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

JOHN NAIMO
AUDITOR-CONTROLLER

December 22, 2014

TO: Supervisor Michael D. Antonovich, Mayor
Supervisor Hilda L. Solis
Supervisor Mark Ridley-Thomas
Supervisor Sheila Kuehl
Supervisor Don Knabe

FROM: John Naimo
Auditor-Controller

SUBJECT: **DEPARTMENT OF PUBLIC SOCIAL SERVICES – INFORMATION TECHNOLOGY AND SECURITY POLICIES REVIEW**

The Board of Supervisors' (Board) Information Technology (IT) and Security Policies (Policies) require all County departments to comply with established Countywide IT security standards to help ensure proper controls over County IT resources. As required by Board Policy 6.108, we are reviewing County departments' compliance with the Policies.

We have completed a review of the Department of Public Social Services' (DPSS or Department) compliance with the Policies and related County standards. Our review included testing system access, physical security over IT equipment, computer antivirus and encryption software, equipment disposition, and IT security awareness training.

Results of Review

Our review disclosed that DPSS needs to improve its controls over IT equipment, computer encryption, and systems access. The following are examples of areas for improvement:

- **Inaccurate IT Inventories** – DPSS needs to improve controls over IT equipment inventories. We noted that 14 (40%) of the 35 items reviewed from DPSS' inventory records were disposed of or missing as far back as 2010 but DPSS did not remove them from their records and document the disposals. Also, ten

(20%) of the 65 items observed at DPSS field offices were not accounted for on DPSS' inventory records provided to us, and over 1,000 items in the inventory records had missing/incorrect information (e.g., missing make/model, custodian, etc.) or were assigned to a custodian who no longer worked at the Department.

DPSS' attached response indicates that they will update their policies for IT equipment control and have trained staff on equipment disposal and physical inventory procedures. DPSS also informed us that they will correct the inaccuracies noted in their equipment inventories.

DPSS' response also indicates that they located one of the missing IT equipment items, and that the ten items we could not find in their inventory records were erroneously left off of an inventory report that DPSS staff generated from their inventory system and provided to the Auditor-Controller. DPSS needs to ensure their inventory system reports are accurate.

- **Computer Incident Response** – DPSS needs to report missing IT equipment through the County's computer incident response procedure. We noted that four IT equipment items, including one server that could have contained County data, went missing in 2010 but DPSS staff did not report the items missing, as required by Board Policy 6.109. Specifically, DPSS staff did not notify their Department Information Security Officer (DISO). As a result, the DISO could not file a police report and notify the Chief Information Office and the Auditor-Controller's Office of County Investigations to minimize the risk to the County of lost data/equipment.

  DPSS' response indicates that they have reported three of the four missing equipment items through the County's incident response procedure. Subsequent to our review, DPSS informed us that they located the other missing item and will not report it through the incident response procedure.

- **Inventory Systems** – DPSS needs to evaluate discontinuing duplicate capital equipment tracking. We noted that DPSS accounts for capital IT equipment in their own asset management system and also in the electronic Countywide Accounting and Purchasing System (eCAPS). DPSS staff indicated that their asset management system does not provide any significant benefit or control beyond the tracking that eCAPS provides. Using both systems can result in discrepancies between capital equipment records, and is resulting in staff performing duplicate data entry to update both systems when equipment is purchased, transferred, or disposed.

  DPSS' response indicates that they will evaluate discontinuing duplicate capital equipment tracking.

- **Portable Computer Encryption** – DPSS needs to improve encryption recordkeeping and ensure portable computers are encrypted. DPSS could not locate encryption documentation for 613 (46%) of the 1,323 laptop computers in their inventory. We analyzed 44 portable computers and noted that five (11%) did not have encryption software installed, as required by Board Policy 6.110. We also noted that staff/managers do not periodically monitor to ensure portable computers are encrypted.

  DPSS' response indicates that they implemented a new encryption software solution with improved reporting capability that the Department uses to monitor for unencrypted devices. DPSS also informed us that they encrypted the five devices noted in our review.

