COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

OSCAR VALDEZ
AUDITOR-CONTROLLER

CONNIE YEE
CHIEF DEPUTY AUDITOR-CONTROLLER

ASSISTANT AUDITOR-CONTROLLERS

MAJIDA ADNAN
RACHELLE ANEMA
ROBERT G. CAMPBELL

May 21, 2025

TO: Each Supervisor

FROM: Oscar Valdez
Auditor-Controller

Robert G. Campbell
Assistant Auditor-Controller / Chief Audit Executive

SUBJECT: **DEPARTMENT OF CONSUMER AND BUSINESS AFFAIRS – INFORMATION TECHNOLOGY AND SECURITY REVIEW (REPORT #K23BQ) - FIRST FOLLOW-UP REVIEW**

We completed a follow-up review of the Department of Consumer and Business Affairs (DCBA or Department) Information Technology (IT) and Security Review dated December 8, 2023 (Report #K23BQ). As summarized in Table 1, DCBA fully implemented six recommendations and partially implemented four recommendations to enhance their IT and security processes. DCBA should fully implement the four outstanding recommendations to strengthen controls and monitoring over IT and security processes. Strong controls in these areas are mandated in the Board of Supervisors' Policy Manual and County Fiscal Manual.

Table 1 - Results of First Follow-up Review

RECOMMENDATION IMPLEMENTATION STATUS				
			OUTSTANDING RECOMMENDATIONS	
PRIORITY RANKINGS	TOTAL RECOS	FULLY IMPLEMENTED	PARTIALLY IMPLEMENTED	NOT IMPLEMENTED
PRIORITY 1	3	2	1	0
PRIORITY 2	7	4	3	0
PRIORITY 3	0	0	0	0
TOTAL	10	6	4	0
			4	

For details of our review and the Department's corrective actions, see Attachment. We will follow up and report back on the one outstanding Priority 1 and three outstanding Priority 2 recommendations.

We thank DCBA management and staff for their cooperation and assistance during our review. If you have any questions please call us, or your staff may contact Zoran Penich at zpenich@auditor.lacounty.gov.

OV:CY:RGC:ZP:mr

Attachment

c: Fesia A. Davenport, Chief Executive Officer
Edward Yen, Executive Officer, Board of Supervisors
Rafael Carbajal, Director, Department of Consumer and Business Affairs

LOS ANGELES COUNTY
AUDITOR-CONTROLLER

Robert G. Campbell ASSISTANT AUDITOR-CONTROLLER	Zoran Penich DIVISION CHIEF

AUDIT DIVISION *Report #K25CY*

DEPARTMENT OF CONSUMER AND BUSINESS AFFAIRS INFORMATION TECHNOLOGY AND SECURITY REVIEW (REPORT #K23BQ) FIRST FOLLOW-UP REVIEW

	RECOMMENDATION	A-C COMMENTS
1	Security Software (Priority 1) - Department of Consumer and Business Affairs (DCBA or Department) management strengthen their security software protection processes to safeguard devices and the data they access and store by: a) Establishing documentation controls, such as a checklist or documented supervisory verification, to provide evidence and assurance that staff properly install encryption and malware protection software on Information Technology (IT) devices prior to deployment. b) Finalize the Service Level Agreement (SLA) with the Internal Services Department (ISD) for the security software functions delegated to ISD. c) Establishing a process to monitor the delegated security software functions to ensure ISD is performing them effectively. **Original Issue/Impact:** We noted DCBA had various security software protection processes. Specifically, DCBA had a process to install encryption and malware protection software on devices before they were assigned to employees. This included registering new devices in their security software console and visually verifying the software was installed from the console/network onto devices before deployment. However, this process did not have documentation controls to provide evidence and assurance that staff performed this activity. We also noted DCBA delegated some of their security software functions to ISD. For example, DCBA relied on ISD to identify, test, and deploy virus definition and software version updates. During our original review, we noted that DCBA drafted an SLA to document the terms and conditions of these services. However, DCBA had not finalized the SLA to confirm each department's role and responsibilities.	**Recommendation Status: Implemented** a) We confirmed DCBA established documentation controls to provide evidence and assurance that staff properly install encryption and malware protection software on IT devices prior to deployment by reviewing the Department's written procedures. The procedures require staff to install and test the security software on the devices prior to deployment, and document installation results. We also confirmed staff adhered to the procedures by reviewing examples of documented installation results. b) We reviewed and confirmed DCBA finalized the SLA with ISD for security software functions delegated to ISD. According to the SLA, ISD will provide anti-virus and malware security software installation services, device security compliance services, centralized security management, monthly vulnerability scans, security software management, and security compliance reporting. c) We confirmed DCBA established a process to monitor delegated security software functions to ensure ISD is performing them effectively by reviewing the Department's written procedures. The procedures require staff to assess security software functions to ensure devices are centrally managed, software product versions are up to date, encryption is enabled, and data is encrypted; work with ISD, as needed, to remediate any findings; and document review results. We also confirmed staff adhered to the procedures by reviewing examples of their documented review results, including remediated findings.

