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

ITEM: 2.8
(ID # 22660)
MEETING DATE:
Tuesday, August 29, 2023

FROM : AUDITOR CONTROLLER:

SUBJECT: AUDITOR-CONTROLLER: Internal Audit Report 2023-020: Riverside County Registrar of Voters Audit, All Districts. [$0]

RECOMMENDED MOTION: That the Board of Supervisors:

1. Receive and file Internal Audit Report 2023-020: Riverside County Registrar of Voters Audit

ACTION:Consent

Ben J. Benoit, COUNTY AUDITOR-CONTROLLER 8/15/2023

MINUTES OF THE BOARD OF SUPERVISORS

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

Ayes:	Jeffries, Spiegel, Perez, Washington, and Gutierrez
Nays:	None
Absent:	None
Date:	August 29, 2023
xc:	Auditor-controller

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	$ 0.00	$ 0.00	$ 0.00	$ 0.00
NET COUNTY COST	$ 0.00	$ 0.00	$ 0.00	$ 0.00
SOURCE OF FUNDS: N/A			Budget Adjustment:	No
			For Fiscal Year:	n/a

C.E.O. RECOMMENDATION: Approve

BACKGROUND:

Summary

In accordance with Board of Supervisors Resolution 83-338, we audited the Riverside County Registrar of Voters Audit. This audit is conducted to provide management and the Board of Supervisors with an independent assessment of internal controls over safeguarding of personally identifiable information and system access controls.

Based upon the results of our audit, we identified opportunities for improvement of internal controls relating to safeguarding of personally identifiable information and system access controls.

We will follow-up in one year to determine if actions were taken to correct the findings noted.

Impact on Residents and Businesses

Provide an assessment of internal controls over the audited areas.

Additional Fiscal Information

Not applicable.

ATTACHMENTS:

A: Riverside County Auditor-Controller's Office - Internal Audit Report 2023-020: Riverside County Registrar of Voters Audit

Internal Audit Report 2023-020

Riverside County
Registrar of Voters
Audit

Report Date: August 29, 2023

AUDITOR CONTROLLER
COUNTY OF RIVERSIDE

Office of Ben J. Benoit
Riverside County Auditor-Controller
4080 Lemon Street, 11th Floor
Riverside, CA 92509
(951) 955-3800

www.auditorcontroller.org

COUNTY OF RIVERSIDE
OFFICE OF THE
AUDITOR-CONTROLLER

County Administrative Center
4080 Lemon Street, 11th Floor
P.O. Box 1326
Riverside, CA 92502-1326
(951) 955-3800
Fax (951) 955-3802

AUDITOR CONTROLLER
COUNTY OF RIVERSIDE

Ben J. Benoit
Riverside County Auditor-Controller

Tanya S. Harris, DPA, CPA
Assistant Auditor-Controller

August 29, 2023

Rebecca Spencer
Registrar of Voters
Riverside County Registrar of Voters
2724 Gateway Dr.
Riverside, CA 92507

Subject: **Internal Audit Report 2023-020: Riverside County Registrar of Voters Audit**

Dear Ms. Spencer:

In accordance with Board of Supervisors Resolution 83-338, we completed an audit of the Riverside County Registrar of Voters to provide management and the Board of Supervisors with an independent assessment of internal controls over safeguarding of personally identifiable information and system access 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.