- **Hard Drive Disposal** – DPSS needs to properly document that all County data is erased from hard drives when computers are disposed of, as required by Board Policy 6.112. We reviewed ten computers that DPSS disposed of, and noted that although DPSS kept lists of the hard drives that they sent to a vendor for destruction, we could not determine which of those hard drives, if any, came from the ten computers reviewed. DPSS also does not require the vendor to provide a certificate of destruction that identifies each hard drive was successfully destroyed, as required by the County's Hard Drive Cleaning Standard. This reduces the vendor's accountability for destroying all hard drive data.

  DPSS' response indicates that they developed a hard drive destruction policy that requires staff to document each hard drive sent for destruction and the device it was removed from. The policy also requires staff to obtain a vendor certification indicating that every hard drive was destroyed.

- **Systems Access** – DPSS needs to restrict unneeded access to sensitive/confidential information in their systems and resolve errors in user activity reports. We reviewed three of DPSS' systems containing sensitive information, and noted that DPSS did not remove systems access for 442 users who terminated or transferred job duties. Errors in user activity reports from DPSS' primary eligibility determination system prevented us from determining if the terminated user accounts were inappropriately accessed after the employees left DPSS. Also, seven (47%) of the 15 Greater Avenues for Independence Employment Activity and Reporting System (GEARS) user accounts reviewed had more access to sensitive client information or payment approval authority than they needed for their job duties.

  DPSS' response indicates that they reminded staff/managers of procedures for restricting systems access when employees terminate or transfer, and for reviewing systems access on a quarterly basis. DPSS also informed us that they

will remove unneeded systems access and ensure that user activity reports are accurate for their eligibility determination system.

- **Antivirus Software** – DPSS needs to ensure all computers have current antivirus protection, as required by Board Policy 6.102. Nine (25%) of the 36 computers reviewed had antivirus software protection that was outdated from nine days up to 14 months.

  DPSS' response indicates that antivirus software was outdated because employees did not always connect to the DPSS network to receive updates. DPSS corrected the outdated antivirus protection and reminded staff to connect to the network more frequently.

- **Physical Security** – DPSS should evaluate implementing surveillance cameras at facilities containing IT resources with sensitive/confidential information. We reviewed seven DPSS field offices that contain critical IT resources and noted that DPSS generally complies with the physical security requirements in Board Policy 6.106. However, we also noted that one of DPSS' most critical data centers containing confidential data does not have surveillance cameras in place to deter/detect intruders.

  DPSS' response indicates that they implemented surveillance cameras at the location noted in our review.

Details of these and other findings and recommendations are included as Attachment I.

Review of Report

We discussed our report with DPSS management. The Department's attached response (Attachment II) indicates general agreement with our findings and recommendations.

We thank DPSS' management and staff for their cooperation and assistance during our review. If you have any questions, please contact me, or your staff may contact Robert Smythe at (213) 253-0101.

JN:AB:RS:MP

Attachments

c: Sachi A. Hamai, Interim Chief Executive Officer
Sheryl L. Spiller, Director, Department of Public Social Services
Robert Pittman, Chief Information Security Officer, Chief Information Office
Public Information Office
Audit Committee

DEPARTMENT OF PUBLIC SOCIAL SERVICES
INFORMATION TECHNOLOGY AND SECURITY POLICIES REVIEW

Background

The Board of Supervisors' (Board) Information Technology (IT) and Security Policies (Policies) require all County departments to comply with Countywide IT Policies, standards, and guidelines. The Policies help protect County IT assets and ensure the confidentiality and integrity of systems data. As required by Board Policy 6.108, we are reviewing County departments' compliance with the Policies.

We have completed a review of the Department of Public Social Services' (DPSS or Department) compliance with the Policies and related County standards and requirements. DPSS has almost 60,000 IT devices such as desktop computers, laptops, servers, multifunction printers, tablets, etc. Our review included testing system access, physical security over IT equipment, computer antivirus and encryption software, equipment disposition, and IT security awareness training (Training).

IT Equipment Control

Board Policies 6.106 and 6.109 require departments to assign IT equipment to specific individuals (custodians) and for custodians to promptly inform management of missing or stolen equipment. Departments must immediately report missing/stolen IT equipment through the County's computer incident response procedure to minimize risk to the County.