Priority Ranking: Recommendations are ranked from Priority 1 to 3 based on the potential seriousness and likelihood of negative impact on the Agency's operations if corrective action is not taken.

RECOMMENDATION		A-C COMMENTS
	DCBA reported over 200 IT devices, such as laptops and desktops, that staff used to process requests for assistance in areas such as immigration services, fraud, identity theft, and elder financial abuse. These weaknesses increase the risk that devices will not have up-to-date software protection against unauthorized access and threats, including viruses, malware, and ransomware. This can lead to security incidents, including breaches of sensitive case data, including personally identifiable information (PII).	
2	**IT Device Inventory (Priority 1)** - DCBA management strengthen their inventory processes and controls to ensure all IT devices are accounted for by: a) Promptly conducting a physical inventory to account for all devices and update their master inventory. b) Establishing an annual physical inventory process that includes reconciling physical counts to their master inventory and investigating discrepancies. **Original Issue/Impact:** DCBA maintained a master inventory of devices and had a process to update those records when they received new devices. DCBA also compared master inventory records to devices that connected to the network to account for devices and investigated discrepancies. However, DCBA's master inventory was initially created based on devices that were connected to the network at a point in time and not based on a physical inventory. DCBA also did not have a process to conduct annual physical inventories of devices to ensure they were all properly accounted for in their master inventory. DCBA reported an inventory of over 200 IT devices used to process and/or investigate complaints. These weaknesses increase the risk of loss or theft of devices to go undetected and unreported. This can lead to unauthorized access and disclosure of PII.	**Recommendation Status: Partially Implemented** a) We confirmed DCBA completed their first physical inventory in November 2024 to account for all IT devices by reviewing their compiled IT device list. However, DCBA did not reconcile this list to update the master inventory list. We worked with DCBA management to clarify the issue and recommendation so they can take appropriate corrective action. DCBA indicated they will reconcile the physical inventory results with their master inventory list during their next physical inventory in May 2025. b) We confirmed DCBA established a process to conduct annual physical inventories that include reconciling physical counts to the master inventory and investigating discrepancies by reviewing their written procedures. The procedures require the IT manager to initiate the annual physical inventory, assign IT support staff to conduct a physical inventory, reconcile the records with the master inventory, investigate any discrepancies, and document results. However, DCBA has not performed these procedures. The Department plans to fully implement this recommendation by May 31, 2025.
3	**Separation of Duties (Priority 1)** - DCBA management immediately separate incompatible duties or establish additional compensating controls for managing IT equipment. **Original Issue/Impact:** During our interviews and review of controls over IT devices and their disposal in Issues No. 2, 4, and 5, we noted the same	**Recommendation Status: Implemented** We confirmed DCBA management separated incompatible duties to strengthen controls for managing IT equipment by reviewing the Department's written procedures. Specifically, DCBA appropriately separated duties for receiving new/returned equipment, updating inventory

Priority Ranking: Recommendations are ranked from Priority 1 to 3 based on the potential seriousness and likelihood of negative impact on the Agency's operations if corrective action is not taken.