AUDITOR CONTROLLER
COUNTY OF RIVERSIDE

Internal Audit Report 2023-020: 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
Dave Rogers, Chief Administrative Officer
Grand Jury

AUDITOR CONTROLLER
COUNTY OF RIVERSIDE

Table of Contents

Page

Executive Summary 4

Results:

Safeguarding of Personally Identifiable Information. 7

System Access Controls. 10

AUDITOR CONTROLLER
COUNTY OF RIVERSIDE

Internal Audit Report 2023-020: Riverside County Registrar of Voters Audit

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 of Voters has a recommended budget of $14.3 million for FY 2023/24 and 42 recommended positions to execute its responsibilities *County of Riverside, Fiscal Year 2023/24 Recommended Budget, 323.*

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 safeguarding of personally identifiable information and system access 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 22, 2023, through June 13, 2023, for operations from July 1, 2021, through June 7, 2023. Following a risk-based approach, our scope initially included the following:

- Operating Expenditures
- Safeguarding of Personally Identifiable Information
- System Access Controls

Through inquiry, observations, and limited examination of relevant documentation, it was determined through a risk assessment of the business processes for operating expenditures, that the risk exposure to the Registrar associated with these processes are well mitigated with internal controls and are functioning as designed. Therefore, we focused our audit scope to internal controls over safeguarding of personally identifiable information and system access controls.

Internal Audit Report 2023-020: Riverside County Registrar of Voters Audit

Audit Highlights

Summary of Existing Conditions

- Currently, there is no written employee acknowledgement in place to affirm employee understanding of handling personally identifiable information (PII). The absence of such employee acknowledgement of understanding can lead to unaddressed misinterpretation of information, decreased accountability in staff and management, and increased risk in unauthorized access to PII.

- System access rights to identify active accounts for employees no longer with the department is not actively monitored. Lack of management monitoring increases the risk of untimely update to system access rights, resulting increased vulnerability to privileged information and liability to the County.

- Active Directory access rights for separated employees were not disabled timely. Additionally, an account remained active as of May 25, 2023, after an employee ended employment with the department. When an account is not closed immediately after an employee separation or transfer, there is a security risk to the information maintained in the systems used by the department.

Summary of Improvement Opportunities

- Establish and collect employee acknowledgement receipts of PII handling. The department can consider utilizing the Riverside County Human Resources' provided training on *Personally Identifiable Information* to keep records of employee training.

- Develop department policies and procedures to ensure written employee acknowledgement forms are completed and collected for newly onboarded employees to affirm employee understanding of handling PII.

- Perform a department review of system access rights to confidential information and update system security access rights in accordance with California Code of Regulations, Title 2, Division 7, Chapter 1, Article 1, §19012, *Requirements for Storage and Security of Voter Registration Information.*

- Develop policies and procedures to ensure timely management review and updates to system access rights.

- Communicate with Riverside County Information Technology department for an alternative to archiving former employees' electronic records for business use instead of maintaining their email accounts active after employee separation.

- Develop policies and procedures to ensure the disabling of accounts are requested and approved within 24 hours of an employee separation or transfer from the department.

Audit Conclusion

Based upon the results of our audit, we identified opportunities for improvement of internal controls relating to safeguarding of personally identifiable information and system access controls.

Internal Audit Report 2023-020: Riverside County Registrar of Voters Audit

Safeguarding of Personally Identifiable Information

Background

Personally identifiable information (PII) is any direct or indirect information that can be used to identify a specific individual. This information includes an individual name, address, social security number, date of birth, email address, phone number, passport number, or driver's license number. State Election Code Section 2194, (b) (1), states, "Notwithstanding any other law, the California driver's license number, the California identification card number, the social security number, and any other unique identifier used by the State of California for purposes of voter identification shown on the affidavit of voter registration of a registered voter, or added to voter registration records {...} are confidential and shall not be disclosed to any person." Government Code, *Voter Information,* §7924.000 (a), states, "Except as provided in Section 2194 of the Elections Code, both of the following are confidential and shall not be disclosed to any person: (1) The home address, telephone number, email address, precinct number, or other number specified by the Secretary of State for voter registration purposes.(2) Prior registration information shown on an affidavit of registration."

The department collects and maintains PII of voters to mail out ballots. Physical copies of voter registrations are maintained in an area with limited access.

Objective

To verify the existence and adequacy of internal controls over safeguarding of PII.