County Fiscal Manual (CFM) Chapter 6 also requires departments to inventory their IT equipment annually and to keep up-to-date IT equipment lists. These controls help ensure County computers and data are accounted for and safeguarded.

Equipment Oversight

We reviewed 100 DPSS IT equipment items, including 35 from DPSS' equipment lists and 65 we observed at eight DPSS field offices, and noted missing IT equipment and significant weaknesses in equipment oversight. These weaknesses could allow County computers and data to go missing or stolen without being detected. Specifically:

- **Missing and Disposed Equipment** – We could not locate 14 (40%) of the 35 items from DPSS' equipment lists. Specifically:
    - DPSS staff indicated that four of these items went missing in 2010, including a server used by DPSS' IT section that could have contained County data. However, we noted staff never removed the items from their inventory, and they did not report the missing items until 2014. Also, DPSS did not follow Department and County computer incident response procedures.

Specifically, staff/managers did not report the losses to their Department Information Security Officer (DISO). As a result, the DISO could not:

- File a police report.
- Make required notifications to the Chief Information Office and the Auditor-Controller's Office of County Investigations, that the items and any associated confidential data or software were missing.

- DPSS staff told us the other ten items were disposed of between 2009 and 2013, but the Department could not document approval for the disposals and they never removed the items from their inventory.

- **Unrecorded Equipment** – Ten (15%) of the 65 equipment items observed at DPSS field offices were not recorded on DPSS' equipment lists. The ten items include some with significant value such as a multifunction printer that could have been purchased for up to $10,000.

- **Inaccurate Tracking** – Twenty-seven (27%) of the 100 items had an inaccurate custodian, location, or equipment description recorded on DPSS' equipment lists. We also analyzed all 59,972 items on DPSS' IT equipment lists and noted that 1,037 (2%) are missing the required make/model, manufacturer's serial number, asset custodian, etc., or are indicated as assigned to an individual who no longer works for DPSS.

We noted that DPSS does not properly conduct physical inventories of their IT equipment because they do not always update their asset listings based on the results of their physical counts. DPSS also does not have up-to-date policies and procedures for maintaining equipment inventories, and staff who manage equipment inventories indicated that they did not receive adequate training in their job duties/responsibilities, as required by CFM 8.3.1.

Recommendations

Department of Public Social Services management:

1. **Update equipment inventories for the inaccuracies noted in our review, ensure staff conduct accurate physical equipment inventories, and investigate and update inventory lists for any discrepancies.**

2. **Report the four missing equipment items through the County's computer incident response process, and remind all staff to report missing equipment to their Department Information Security Officer.**

3. **Ensure staff document approvals for all equipment disposals.**

4. **Update policies and procedures for maintaining equipment inventories, and train staff on their duties and responsibilities for managing equipment inventories.**

Inventory Systems

CFM Chapter 6 requires departments to use the electronic Countywide Accounting and Purchasing System (eCAPS) to account for capital IT equipment with a useful life over one year and acquisition cost over $5,000.

We noted that DPSS accounts for capital IT equipment in their own asset management system and in eCAPS. As a result, staff perform duplicate data entry to update both systems when capital equipment is purchased, disposed, or transferred to a new custodian. DPSS' materials management staff indicated that tracking capital assets in DPSS' asset management system does not provide any significant benefit or control beyond the tracking that eCAPS provides. In addition, the duplicate data entry is time-consuming and can result in discrepancies between the systems.

To save staff time and improve the accuracy of capital equipment inventories, DPSS management should evaluate discontinuing duplicate capital equipment tracking in their asset management system.

Recommendation

5. **Department of Public Social Services management evaluate discontinuing duplicate capital equipment tracking in their asset management system.**

Portable Computer Encryption

Board Policy 6.110 requires departments to encrypt all County owned portable computers. Encryption helps render data unreadable if a computer is lost or stolen, and protects against unauthorized disclosure of personal/confidential information such as the recent breach at a Department of Health Services' contractor.

