systems that do not support the reporting of deactivation dates."

Management Reply

"**Concur.** The department will implement a manual process for tracking badge deactivation, until the new RCIT badge system is fully implemented. Once the RCIT badge system is operational this manual process will be discontinued."

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 department has implemented a formal manual process to track and document badge deactivation, including deactivation dates, for all employee separations and transfers. This interim control ensures timely revocation of physical access and compliance with County Information Security Standards. In parallel, the department is actively advancing implementation of the RCIT-managed badge access system, which will provide enhanced audit logging and reporting capabilities. The department anticipates timely completion.

Recommendation 1.3

"Revise Registrar's Policy H-16, [Badge] System Access Rights, to include verbiage requiring that badge access be disabled within 24 hours of an employee's separation or transfer from the department, and to include documented approval for all deactivations."

Management Reply

"**Concur**. The department will revise Policy H-16 to include verbiage requiring badge access be disabled within 24 hours of an employee's separation or transfer. All deactivations will require documented approval."

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 department has taken corrective action to enhance physical access controls. Policy H-16 has been revised to require badge access be disabled within 24 hours of an employee's separation or transfer and to require documented approval for all badge deactivations.

Finding 2: Access Rights

"Standard Practice Manual 1001, Internal Control, states, 'Duties are divided or segregated so that no one person has complete control over a key function or activity.' Additionally, County of Riverside Information Security Standard Revision 2.0, Section 4.1.5, Separation of Duties, states, 'Document separation of duties of individuals,' and 'define system access authorizations to support separation of duties.'

Three employees have unrestricted access to a shared spreadsheet used to track badge additions and removals for temporary employees. This spreadsheet is maintained outside of the

department's badge access system, and the number of temporary employees tracked in it increases during election periods when more temporary staff are onboarded. The department has not established appropriate access controls or segregation of duties for the shared spreadsheet, allowing multiple users to modify its contents without restriction. Without appropriate access controls and segregation of duties, unrestricted access to the shared badge tracking spreadsheet increases the risk of unauthorized modifications, data integrity issues, and undetected errors or malicious changes, potentially leading to inaccurate badge access records and security vulnerabilities."

Current Status

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

The department has implemented access controls with segregation of duties for the shared badge tracking spreadsheet, ensuring only authorized personnel can make changes and all modifications are fully auditable. These controls align with Standard Practice Manual 1001 and County of Riverside Information Security Standard Revision 2.0, Section 4.1.5, by documenting duties and defining system access authorizations. These measures reduce the risk of unauthorized changes, data integrity issues, and errors, while preparing the department for a seamless transition to the RCIT-managed badge access system.

Recommendation 2

"Implement access controls and segregation of duties for the shared badge tracking spreadsheet to ensure only authorized personnel can make changes and establish an audit trail to maintain the integrity of the records."

Management Reply

"**Partially Concur**. Previously, the Registrar of Voters managed a shared spreadsheet, which was accessed solely by three administrative staff members and maintained an audit trail via Excel tracking. To enhance this process the ROV will implement access controls and segregation of duties for the shared badged tracking spreadsheet to ensure only authorized personnel can make changes and to establish an audit trail maintaining the integrity of the records."

Current Status

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

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 department has implemented access controls with segregation of duties for the shared badge tracking spreadsheet, ensuring only authorized personnel can make changes and all modifications are fully auditable.

Finding 3: Monitoring Badge Activity Logs

"County of Riverside Information Security Standard Revision 2.0, Section 4.16.4, Personnel Termination, states, 'County Departments and IT Administrators shall upon termination of individual employment: disable system access; terminate or revoke any authenticators and credentials associated with the individual; and notify personnel as appropriate.' Additionally, NIST SP 800-53, Rev. 5, PE-2, Physical Access Authorizations, states, 'Review the access list detailing authorized facility access by individuals' and 'remove individuals from the facility access list when access is no longer required.'

