# INTERNAL AUDIT DEPARTMENT

## First & Final Close-Out Follow-Up Information Technology Audit: OC Public Works Selected Cybersecurity Controls As of June 30, 2025

**Audit No. 2414-F1**
**Report Date: October 27, 2025**

### Recommendation Status

| | |
|---|---|
| 4 | Implemented |
| 0 | In Process |
| 0 | Not Implemented |
| 0 | Closed |

# INTERNAL AUDIT DEPARTMENT

Audit No. 2414-F1

October 27, 2025

To: Kevin Onuma, PE
OC Public Works Director

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

Digitally signed by Agripino Alonso
Date: 2025.10.27 13:05:08 -07'00'

Subject: First & Final Close Out Follow-Up Information Technology Audit: OC Public Works Selected Cybersecurity Controls

---

We have completed a follow-up audit of OC Public Works Selected Cybersecurity Controls as of June 30, 2025, original Audit No. 2414 dated March 31, 2025. Details of our results immediately follow this letter. Additional information, including background and our scope, is included in Appendix A.

We followed up on the status of the four recommendations from our original audit and concluded that OC Public Works 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 OC Public Works 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
OC Public Works Distribution
Foreperson, Grand Jury
Robin Stieler, Clerk of the Board
Eide Bailly LLP, County External Auditor

## RESULTS

| | |
|---|---|
| **FINDING NO. 1** | **User Account Creation Process**<br>OCPW did not have a formalized user account creation process for its critical system. New user accounts were informally requested via email or Microsoft Teams. Since Microsoft Teams messages are temporary and not retained, OCPW did not always maintain documentation to support user account requests and management's approval. |
| **CATEGORY** | **Control Finding** |
| **RECOMMENDATION** | OCPW management formalize its user account creation process and ensure request and approval documentation is retained prior to provisioning user accounts in its critical system. |
| **CURRENT STATUS** | **Implemented.** We confirmed that OCPW utilizes a new tool to facilitate new user account creation requests. This tool documents and retains required request details and approvals prior to provisioning new user accounts.<br>Based on the actions taken by OCPW, we consider this recommendation implemented. |

| | |
|---|---|
| **FINDING NO. 2** | **User Account Management**<br>OCPW did not disable certain dormant user accounts timely in their critical system. In addition, OCPW did not perform periodic user access certification reviews to ensure access was restricted to personnel with a direct business need and is disabled when it is no longer needed. |
| **CATEGORY** | **Control Finding** |
| **RECOMMENDATION** | OCPW management:<br>A. Ensure dormant user accounts are disabled timely.<br>B. Perform periodic user access certification reviews to ensure access is restricted to personnel with direct business need and access no longer needed is disabled. |
| **CURRENT STATUS** | **Implemented.** OCPW has improved their process of disabling user accounts timely after separation for intern and temporary access, which were the causes of the dormant accounts noted in our original review. OCPW also now uses a tool to document the completion of its periodic user access reviews (UARs) for its critical system to ensure access is restricted to personnel with a direct business need and that access no longer needed is disabled.<br>OCPW's UAR identified several unnecessary user accounts and removed these accounts from the system. OCPW plans on performing subsequent UARs semiannually. |

| | |
|---|---|
| | Based on the actions taken by OCPW, we consider this recommendation implemented. |

| | |
|---|---|
| **FINDING NO. 3** | **Change Management Process**<br>OCPW did not have a formalized process that clearly documents changes to its critical system. While OCPW indicated they required changes to be approved by someone other than the requestor, properly justified, and tested, they were unable to effectively associate evidence of business justification, testing plan and results, segregation of duties, and approvals for each change that was deployed into production. |
| **CATEGORY** | **Control Finding** |
| **RECOMMENDATION** | OCPW management develop a formalized change management process over its critical system that clearly shows the business justification, testing plan and results, segregation of duties, and approvals prior to deploying changes into production. |
| **CURRENT STATUS** | **Implemented.** We confirmed that OCPW's production change request documentation now includes a clear business justification and testing results. OCPW ensures duties related to changes are adequately segregated by ensuring that different staff request, approve, and deploy all changes.<br>Based on the actions taken by OCPW, we consider this recommendation implemented. |

| | |
|---|---|
| **FINDING NO. 4** | **IT Procedures Not Finalized**<br>OCPW was in the process of finalizing IT procedures, including their Identity and Access Management (IAM) and Change Management Procedures, that are required by the County Cybersecurity Policy and County Vulnerability Management Policy. |
| **CATEGORY** | **Control Finding** |
| **RECOMMENDATION** | OCPW management finalize its applicable IT procedures to comply with County policy. |
| **CURRENT STATUS** | **Implemented.** We reviewed and confirmed that OCPW finalized its IAM and Change Management Procedures that comply with the County Cybersecurity and the County Vulnerability Management Policies.<br>Based on the actions taken by OCPW, 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 | Senior Auditor |
| | Gabriela Cabrera, CIA | Administrative Services Manager |

## APPENDIX A: ADDITIONAL INFORMATION

| | |
|---|---|
| **SCOPE** | Our follow-up audit was limited to reviewing actions taken by OC Public Works as of June 30, 2025, to implement the four recommendations from our original audit, dated March 31, 2025. |
| **BACKGROUND** | The original audit reviewed selected cybersecurity controls administered by OC Public Works. The original audit identified four Control Findings. |

## 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. |