INTERNAL AUDIT DEPARTMENT

First & Final Close-Out Follow-Up
Information Technology Audit:
OCIT Selected Internet of Things (IoT)
Device Security Controls
As of June 30, 2025

Audit No. 2314-F1
Report Date: December 18, 2025

Recommendation Status

2	Implemented
0	In Process
0	Not Implemented
0	Closed

OC Board of Supervisors

CHAIR DOUG CHAFFEE
4th DISTRICT

VICE CHAIR KATRINA FOLEY
5th DISTRICT

SUPERVISOR JANET NGUYEN
1st DISTRICT

SUPERVISOR VICENTE SARMIENTO
2nd DISTRICT

SUPERVISOR DONALD P. WAGNER
3rd DISTRICT

INTERNAL AUDIT DEPARTMENT

Audit No. 2314-F1

December 18, 2025

To: KC Roestenberg
Chief Information Officer

From: Aggie Alonso, CPA, CIA, CRMA
Internal Audit Department Director

Digitally signed by
Agripino Alonso
Date: 2025.12.18 11:21:51
-08'00'

Subject: First & Final Close Out Follow-Up Information Technology Audit: OCIT Selected Internet of Things (IoT) Device Security Controls

---

We have completed a follow-up audit of Selected Internet of Things (IoT) Device Security Controls administered or monitored by OCIT as of June 30, 2025, original Audit No. 2314, dated December 17, 2024. Additional information, including background and our scope, is included in Appendix A.

We followed up on the status of the two recommendations from our original audit and concluded that OCIT implemented all recommendations. Therefore, this report represents the final close-out of the original audit. Due to the sensitive nature of the findings, we issued the original report as restricted. However, now that the department has implemented the recommendations and taken corrective action to address the vulnerabilities, we are issuing this final close-out report publicly, consistent with our new restricted reporting protocols.

We appreciate the assistance extended to us by OCIT personnel during our follow-up audit. If you have any questions, please contact me at (714) 834-5442 or Deputy Director Jose Olivo at (714) 834-5509.

Attachments

Other recipients of this report:
Members, Board of Supervisors
Members, Audit Oversight Committee
County Executive Office Distribution
OCIT Distribution
Foreperson, Grand Jury
Robin Stieler, Clerk of the Board
Eide Bailly LLP, County External Auditor

RESULTS

FINDING NO. 1	**Privileged Generic Accounts** Two of OCIT's critical systems, including the badge reader device management system and surveillance camera system, contained generic user accounts with administrative access which reduces accountability for system activity and increases the risk of unauthorized access to sensitive and critical data. Also, the systems did not have role-based user access controls to ensure access rights aligned with job responsibilities. Additionally, OCIT staff were sharing the badge reader device management system and surveillance camera system software vendors' default administrative account.
CATEGORY	**Significant Control Weakness**
RECOMMENDATION	OCIT: A. Document the business purpose and obtain approval for necessary generic accounts; otherwise, eliminate or disable the accounts. B. Collaborate with [redacted] software vendor to implement robust access controls to further meet County policy.
STATUS	**Implemented.** OCIT recently combined these two critical systems into one system, disabled unnecessary generic accounts, and ensured that all remaining active accounts were unique and assigned to employees with a business need. In addition, we confirmed that OCIT collaborated with the [redacted] software vendor to enhance access controls, including disabling the software default administrator account and implementing role-based user access to ensure access rights align with job responsibilities. Based on the actions taken by OCIT, we consider this recommendation implemented.

FINDING NO. 2	**Outdated Software Version** OCIT was using an outdated employee badge reader device management system that was no longer supported by the system vendor and lacked certain IT controls, such as user access controls and security audit logging capabilities.
CATEGORY	**Control Finding**
RECOMMENDATION	OCIT collaborate with [redacted] software vendor to upgrade the software to ensure the following security controls are implemented: A. Robust logical access controls. B. Security event audit logging reporting features to clearly show user activities in the systems.

STATUS	**Implemented.** We confirmed OCIT implemented a new badge reader management system that enforces role-based user access controls to ensure account profiles align with job responsibilities. In addition, the system now includes audit logging features that record user activity and configuration changes by documenting the user, date, and specific modifications. Based on the actions taken by OCIT, we consider this recommendation implemented.

AUDIT TEAM	Michael Dean, CPA, CIA, CISA	Assistant Deputy Director
	Jimmy Nguyen, CISA, CFE, CEH	Senior IT Audit Manager
	Michael Steinhaus, CISA, CIA, CPA	IT Audit Manager
	JC Lim, CIA, CISA, CFE	Senior IT Auditor
	Gabriela Cabrera, CIA	Administrative Services Manager

APPENDIX A: ADDITIONAL INFORMATION

SCOPE	Our follow-up audit was limited to reviewing actions taken by OCIT as of June 30, 2025, to implement the two recommendations from our original audit, dated December 17, 2024.
BACKGROUND	In the original audit, we reviewed selected Internet of Things (IoT) device security controls administered or monitored by OCIT and identified one Significant Control Weakness and one Control Finding.

APPENDIX B: FOLLOW-UP AUDIT IMPLEMENTATION STATUS

Implemented	In Process	Not Implemented	Closed
The department has implemented our recommendation in all respects as verified by the follow-up audit. No further follow-up is required.	The department is in the process of implementing our recommendation. Additional follow-up may be required.	The department has taken no action to implement our recommendation. Additional follow-up may be required.	Circumstances have changed surrounding our original finding/ recommendation that: (1) make it no longer applicable or (2) the department has implemented and will only implement a portion of our recommendation. No further follow-up is required.