Registrar can generate badge access logs that track badge usage within department-maintained facilities. However, documentation demonstrating a formal review and approval process for these logs - particularly for critical areas and sensitive operational periods - is not maintained. As a result, we could not determine whether badge access logs are regularly reviewed and approved. The department does not have a process in place to perform or document such reviews. Regular monitoring of badge activity, especially in areas housing critical systems and sensitive information, and during restricted or non-standard timeframes, enables the department to identify suspicious behavior and respond proactively to potential security threats. Consistent review of access data also strengthens the department's ability to investigate incidents by offering clearer insight into access patterns and anomalies. In the event of a security issue, this information supports quicker, more effective responses and helps establish accountability by identifying individuals involved."

Current Status

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

The department has taken corrective action to enhance monitoring of badge activity. Policy H-16 has been revised to require periodic review and documented approval of badge access logs, with emphasis on critical areas and sensitive operational periods. These updates ensure access is monitored consistently, potential security threats are identified proactively, and accountability for facility access is maintained.

Recommendation 3.1

"Develop and implement a process to periodically monitor and review badge activity-focusing on critical areas and sensitive operational timeframes - and document the results to identify anomalies or potential unauthorized access."

Management Reply

"Partially Concur. The department currently has a process in effect to periodically review badge activity. To enhance this process, the ROV will incorporate additional monitoring measures and provide more detailed tracking of badge activity."

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 department has revised Policy H-16 to establish periodic monitoring and documented review of badge activity, with a focus on critical areas and sensitive operational periods. These enhancements provide more detailed tracking of access, enable identification of anomalies or potential unauthorized activity, and ensure accountability for facility access.

Recommendation 3.2

"Revise Registrar's Policy H-16, [Badge] System Access Rights, to incorporate procedures for periodic monitoring and review of badge activity in critical areas and during sensitive operational timeframes to detect anomalies or suspicious behavior."

Management Reply

"Concur. The department will revise Policy H-16, [Badge] System Access Rights, to include procedures for periodic monitoring and review of badge activity in critical areas and during sensitive operational timeframes."

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 department has revised Policy H-16 to establish periodic monitoring and documented review of badge activity, with a focus on critical areas and sensitive operational periods. These enhancements provide more detailed tracking of access, enable identification of anomalies or potential unauthorized activity, and ensure accountability for facility access.

Finding 4: Timely Terminations of System Access

"Registrar's Policy H-15, Timely Termination of System Access Rights, states, 'The Registrar of Voters will create and approve Employee Termination Tickets via the RCIT [service management system] in a timely manner to ensure disabling of accounts for departed employees within 24 hours of their departure.' Additionally, County of Riverside Information Security Standard Revision 2.0, Section 4.16.4, Personnel Termination, states, 'County Departments and IT Administrators shall upon termination of individual employment: disable system access; terminate or revoke any authenticators and credentials associated with the individual; and notify personnel as appropriate.'

Six out of eight (75%) employees who separated from the department and had access to the election management system did not have their access revoked timely. As of April 29, 2025, one of these accounts remained active, despite the employee having separated from the department on September 29, 2023. On average, it took 37 days to deactivate access following separation, with the longest delay being 76 days and the shortest being 2 days. Requests to deactivate election management system accounts were not submitted within 24 hours of employee separation or transfer from the department. Additionally, the department indicated that certain accounts are intentionally kept active to preserve access to critical historical information that is otherwise unavailable. Not promptly disabling access to the department's election management system after employee separation or transfer increases the risk of unauthorized access and reduces assurance over system integrity. Timely deactivation helps ensure that only current personnel have access, supporting sound access control practices and promoting confidence in the department's security protocols."

Current Status

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

The department has reinforced Policy H-15 to ensure Election Information Management System accounts are deactivated within 24 hours of employee separation or transfer. Accounts requiring continued access to preserve critical historical information are now managed through formal procedures with RCIT for secure archiving or transfer.

Recommendation 4.1

"Ensure deactivation requests for election management system accounts are submitted within 24 hours of employee separation or transfer from the department."

Management Reply

"**Partially Concur.** The department ensures deactivation requests for Election Management System accounts are submitted within 24 hours of an employee's separation, unless continued access is needed by supervisors or executive staff to maintain operations."