RECOMMENDATION		A-C COMMENTS
	individuals performed the duties of receiving new/returned equipment, updating inventory records to account for that equipment, safeguarding equipment, approving equipment disposals, and disposing of surplus equipment. These duties were incompatible and should be separated, or DCBA needed to establish additional compensating controls as necessary. This weakness significantly increases the risk that IT devices will be lost or stolen, and that those losses go undetected. This can lead to unauthorized access and disclosure of PII.	records, safeguarding equipment, approving equipment disposals, and disposing of surplus equipment.
4	IT Device Sanitization (Priority 2) - DCBA management improve their sanitization processes by establishing controls, such as reconciliations between lists of salvaged IT devices, hard drives, and sanitization certificates, to ensure all salvaged IT devices are sanitized. **Original Issue/Impact:** We noted DCBA had a process to sanitize devices before disposal or reissuance. Specifically, DCBA staff removed hard drives from salvaged devices and used software to immediately sanitize them. The software provided sanitization certificates for their records. However, DCBA did not have other controls to confirm all hard drives were properly removed and sanitized. For example, while staff maintained sanitization certificates, they did not require staff to maintain lists of salvaged devices and hard drives or require reconciliations between those lists and sanitization certificates. This weakness increased the risk for unauthorized access, use and/or exposure of DCBA data, including PII, stored in devices. This can lead to unauthorized disclosure of PII.	**Recommendation Status: Implemented** We confirmed DCBA established controls to ensure all salvaged IT devices are sanitized by reviewing the Department's updated written procedures. The procedures require staff to maintain a list of salvaged devices and the Department Information Security Officer (DISO) to reconcile sanitization certificates with the list of salvaged devices. We also confirmed staff adhered to the procedures by reviewing sanitization reconciliation examples.
5	Physical Security (Priority 2) - DCBA management strengthen their physical security processes and controls to ensure all IT devices are physically secured by: a) Establishing documentation controls, such as requirements to annotate a list of keycard assignments and/or e-mail their supervisor their review results, to provide documented evidence and assurance that keycard assignments remain appropriate based on staff's job duties.	**Recommendation Status: Implemented** a) We confirmed DCBA management established documentation controls to provide documented evidence and assurance that keycard assignments remain appropriate based on staff's job duties by reviewing the Department's written procedures. The procedures require staff to review quarterly keycard system user access reports to ensure employees are assigned the appropriate level of access based on job duties, immediately restrict access to employees with

Priority Ranking: Recommendations are ranked from Priority 1 to 3 based on the potential seriousness and likelihood of negative impact on the Agency's operations if corrective action is not taken.

	RECOMMENDATION	A-C COMMENTS
	b) Establishing a process for conducting periodic reviews (e.g., documented walkthroughs) to ensure staff comply with requirements for safeguarding IT devices and wearing identification. **Original Issue/Impact:** DCBA had various processes to help physically secure IT devices. This included requirements to safeguard devices (e.g., new and salvaged laptops and desktops) in a secured room and to restrict access to that room with keycards. In addition, DCBA required that management request/authorize their staff's access to the storage room and that staff wear identification badges in that room to help support that they were authorized. DCBA also required that management review the appropriateness of keycard assignments on a quarterly basis. However, we noted control weaknesses and other areas for improvement. Specifically: • DCBA did not have documentation controls that provided evidence and assurance that management reviewed the appropriateness of keycard assignments. Management told us they performed a visual review of keycard assignments, but there was no documented evidence for that activity. • DCBA did not have a process for conducting periodic reviews (e.g., documented walkthroughs) to ensure staff comply with requirements for safeguarding devices and wearing badges in the IT storage room. At the time of our review, DCBA reported over 50 IT devices in storage. These weaknesses increase the risk of unauthorized access to DCBA's storage room going undetected and of unsecured devices. This can lead to device tampering, damage, or theft.	unauthorized elevated access, send a user access change notification to the employee's manager, and document the review results. We also confirmed staff adhered to the procedures by reviewing examples of documented keycard system user access reports. b) We confirmed DCBA established a process to ensure staff comply with requirements for safeguarding IT devices and wearing identification by reviewing the Department's written procedures. The procedures require staff to perform quarterly information asset and identification reviews, which include conducting office walkthroughs to ensure information assets are not left unattended in unsecured areas and staff are wearing appropriate identification in the secured IT storage rooms, and remediate identified non-compliances. We also confirmed staff adhered to the procedures by reviewing an annotated information asset and identification review report.
6	**System Access (Priority 2)** - DCBA management strengthen their user access processes and controls to prevent unauthorized access and exposure of County data by: a) Reminding staff to use and retain request forms to ensure they are adding, removing, and updating user access based on their job duties. b) Reminding staff to perform periodic user access reviews and maintain documentation to ensure user access assignments remain appropriate based on users' job duties.	**Recommendation Status: Implemented** a) We reviewed the Department's written procedures and confirmed DCBA management developed an alternative process to retain request forms to ensure they are adding, removing, and updating user access based on their job duties. The procedures require managers to complete request forms to add, remove, and update system access based on the users' job duties, and the DISO or Assistant Department Information Security Officer (ADISO)

Priority Ranking: Recommendations are ranked from Priority 1 to 3 based on the potential seriousness and likelihood of negative impact on the Agency's operations if corrective action is not taken.

