PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Information Technology Audit: Public Defender Selected Cybersecurity Controls

For the Year Ended February 29, 2020

Audit No. 1942
Report Date: December 9, 2020

Number of Recommendations

1	Critical Control Weaknesses
4	Significant Control Weaknesses
4	Control Findings

OC Board of Supervisors

CHAIRWOMAN MICHELLE STEEL	VICE CHAIRMAN ANDREW DO	SUPERVISOR DONALD P. WAGNER	SUPERVISOR DOUG CHAFFEE	SUPERVISOR LISA A. BARTLETT
SECOND DISTRICT	FIRST DISTRICT	THIRD DISTRICT	FOURTH DISTRICT	FIFTH DISTRICT

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Information Technology Audit:
Public Defender Selected Cybersecurity Controls

December 9, 2020

AUDIT HIGHLIGHTS

SCOPE OF WORK	Perform an Information Technology Audit of Public Defender selected IT Cybersecurity controls for the year ended February 29, 2020.
RESULTS	• We concluded controls provided reasonable assurance that data recorded, processed and reported remains complete, accurate and valid throughout the data backup (update and storage) process. • We concluded controls were generally effective to provide reasonable assurance that inventory of IT hardware assets is performed to ensure that only authorized systems are connected to the network. • We concluded controls over provisioning and deprovisioning of user access should be improved. • We concluded controls over privileged user access management should be improved. • We concluded controls over malware defense should be improved. • We concluded controls over vulnerabilities management should be improved.
RISKS	As a result of our findings, potential risks include: • Unauthorized logical access to, and exposure of, sensitive data. • Installation, spread, and execution of malicious code that could result in a cybersecurity incident such as data exposure and unauthorized access.
NUMBER OF RECOMMENDATIONS 1 CRITICAL CONTROL WEAKNESSES 4 SIGNIFICANT CONTROL WEAKNESSES 4 CONTROL FINDINGS	Opportunities for enhancing internal control include: • Performing periodic privileged service account and user access certification reviews. • Ensuring all network systems have malware software installed as needed. • Implementing a central log management system.

Report suspected fraud, or misuse of County resources by vendors, contractors, or County employees to 714.834.3608

AUDIT NO. 1942

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Audit No. 1942

December 9, 2020

To: Martin Schwartz
Interim Public Defender

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

Subject: Information Technology Audit: Public Defender Selected Cybersecurity Controls

---

We have completed an Information Technology Audit of selected cybersecurity controls at the Public Defender for the year ended February 29, 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 objectives, scope, and methodology are included in Appendix B.

Public Defender concurred with all our recommendations and the Internal Audit Department considers management's response appropriate to the recommendations in this report.

We will include the results of this audit in a future status report submitted quarterly to the Audit Oversight Committee and the Board of Supervisors. In addition, we will request your department complete a Customer Survey of Audit Services, which you will receive shortly after the distribution of our final report.

We appreciate the courtesy extended to us by Public Defender personnel during our 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
Members, Audit Oversight Committee
Public Defender Distribution
Foreperson, Grand Jury
Robin Stieler, Clerk of the Board of Supervisors
Eide Bailly LLP, County External Auditor

RESULTS

BUSINESS PROCESS & INTERNAL CONTROL STRENGTHS	Business process and internal control strengths noted during our audit include: ✓ Comprehensive IT asset management software is used to track and manage that only authorized systems are connected to the network. ✓ Robust data backup and recovery software is used to ensure continuous data availability for critical systems. ✓ Various security tools are used to monitor, detect, and prevent the spread of malware attacks. ✓ Two-factor authentication is required for all remote end users that access the department network.

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

FINDING NO. 2	**Department IT Policy & Procedures** Departmental IT policy and procedures were in various stages of being developed. Public Defender IT has developed draft revisions to some key policy and procedures (e.g., privileged user access rights management, provisioning of new user access, deprovision user access upon separation, vulnerability management, IT inventory of asset, malware software) and has not developed a policy and procedure for disaster recovery testing. Cybersecurity incidents are becoming more common. Accordingly, customized and documented procedures (e.g., data collection, team responsibilities, legal procedures, communication strategies) are important to have on-hand to properly prepare and increase the opportunity for a department to understand, manage, and recover from a cybersecurity incident.
CATEGORY	**Control Finding**
RISK	Lack of IT policy and procedures can result in a lack of understanding of IT business processes, cybersecurity violations, delayed implementation of systems, or delayed response to a cybersecurity incident.

