

**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, 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
- ✗ 0 Not Implemented



COUNTY OF RIVERSIDE

**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.

TEL:
(951) 955-3800

ADDRESS:
4080 Lemon Street, 6th Floor
Riverside, CA 92501

WEB:
<https://auditorcontroller.org>



Internal Audit Report 2026-311: Riverside County Registrar of Voters, 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 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

	Page
Results:	
Physical Access Control Management.....	4
Application Controls.....	7
Attachments:	
A. Internal Audit Report 2025-013	
B. Status of Findings as Reported by Riverside County Registrar of Voters on January 29, 2026	



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