Audit Methodology

To accomplish these objectives, we:

- Obtained an understanding of Board Policy A-58, California Election Codes 2194, and California Code of Regulations, Title 2, Division 7, Chapter 1, Article 1, §19012, *Requirements for Storage and Security of Voter Registration Information.*
- Requested the department policies and procedures over training on PII.
- Conducted interviews and performed walk-throughs with department's personnel over safeguarding of PII.
- Verified if training on PII is provided to employees.
- Verified if copies of employee training acknowledgement are maintained.

- Performed on-site visit to review records management, records destruction, and verified access to physical originals containing PII is restricted.
- Verified if access to applications which store PII is updated to remove departed employees.

Finding 1: Employee Acknowledgement of PII Training

The department provides California Election Codes 2194 regarding voters' handling of PII training to new employees. Requiring written employee acknowledgement forms is currently not in place to affirm employee understanding of handling PII. Riverside County Standard Practice Manual 1001, *Internal Control*, states, "Well-documented policies and procedures are established and maintained to promote employee understanding of job duties." The department does not have policies and procedures that mandate the use of acknowledgement forms from employees to confirm their agreement to and commitment in following proper PII handling protocols. Lack of employee acknowledgement of understanding can lead to unaddressed misinterpretation of information, decreased accountability in staff and management, and increased risk in unauthorized access to PII.

Recommendation 1.1:

Establish and collect employee acknowledgement forms of PII handling. The department can consider utilizing the Riverside County Human Resources' provided training on *Personally Identifiable Information* to keep records of employee training.

Management's Response:

"**Concur.** All staff are currently trained on the confidentiality of PII. We will add a written employee acknowledgement form as part of our new employee orientation packet."

Actual/Estimated Date of Corrective Action: September 1, 2023.

Recommendation 1.2:

Develop department policies and procedures to ensure written employee acknowledgement forms are completed and collected for new employees to affirm employee understanding of handling PII.

Internal Audit Report 2023-020: Riverside County Registrar of Voters Audit

Management's Response:

"**Concur.** All staff are currently trained on the confidentiality of PII. We will add a written employee acknowledgement form as part of our new employee orientation packet."

Actual/Estimated Date of Corrective Action: January 1, 2024.

Finding 2: Monitoring System Access rights

Access rights to identify active accounts for employees no longer with the department are not actively monitored. Three former temporary assignment program employees continue to have access to the Registrar's election information management system (As of May 25, 2023). California Code of Regulations, Title 2, Division 7, Chapter 1, Article 1, §19012, *Requirements for Storage and Security of Voter Registration Information,* (b)(2)(B) and (b)(2)(D), states, "Any person who has directly or indirectly obtained voter registration information from a source agency shall practice the principles of "least privilege" by restricting user access to the minimum need based on users' job necessity", and "Remove, deactivate, or disable accounts or default credentials." The department does not have procedures to monitor system access rights periodically. Lack of management monitoring increases the risk of untimely update to system access rights, resulting increased vulnerability to privileged information and liability to the county.

Recommendation 2.1:

Perform periodic department reviews of system access rights to confidential information and update system security access rights in accordance with California Code of Regulations, Title 2, Division 7, Chapter 1, Article 1, §19012, *Requirements for Storage and Security of Voter Registration Information.*

Management's Response:

"**Concur.** Management currently reviews system access rights prior to each election. We will increase the frequency in which system access rights are reviewed."

Actual/Estimated Date of Corrective Action: January 1, 2024.

Internal Audit Report 2023-020: Riverside County Registrar of Voters Audit

Recommendation 2.2:

Develop policies and procedures to ensure timely management review and updates to system access rights.

Management's Response:

"**Concur.** Management currently reviews system access rights prior to each election. We will increase the frequency in which system access rights are reviewed."

Actual/Estimated Date of Corrective Action: January 1, 2024.