RECOMMENDATION	Public Defender management finalize comprehensive IT policy and procedures that govern all critical IT business process.
MANAGEMENT RESPONSE	**[Concur].** We are in the process of approving the IT Policy and Procedures for Access Control and Management Policy, Asset Management Policy, Business Continuity and Disaster Recovery Policy and Controls Management Policy. We are estimating to have these IT Policies and Procedures complete no later than the end of calendar year 2020. Once the IT Policy and Procedures are in place, we will train staff on the Policy and Procedures.

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

FINDING NO. 8	**Backup Software Notification Alerts** Backup failure notifications were not enabled. While Public Defender IT staff reviews backup job log results from the data recovery and backup software daily to ensure scheduled critical backup jobs are processed successfully, we noted the software did not have notification alert features enabled to automatically notify IT staff of backup job failures. Subsequent to our review, and as a result of our audit fieldwork, Public Defender immediately enabled the feature in the backup software.
CATEGORY	**Control Finding**
RISK	Untimely backups and the absence of backup job failure notifications increases the risk that critical information could be lost.
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.
MANAGEMENT RESPONSE	**[Concur].** We have worked with our backup vendor and enabled the email notifications for backup jobs. This finding has been mitigated.

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
	Zan Zaman, CPA, CIA, CISA	Audit Manager

APPENDIX A: RESTRICTED INFORMATION

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

APPENDIX B: ADDITIONAL INFORMATION

OBJECTIVES	Our audit objectives were to determine if Public Defender cybersecurity controls: 1. Provide reasonable assurance that regular and privileged access to critical systems is limited to authorized individuals. 2. Provide reasonable assurance that regular and privileged access to critical systems is disabled timely upon termination. 3. Provide reasonable assurance that data recorded, processed, and reported remains complete, accurate and valid throughout the data backup (update and storage) process. 4. Provide reasonable assurance that anti-malware software prevents the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action. 5. Provide reasonable assurance that vulnerabilities are appropriately managed to identify, remediate, and minimize the window of opportunity for attackers. 6. Provide reasonable assurance that inventory of IT hardware assets is performed to ensure that only authorized systems are connected to the network.
SCOPE & METHODOLOGY	Our audit scope was limited to high-risk cybersecurity controls over governance, security management, and computer operations at Public Defender for the year ended February 29, 2020. Our methodology included inquiry, observation, examination of documentation, and sampling of relevant items.
EXCLUSIONS	We did not examine application controls or any processes that involve external parties such as OCIT or systems managed by the State of California, nor any services/activities performed or provided by the County or state's third-party vendors.
PRIOR AUDIT COVERAGE	No audits of this scope have been issued for Public Defender in the last 10 years.

INTERNAL AUDIT DEPARTMENT

BACKGROUND	The Orange County Public Defender provides legal representation to those unable to afford a lawyer in criminal, juvenile, mental health and dependency cases in an efficient and cost-effective manner. These services are provided through three independent units: the Public Defender's Office, the Alternate Defender's Office, and the Associate Defender's Office. The units operate under the administrative supervision of the Public Defender. The three segments employ approximately 210 attorneys and approximately 195 additional support staff (including administrative staff, investigators, investigative assistants, clerical staff, IT personnel, and paralegals). The IT department supports and manages the Public Defender's network infrastructure security, as well as a case management system designed for Public Defender offices that interfaces with other justice partners such as the District Attorney and courts.