	RECOMMENDATION	A-C COMMENTS
	Original Issue/Impact: DCBA had processes to restrict user access to their critical systems, eConsumer and 3Di, which were used to manage complaint cases. However, we noted process and control weaknesses that increased the risk of inappropriate access assignments and non-compliance with access requirements. Specifically: • DCBA required that staff use a request form to add, remove, and update users' access based on job duties and with management authorization. However, DCBA did not retain the required documentation to support staff performed this critical activity. As a result, there was no assurance that staff were following this process and appropriately adding, removing, and updating users' access based on job duties. • DCBA required staff to conduct quarterly user access reviews to ensure access assignments remained appropriate. This included identifying inactive users and working with managers to ensure access was appropriate. However, DCBA did not retain documentation, such as an inactive user list and correspondence with managers, to support they performed this critical activity. As a result, there was no assurance that staff were following this process and access assignments remained appropriate. DCBA reported over 200 system users, including staff and volunteers for their critical systems, eConsumer and 3Di. These weaknesses increase the risk users may have inappropriate or unneeded eConsumer and 3Di access. This can lead to unauthorized access or disclosure of DCBA data, including PII, without being detected.	to review, approve, and retain the request forms. We also confirmed the staff adhered to the procedures by reviewing examples of approved request forms. b) We reviewed the Department's written procedures and confirmed DCBA management developed an alternative process to retain user access review reports to ensure user access assignments remain appropriate based on users' job duties. The procedures require the DISO or ADISO to perform quarterly critical system user access reviews to ensure staff are assigned an appropriate level of access based on their job duties, and maintain the review results. We also confirmed staff adhered to the procedures by reviewing examples of user access review results, including resolved findings.
7	**IT Risk Assessment (Priority 2)** - DCBA management: a) Establish a process to periodically conduct IT risk assessments to ensure IT security threats and vulnerabilities are identified, prioritized, and remediated. b) Promptly conduct an IT risk assessment in accordance with the process established in the recommendation above. **Original Issue/Impact:** We noted DCBA did not have a process to periodically conduct IT risk assessments to identify IT security threats and	**Recommendation Status: Implemented** a) We confirmed DCBA management established a process to periodically conduct IT risk assessments to ensure IT security threats and vulnerabilities are identified, prioritized, and remediated by reviewing the Department's written procedures. The procedures require staff to conduct annual risk assessments, including the DISO completing the departmental risk register, documenting and implementing action plans to remediate/mitigate identified vulnerabilities, and communicating the results to executive management.

Priority Ranking: Recommendations are ranked from Priority 1 to 3 based on the potential seriousness and likelihood of negative impact on the Agency's operations if corrective action is not taken.

RECOMMENDATION		A-C COMMENTS
	vulnerabilities and had never conducted an IT risk assessment. This weakness increases the risk that staff may not properly or consistently assess risk and remediate threats and vulnerabilities impacting over 200 IT devices and critical IT areas. This can lead to issues, such as device malfunctions, operational downtime, and/or the exposure of DCBA data.	b) We confirmed DCBA conducted an IT risk assessment in accordance with their written procedures by reviewing their completed risk register, including a risk assessment questionnaire that covers each facility.
8	**Information Security Awareness Training (Priority 2)** - DCBA management strengthen their security awareness training processes by establishing documentation controls, such as requirements for staff to annotate training compliance reports and/or e-mail their supervisors review results, to provide evidence and assurance that staff monitor and ensure training is completed timely. **Original Issue/Impact:** DCBA required information security awareness training to be provided to new hires within ten days of the hiring date and to all other staff annually. DCBA also had processes to monitor that staff completed the training timely. This included conducting weekly visual reviews of training compliance reports in their training system to identify staff who had not completed training and following up on their progress with e-mails. However, that process did not have sufficient documentation controls to provide evidence and assurance that staff performed this activity. This weakness increases the risk of the misuse of IT resources, unprotected devices, and data exposure. This can lead to costly data breaches.	**Recommendation Status: Partially Implemented** We confirmed DCBA established documentation controls to provide evidence and assurance that staff monitor and ensure training is completed timely by reviewing their written procedures. The procedures require the Human Resources training coordinator to document their review of the bi-monthly information security awareness training compliance reports, send e-mail notifications to non-compliant staff and their managers, and annotate/update the master training compliance reports for employee compliance changes. However, DCBA has not performed these reviews. The Department plans to fully implement this recommendation by June 30, 2025.
9	**Management Monitoring (Priority 2)** - DCBA management develop ongoing self-monitoring processes that include: a) Examining processes/control activities, such as a review of an adequate number of transactions on a regular basis to ensure adherence to County rules. b) Documenting the monitoring activity and retaining evidence so it can be validated. c) Elevating material exceptions timely so management is aware of control risks and can take appropriate corrective actions.	**Recommendation Status: Partially Implemented** We confirmed DCBA management developed ongoing self-monitoring processes to regularly evaluate and document that IT device inventory and information security awareness training processes and controls are working as intended by reviewing their written procedures. However, DCBA has not performed these activities. We also confirmed DCBA management developed ongoing self-monitoring processes to regularly evaluate and document that security software, IT device sanitization, physical security, system access, and IT risk assessment processes and