DPSS could not locate encryption documentation for 613 (46%) of the 1,323 laptop computers in their inventory because their encryption records did not always have enough information, such as an asset tag or serial number, to identify the encrypted device. We analyzed 44 portable computers assigned to DPSS staff and noted that five (11%) did not have encryption software installed. This occurred in part because one field office bypassed DPSS' central receiving unit that is responsible for receiving and encrypting all portable computers. In addition, DPSS management does not periodically monitor the Department's portable computers to ensure that each device has been encrypted.

To protect County data and software on portable computers, DPSS needs to implement the following recommendations.

Recommendations

Department of Public Social Services management:

6. **Enhance encryption documentation so staff can locate the encryption records for all portable computers.**

7. **Encrypt all portable computers, and ensure all portable computers are requested and processed through the Department's central receiving unit.**

8. **Periodically monitor to ensure all portable computers are encrypted.**

Hard Drive Disposal

Board Policy 6.112 requires departments to erase all data and software from computer hard drives before disposing the hard drives from County inventory. The County's Hard Drive Cleaning Standard requires departments who contract for hard drive erasing services to obtain a certification from the vendor. The vendor certification should include the serial number of every hard drive erased or destroyed, the date/method of destruction, and name/signature of the person who performed the destruction.

We reviewed ten computing devices that DPSS disposed of and noted that they could not adequately document that any of the hard drives were successfully removed and destroyed. While DPSS provided some lists of hard drives that they sent to their vendor for destruction, they could not document which of the hard drives, if any, came from the ten computing devices reviewed. DPSS also did not require the vendor to provide a certificate of destruction that includes:

- Hard drive serial number of every device destroyed;
- Date and method of hard drive destruction; and
- Printed name and signature of the person who performed the destruction.

DPSS indicated that they dispose of approximately 300-400 computing devices a year that contain confidential information. To reduce the risk of inappropriately disclosing confidential information, DPSS needs to implement the following recommendations.

Recommendations

Department of Public Social Services management:

9. **Document the serial number of every hard drive removed from a computing device for destruction, and the device that each hard drive was removed from.**

10. **Require vendors who dispose of computer hard drives to provide certificates of destruction that include the serial number of every hard drive destroyed, date/method of destruction, and printed name/signature of the person who performed the destruction.**

Systems Access

Board Policy 3.040 requires departments to safeguard personal and confidential information on their IT systems. CFM 8.7.4.2 requires departments to limit unneeded systems access by immediately updating user access when employees terminate or change job duties.

Inappropriate Access

We reviewed user access for three of the 59 mission critical DPSS systems; the Los Angeles Eligibility Automated Determination, Evaluation, and Reporting (LEADER) system, the Greater Avenues for Independence Employment Activity and Reporting System (GEARS), and the In-Home Supportive Services Case Assignment Management System (CAMS), and noted the following unneeded access:

- One CAMS, two GEARS, and 439 LEADER system users terminated or transferred from DPSS but continued to have access for 15 days to three years after termination. We reviewed system activity reports for seven of these LEADER user accounts, and noted that one account (14%) was used after the employee's transfer date to view personal and confidential information for clients in the CalWORKs program.

  Subsequent to our review, DPSS indicated that they investigated the transferred user's activity and determined that the account was not used after the employee left DPSS. The Department indicated that there was an error in the user activity report generated during the audit, and that the error made it appear that the user had accessed the system. DPSS needs to resolve errors in LEADER user activity reports to ensure the Department can identify any inappropriate system activity.

- Seven (47%) of the 15 GEARS user accounts reviewed have more access than they need for their job duties. Specifically, six employees with accounting and staff support duties can view confidential client information they do not need for

their job duties. Another user changed job duties in 2008, but DPSS never restricted access that he no longer needed for his job duties, such as access to approve metro card payments.

Most of the inappropriate access noted above occurred because DPSS staff did not follow the Department's procedures for immediately updating or removing systems access when employees terminate or transfer job duties.