INTERNAL AUDIT DEPARTMENT

PURPOSE & AUTHORITY	We performed this audit in accordance with the FY 2019-20 Audit Plan and Risk Assessment approved by the Audit Oversight Committee (AOC) and the Board of Supervisors (Board).
PROFESSIONAL STANDARDS	Our audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing issued by the International Internal Audit Standards Board.
FOLLOW-UP PROCESS	In accordance with professional standards, the Internal Audit Department has a process to follow-up on its recommendations. A first follow-up audit will generally begin six months after release of the initial report. The AOC and Board expect that audit recommendations will typically be implemented within six months or sooner for significant and higher risk issues. A second follow-up audit will generally begin six months after release of the first follow-up audit report, by which time all audit recommendations are expected to be implemented. Any audit recommendations not implemented after the second follow-up audit will be brought to the attention of the AOC at its next scheduled meeting. A Follow-Up Audit Report Form is attached and is required to be returned to the Internal Audit Department approximately six months from the date of this report in order to facilitate the follow-up audit process.
MANAGEMENT'S RESPONSIBILITY FOR INTERNAL CONTROL	In accordance with the Auditor-Controller's County Accounting Manual No. S-2 Internal Control Systems: "All County departments/agencies shall maintain effective internal control systems as an integral part of their management practices. This is because management has primary responsibility for establishing and maintaining the internal control system. All levels of management must be involved in assessing and strengthening internal controls." Internal control should be continuously evaluated by management and weaknesses, when detected, must be promptly corrected. The criteria for evaluating internal control is the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control – Integrated Framework. Our audit complements but does not substitute for department management's continuing emphasis on control activities and monitoring of control risks.
INTERNAL CONTROL LIMITATIONS	Because of inherent limitations in any system of internal control, errors or irregularities may nevertheless occur and not be detected. Specific examples of limitations include, but are not limited to, resource constraints, unintentional errors, management override, circumvention by collusion, and poor judgment. Also, projection of any evaluation of the system to future periods is subject to the risk that procedures may become inadequate because of changes in conditions or the degree of compliance with the procedures may deteriorate. Accordingly, our audit would not necessarily disclose all weaknesses in the department's operating procedures, accounting practices, and compliance with County policy.

APPENDIX C: REPORT ITEM CLASSIFICATION

Critical Control Weakness	Significant Control Weakness	Control Finding
These are audit findings or a combination of audit findings that represent critical exceptions to the audit objective(s) and/or business goals. Such conditions may involve either actual or potential large dollar errors or be of such a nature as to compromise the department's or County's reputation for integrity. Management is expected to address **Critical Control Weaknesses** brought to its attention immediately.	These are audit findings or a combination of audit findings that represent a significant deficiency in the design or operation of internal controls. **Significant Control Weaknesses** require prompt corrective actions.	These are audit findings concerning the effectiveness of internal control, compliance issues, or efficiency issues that require management's corrective action to implement or enhance processes and internal control. **Control Findings** are expected to be addressed within our follow-up process of six months, but no later than twelve months.

APPENDIX D: PUBLIC DEFENDER MANAGEMENT RESPONSE

LAW OFFICES

ORANGE COUNTY PUBLIC DEFENDER

MARTIN F. SCHWARZ
INTERIM PUBLIC DEFENDER

MARK S. BROWN
SENIOR ASSISTANT PUBLIC DEFENDER

TRACY R. LESAGE
SENIOR ASSISTANT PUBLIC DEFENDER

LAURA J. JOSE
SENIOR ASSISTANT PUBLIC DEFENDER

801 Civic Center Drive West, Suite 400
SANTA ANA, CA 92701-4026
(657) 251-6090 FAX: (714) 479-0825
www.pubdef.ocgov.com

October 8, 2020

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

SUBJECT: Response to Information Technology Audit—Public Defender Selected Cybersecurty Contols, Audit No. 1942

I am providing the Public Defender's response to the Information Technology Audit of selected cybersecurity controls at Law Offices of the Public Defender for the year ending February 9, 2020.

I would like to express my appreciation for the professionalism and support provided by your Department in conducting this audit.

Finding 1

[redacted]

Finding 2

We are in the process of approving the IT Policy and Procedures for Access Control and Management Policy, Asset Management Policy, Business Continuity and Disaster Recovery Policy and Controls Management Policy. We are estimating to have these IT Policies and Procedures complete no later than the end of calendar year 2020. Once the IT Policy and Procedures are in place, we will train staff on the Policy and Procedures.

CENTRAL OFFICE	HARBOR OFFICE	JUVENILE OFFICE	MENTAL HEALTH	NORTH OFFICE	WEST OFFICE
801 Civic Center Drive West, Suite 300 Santa Ana, CA 92701 (657) 251-6460	4601 Jamboree Rd. Suite 101 Newport Beach, CA 92660 (657) 251-6553	341 City Drive S. Suite 307 Orange, CA 92868 (657) 251-6718	200 W. Santa Ana Blvd. Suite 970 Santa Ana, CA 92701 (657) 251-6414	1440 N. Harbor Blvd. 4th Floor Fullerton, CA 92835 (657) 251-6472	14120 Beach Blvd. Suite 200 Westminster, CA 92683 (657) 251-6562

Finding 3

[redacted]

Finding 4

[redacted]

Finding 5

[redacted]

Finding 6

[redacted]

Finding 7

[redacted]

Finding 8

We have worked with our backup vendor and enabled the email notifications for backup jobs. This finding has been mitigated.

Finding 9

[redacted]

Respectfully Submitted,

Martin F. Schwarz
Interim Public Defender