Priority Ranking: Recommendations are ranked from Priority 1 to 3 based on the potential seriousness and likelihood of negative impact on the Agency's operations if corrective action is not taken.

	RECOMMENDATION	A-C COMMENTS
	Original Issue/Impact: DCBA needed to develop ongoing self-monitoring processes to regularly evaluate and document that the following IT and security processes and controls were working as intended: • Security software, as noted in Issue No. 1. • IT device inventory, as noted in Issue No. 2. • IT device sanitization, as noted in Issue No. 4. • Physical security, as noted in Issue No. 5. • System access, as noted in Issue No. 6. • IT risk assessments, as noted in Issue No. 7. • Information security awareness training, as noted in Issue No. 8. This weakness prevents management from having reasonable assurance that important departmental and County IT and security objectives are being achieved. Increased risk for not promptly identifying and correcting process/control weaknesses or instances of non-compliance with County IT and security rules, such as unprotected devices, employee improprieties, and unsecured IT devices.	controls are working as intended by reviewing their written procedures. The procedures require the DISO to perform periodic monitoring reviews of IT and security processes and controls to ensure they are working as intended. However, the DISO is also responsible for performing the operational processes they are monitoring (i.e., no independent monitoring reviews). Self-monitoring needs to be performed by managers who are not directly involved in the processes being monitored to provide reasonable assurance that staff are adhering to procedures. We worked with DCBA management to clarify the issue and recommendation so they can take appropriate corrective action. The Department plans to fully implement this recommendation by September 30, 2025.
10	**Written Procedures (Priority 2)** - DCBA management establish written standards and procedures to adequately guide supervisors and staff in the performance of their duties for all IT and security processes. **Original Issue/Impact:** DCBA needed to develop written standards and procedures to adequately guide supervisors and staff in the performance of their duties for the following processes: • Security software, including documenting security software installation, monitoring compliance, and monitoring delegated IT and security functions. • IT equipment inventories, including performing reconciliations and investigating discrepancies. • IT device sanitization, including performing periodic reconciliations. • Physical security, including conducting documented periodic reviews (e.g., walkthroughs) and quarterly reviews of keycard assignment appropriateness. • System access, including maintaining access authorizations, performing documented user access appropriateness reviews, and performing periodic reviews of terminated/transferred user reports.	**Recommendation Status: Partially Implemented** We reviewed and confirmed DCBA management established written standards and procedures to adequately guide supervisors and staff in the performance of their duties over all areas noted in our initial review except for management monitoring of internal controls, as noted in Recommendation No. 9. The Department plans to fully implement this recommendation by June 30, 2025.

Priority Ranking: Recommendations are ranked from Priority 1 to 3 based on the potential seriousness and likelihood of negative impact on the Agency's operations if corrective action is not taken.

	RECOMMENDATION	A-C COMMENTS
	• IT risk assessments, as noted in Issue No. 7. • Information security awareness training, as noted in Issue No. 8. • Management monitoring of internal controls, as noted in Issue No. 9. Developing written standards and procedures will reduce the risk DCBA staff will perform tasks, such as installing security software, incorrectly or inconsistently. It also helps ensure DCBA data is appropriately protected and improves management's ability to evaluate the IT security controls environment. This reduces the risk of non-compliance with County and departmental IT security rules.	

We conducted our review in conformance with the International Standards for the Professional Practice of Internal Auditing. For more information on our auditing process, including recommendation priority rankings, the follow-up process, and management's responsibility for internal controls, visit auditor.lacounty.gov/audit-process-information.

Priority Ranking: Recommendations are ranked from Priority 1 to 3 based on the potential seriousness and likelihood of negative impact on the Agency's operations if corrective action is not taken.