PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

First Follow-Up Information Technology Audit: Public Defender Selected Cybersecurity Controls

As of September 30, 2021

Audit No. 2059-B (Reference 1942-F1)
Report Date: January 27, 2022

Recommendation Status

7	Implemented
1	In Process
0	Not Implemented
1	Closed

OC Board of Supervisors

CHAIRMAN DOUG CHAFFEE	VICE CHAIRMAN DONALD P. WAGNER	SUPERVISOR ANDREW DO	SUPERVISOR KATRINA FOLEY	SUPERVISOR LISA A. BARTLETT
4th DISTRICT	3rd DISTRICT	1st DISTRICT	2nd DISTRICT	5th DISTRICT

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Audit No. 2059-B
(Reference 1942-F1)

January 27, 2022

To: Martin Schwarz
Public Defender

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

Digitally signed by Agripino Alonso
Date: 2022.01.27 13:49:10 -08'00'

Subject: First Follow-Up Information Technology Audit: Public Defender Selected Cybersecurity Controls

---

We have completed a first follow-up audit of selected cybersecurity controls administered by Public Defender as of September 30, 2021, original Audit No. 1942, dated December 9, 2020. Due to the sensitive nature of specific findings (restricted information), only the results for Finding Nos. 2 and 8 immediately follow this letter. Results for the remaining findings are included in Appendix A (which is redacted from public release), and additional information including background and our scope is included in Appendix B.

Recipients of this restricted information must exercise due care in electronic and non-electronic storage, distribution/transportation, and retention/destruction of this report. Furthermore, the restricted information in this report IS NOT subject to disclosure under the California Public Records Act.

Our first follow-up audit concluded that Public Defender implemented seven (7) recommendations, one (1) recommendation is in process, and one (1) recommendation is closed. A second follow-up audit will be performed in approximately six months and a follow-up audit report form is attached to facilitate that audit. Any recommendations not implemented or in process at that time will be brought to the attention of the Audit Oversight Committee at its next scheduled meeting.

We appreciate the assistance extended to us by Public Defender personnel during our follow-up audit. If you have any questions, please contact me at 714.834.5442 or Assistant Director Scott Suzuki at 714.834.5509.

Attachments
Other recipients of this report:
Members, Board of Supervisors
Chair, Audit Oversight Committee
Frank Kim, County Executive Officer
Joel Golub, Chief Information Officer

RESULTS

FINDING NO. 1	Removed due to the sensitive nature of the finding.

FINDING NO. 2	**Department IT Policy & Procedures**
CATEGORY	**Control Finding**
RECOMMENDATION	Public Defender management finalize comprehensive IT policy and procedures that govern all critical IT business processes.
CURRENT STATUS	**Implemented.** Public Defender finalized and implemented IT policy and procedures governing critical IT business processes including privileged user access rights management, provisioning of new user access, deprovisioning user access upon separation, vulnerability management, IT inventory of assets, malware software, and business continuity and disaster recovery. Based on the actions taken by Public Defender, we consider this recommendation implemented.

FINDING NOS. 3 - 7	Removed due to the sensitive nature of the findings.

FINDING NO. 8	**Backup Software Notification Alerts**
CATEGORY	**Control Finding**
RECOMMENDATION	Public Defender management ensure data recovery and backup software is configured to automatically notify appropriate staff of data backup job failure in the event the primary IT staff is unavailable.
CURRENT STATUS	**Implemented.** Public Defender configured its data recovery and backup software to notify primary and backup IT staff in the event of a backup job issue. Based on the actions taken by Public Defender, we consider this recommendation implemented.

FINDING NO. 9	Removed due to the sensitive nature of the finding.

INTERNAL AUDIT DEPARTMENT

AUDIT TEAM	Scott Suzuki, CPA, CIA, CISA, CFE	Assistant Director
	Jimmy Nguyen, CISA, CFE, CEH	IT Audit Manager II
	Scott Kim, CPA, CISA, CFE	IT Audit Manager I
	Alejandra Hernandez	Senior Auditor
	Mari Elias, DPA	Administrative Services Manager

APPENDIX A: RESTRICTED INFORMATION

Content in Appendix A has been removed from this report due to the sensitive nature of the specific findings.

INTERNAL AUDIT DEPARTMENT

APPENDIX B: ADDITIONAL INFORMATION

SCOPE	Our follow-up audit was limited to reviewing actions taken by Public Defender as of September 30, 2021 to implement the nine (9) recommendations from our original Audit No. 1942, dated December 9, 2020.
BACKGROUND	The original audit evaluated high-risk cybersecurity controls over governance, security management, and computer operations at Public Defender. The original audit identified one (1) Critical Control Weakness, four (4) Significant Control Weaknesses, and four (4) Control Findings.

INTERNAL AUDIT DEPARTMENT

APPENDIX C: 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.