Recommendations

Department of Public Social Services management:

11. **Immediately cancel terminated and transferred employees' systems access, limit unneeded GEARS access, and remind staff to update or remove systems access when employees terminate or transfer.**

12. **Periodically monitor all users' access for appropriateness.**

13. **Resolve errors in LEADER user activity reports to ensure the Department can identify any inappropriate system activity.**

Access Controls

Board Policy 6.101 requires that systems have appropriate user authentication such as log-on identifications and complex passwords that reset every 90 days.

We noted 38 LEADER users with high-level system administrator access are never forced to reset their passwords, increasing the risk that a compromised password could be used to access sensitive system information. We also noted that GEARS passwords are not case-sensitive, making them easier to guess.

Recommendations

Department of Public Social Services management:

14. **Ensure all LEADER users are forced to reset their password every 90 days.**

15. **Evaluate modifying GEARS to require case-sensitive passwords.**

Antivirus Software

Board Policy 6.102 requires departments to ensure they have functioning up-to-date antivirus software protection for all County computers. Departments must update antivirus software regularly to protect against the most current threats.

Nine (25%) of the 36 computers reviewed had antivirus software protection that was outdated from nine days up to 14 months. The computers with outdated antivirus software are assigned to units processing critical and sensitive information such as LEADER technology management and Medi-Cal services sections.

Recommendation

16. Department of Public Social Services management ensure all computers have current antivirus protection.

Physical Security

Board Policy 6.106 requires departments to physically safeguard IT resources from tampering, damage, theft, or unauthorized physical access. These controls help prevent data breaches such as the recent breach at a Department of Health Services' contractor.

We conducted interviews and walk-throughs at seven DPSS field offices that house critical IT resources such as data centers, computers, multifunction printers, etc., and noted that DPSS generally complies with Board Policy 6.106. However, we also noted that one of DPSS' most critical data centers containing confidential data could potentially benefit from surveillance cameras to deter/detect intruders. Another facility containing confidential data has functioning surveillance cameras, but the footage is recorded-over after 48 hours of recording, increasing the risk that a security incident on a Friday could be recorded-over if it was not discovered until the following Monday.

Board Policy 6.106 does not specifically require surveillance cameras. However, to deter intruders and increase the likelihood of DPSS recovering any stolen IT equipment or data, DPSS should evaluate implementing the following recommendations.

Recommendations

Department of Public Social Services management evaluate:

17. Implementing surveillance cameras at facilities containing critical information technology resources or confidential client data.

18. Increasing the retention period for recorded surveillance footage to increase the likelihood that security incidents can be captured.

Information Security Training

Board Policy 6.111 requires departments to provide Training to all IT resource users at the time they are hired and periodically thereafter. Training should be documented to assist management in determining employee awareness and participation.

We noted that DPSS does a good job providing Training at new employee orientation, but can improve their process for Training thereafter. DPSS management provides ongoing Training to staff through bulletins and newsletters on security topics. However, DPSS does not have a plan that outlines the frequency and type of content that they need to deliver to staff. As a result, we could not determine whether DPSS delivered all the intended Training content through the bulletins and newsletters. In addition, DPSS could not document that IT users received and were aware of the Training materials.

After the start of our audit, DPSS conducted a comprehensive classroom Training. We reviewed Training documentation at six field offices and could not determine if the Department trained all necessary staff due to a lack of information. For example, DPSS did not have a list of all required attendees so that we could verify that each was on a sign-in sheet. In addition, many of the sign-in sheets did not include enough information to identify the attendee, such as an employee identification number and work location.

Board Policy 6.111 does not specify IT training content or how it should be documented. However, DPSS can improve their Training delivery by developing a plan that outlines the Training content that staff need to receive, and the documentation needed to evaluate staff participation and awareness.

Recommendation

19. Department of Public Social Services management develop a plan that outlines the information technology security awareness training content staff need to receive, and the documentation needed to evaluate staff participation and awareness.