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 department ensures deactivation requests for Election Information Management System accounts are submitted within 24 hours of an employee's separation or transfer. Policy H-15 has been reinforced to formalize this requirement, and any accounts requiring continued access for historical purposes are managed through secure archiving or transfer procedures in coordination with RCIT.

Recommendation 4.2

"Collaborate with Riverside County Information Technology to establish and implement a process to archive or transfer critical historical information from user accounts prior to employee separation, allowing accounts to be deactivated timely."

Management Reply

"**Concur.** To address historical data management, we will partner with RCIT to develop and implement formal procedures for archiving or securely transferring critical historical records."

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 department, in coordination with RCIT, has implemented formal procedures to archive or securely transfer critical historical records from user accounts prior to employee separation. This process ensures accounts are deactivated promptly while maintaining access to essential historical information.

Finding 5: Downtime Procedures for Business Continuity

"NIST SP 800-53, Rev. 5, Section 3.6, Contingency Planning, CP-1, Policies and Procedures, states, 'Develop, document, and disseminate ... a contingency planning policy that: Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance... [and] includes procedures to facilitate implementation of the contingency planning policy and associated controls.' Additionally, Standard Practice Manual 1001, Internal Control, states that, to maintain an effective system of internal control, 'Well-documented policies and procedures are established and maintained to promote employee understanding of job duties, provide day-to-day guidance to staff and help ensure continuity during employee absences or turnover.'

The Registrar has not developed written procedures for continuing operations in the event the election management system becomes unavailable due to downtime or an emergency. While the department has a Continuity of Operations and Continuity of Government Plan that addresses critical functions, recovery priorities, leadership succession, and emergency coordination, it does not include specific manual procedures for operating without the system. In such cases, the department relies on general State guidance and informal support from neighboring counties.

Without written procedures for continuing operations during election management system downtime or emergencies, there is an increased risk of delays or inconsistencies in carrying out certain election functions. While general State guidance and support from neighboring counties may provide some assistance, formally documented processes can help promote clearer roles, more timely responses, and continuity of operations that are specific and unique to department processes and expectations."

Current Status

Reported Finding Corrected? ☐ **Yes** ☒ **No**

Development of comprehensive, system specific manual procedures is currently underway, and the department is actively working to finalize these procedures. Pending full implementation of these procedures, the department will adhere to the Secretary of State's contingency guidance to maintain uninterrupted election operations during any system outage.

Recommendation 5.1

"Develop detailed, written procedures that outline how critical election functions will be carried out in the event the election management system becomes unavailable. These should include manual workarounds, communication protocols, and clearly defined roles and responsibilities."

Management Reply

"**Partially Concur.** We maintain a reliable partnership with both our EIMS vendor and the California Secretary of State (SOS). In the event of a system outage, we will follow the SOS contingency guidance to ensure uninterrupted election operations. The department will also develop comprehensive, written procedures detailing how essential election functions will be managed if the Election Information Management System becomes unavailable."

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 department maintains a reliable partnership with both our Election Information Management System (EIMS) vendor and the California Secretary of State (SOS). In the event of a system outage, the department will follow SOS contingency guidance to ensure uninterrupted election operations. Concurrently, the department is actively developing comprehensive, system specific written procedures detailing how essential election functions will be managed if the EIMS becomes unavailable. The estimated completion date for full implementation is February 27, 2026.

Recommendation 5.2

"Periodically test the election management system downtime procedures through tabletop exercises or simulations and document the results to identify improvement areas and support staff preparedness."

Management Reply

"**Partially Concur.** We conduct simulation exercises before each election to validate our processes. Our primary system of record is VoteCal, the statewide voter registration database managed by the California Secretary of State. We will continue working closely with the Secretary of State and our EIMS vendor to test and validate system functionality and resilience before each election."

Art Tinoco
Registrar of Voters

Registrar of Voters

RivCo VOTE
Your Voice. Every Vote. Our Future.

Matthew Ceballos
Assistant Registrar of Voters

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 department conducts simulation exercises before each election to validate downtime procedures. We work closely with the Secretary of State and our EIMS vendor to test system functionality and resilience. Results are documented to identify improvement opportunities and ensure staff preparedness for any system outage.