System Access Controls

Background

System access controls within information systems ensure proper confidentiality, integrity, and availability to the data stored within the system. Sensitive information is any information that must be protected from unauthorized access to maintain the information security of an organization or an individual. Authentication is a control which confirms a user's identity to provide access to a systems sensitive information. Authentication is often achieved by using login credentials such as a username and password. Authentication relies on the presumption that the user is authorized to use the system and that only the user knows the login credentials to gain access.

Active Directory is a directory service which allows Riverside County Information Technology and the County Registrar of Voters to manage permissions and access to network resources, and linked data applications utilized by the department. When a user ends employment with the Registrar, it is the department's responsibility to create and approve a help desk ticket to request the removal of the departed employees' access rights to their Active Directory account. Once the ticket is approved by the Registrar's personnel, Riverside County Information Technology is notified to disable Active Directory to remove permissions and network access.

System applications can be linked to Active Directory in a such a way that terminating Active Directory accounts will also terminate access to the linked system applications. For system applications not linked to Active Directory, county departments must manually terminate accounts for employees no longer employed with the department.

Additionally, external agencies or entities may grant Riverside County employees' access to system applications, at which point it is the responsibility of county departments to request account terminations upon an employee's separation from the department.

Objective

To verify the existence and adequacy of internal controls over system access rights upon employee separation.

Audit Methodology

To accomplish these objectives, we:

- Obtained an understanding of County of Riverside Information Security Standard v1.0.
- Interviewed key personnel regarding the department's employee access termination processes.
- Obtained a listing of employees who had access to Active Directory during the audit review period.
- Obtained report from Riverside County Information Technology that detailed Registrar of Voters ticket creation and approval dates for disabling employee access to Active Directory.
- Verified whether access rights to the system applications linked to Active Directory were disabled within 24 hours of employee departure from the department.
- Verified whether requests to disable Active Directory access right were created and approved by department personnel within 24 hours of the employee departure from the department.

Finding 3: Timely Termination of Access Rights

Employee access right termination requests are not created and approved in a timely manner. See Table A for a summary of findings.

Table A: Summary of Conditions/Concerns - System Access Controls

System	Findings
Active Directory	Seven out of 7 (100%) separated employees did not have their Active Directory account termination requests created and approved in a timely manner. The average time elapsed between employee departure and ticket approval was 78 days, with the longest taking 173 days for approval and the shortest taking 5 days.
	One out of 7 (14%) separated employees remained active as of June 7, 2023, 356 days after employee departure.

County of Riverside Information Security Standard v1.0, Section 4.1, *Account and Access Management*, states, "Accounts for terminated or transferred employees shall be disabled or removed on the day of termination or transfer." Written procedures to ensure the compliance with 24-hour disabling of accounts for departed employees as stated in Riverside County Information Technology Security Standards are currently not in place. Additionally, the Registrar stated Active Directory accounts were kept active to allow access to the former employees' email accounts. Allowing accounts to remain open after employment has ended exposes the department to risk where information maintained in department systems 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 3.1:

Communicate with Riverside County Information Technology department for an alternative to archiving former employees' electronic records for business use instead of maintaining their email addresses active after employee separation.

Management's Response:

"**Partially Concur.** Our current practice is to change all passwords for departed employees. This ensures that the employees no longer have access but allows for the department to continue to have access to their electronic files for cross training purposes. We will work with RCIT to for an alternative solution."

Actual/Estimated Date of Corrective Action: January 1, 2024.

Internal Audit Report 2023-020: Riverside County Registrar of Voters Audit

Recommendation 3.2:

Develop policies and procedures to ensure the disabling of accounts are requested and approved within 24 hours of an employee separation or transfer from the department.

Management's Response:

"**Partially Concur.** Our current practice is to change all passwords for departed employees. This ensures that the employees no longer have access but allows for the department to continue to have access to their electronic files for cross training purposes. We will work with RCIT to for an alternative solution."

Actual/Estimated Date of Corrective Action: January 1, 2024.