County of Los Angeles
DEPARTMENT OF PUBLIC SOCIAL SERVICES
12860 CROSSROADS PARKWAY SOUTH · CITY OF INDUSTRY, CALIFORNIA 91746
Tel (562) 908-8400 · Fax (562) 695-4801

SHERYL L. SPILLER
Director

PHIL ANSELL
Chief Deputy

Board of Supervisors
GLORIA MOLINA
First District
MARK RIDLEY-THOMAS
Second District
ZEV YAROSLAVSKY
Third District
DON KNABE
Fourth District
MICHAEL D. ANTONOVICH
Fifth District

October 30, 2014

TO: John Naimo
Auditor-Controller

FROM: Sheryl L. Spiller, Director

SUBJECT: **DEPARTMENT OF PUBLIC SOCIAL SERVICES RESPONSE TO THE AUDITOR-CONTROLLER'S INFORMATION TECHNOLOGY AND SECURITY POLICIES REVIEW DRAFT REPORT**

Attached is the Los Angeles County Department of Public Social Services' (DPSS) response to the Auditor-Controller's draft report on the DPSS Information Technology and Security Policies Review. The draft report was received on September 12, 2014, and listed a total of 19 recommendations.

As described in the enclosure, DPSS has completed 11 recommendations. Recommendation 15 and 16 are targeted for implementation by November 28, 2014; Recommendation 1, 3, 4, 5 and 6 are targeted for implementation by December 31, 2014; and Recommendation 13 is targeted for implementation by February 28, 2015.

Please let me know if you have any questions, or your staff may contact Francisco Sanchez, Chief, Research, Evaluation and Quality Assurance Division, at (562) 908-5879.

SLS:lb

Attachment

Attachment

AUDITOR-CONTROLLER'S INFORMATION TECHNOLOGY AND SECURITY POLICIES REVIEW

DEPARTMENT OF PUBLIC SOCIAL SERVICES RESPONSE TO RESULTS AND RECOMMENDATIONS

IT EQUIPMENT CONTROL

Board Policies 6.106 and 6.109 require departments to assign IT equipment to specific individuals (custodians) and for custodians to promptly inform management of missing or stolen equipment. Departments must immediately report missing/stolen IT equipment through the County's computer incident response procedure to minimize risk to the County.

County Fiscal Manual (CFM) Chapter 6 also requires departments to inventory their IT equipment annually and to keep up-to-date IT equipment lists. These controls help ensure County computers and data are accounted for and safeguarded.

(DPSS recommends that the review period, August 15, 2013 through June 20, 2014, be included in the report.)

Equipment Oversight

We reviewed 100 DPSS IT equipment items, including 35 from DPSS' equipment lists and 65 we observed at eight DPSS field offices, and noted missing IT equipment, and significant weaknesses in equipment oversight. These weaknesses could allow County computers and data to go missing or stolen without being detected. Specifically:

- **Missing and Disposed Equipment** - We could not locate 14 (40%) of 35 items from DPSS' equipment lists. Specifically:
    - DPSS staff indicated that four of these items went missing in 2010, including a server used by DPSS' IT section that could have contained County data. However, we noted staff never removed the items from their inventory, and they did not report the missing items until 2014. Also, DPSS did not follow Department and County computer incident response procedures. Specifically, staff/managers did not report the losses to the Department's Information Security Officer (DISO). As a result, the DISO could not:
        - File a police report.
        - Make required notifications to the Chief Information Office, Auditor-Controller Office of County Investigations, etc., that the items and any associated confidential data or software were missing.

- DPSS staff told us the other ten items were disposed of between 2009 and 2013, but the Department could not document approval for the disposals and they never removed the items from their inventory.

- **Unrecorded Equipment** - Ten (15%) of 65 equipment items observed at DPSS field offices were not recorded on DPSS' equipment lists. The ten items include some with significant value such as a multifunction printer that could have been purchased for up to $10,000.

- **Inaccurate Tracking** - Twenty-seven (27%) of 100 items had an inaccurate custodian, location, or equipment description recorded on DPSS' equipment lists. We also analyzed all 59,981 items on DPSS' IT equipment lists and noted that 1,336 (2%) are missing the required make/model, manufacturer's serial number, asset custodian, etc., or are indicated as assigned to an individual who no longer works for DPSS.

We noted that DPSS does not properly conduct physical inventories of their IT equipment because they do not always update their asset listings based on the results of their physical counts. DPSS also does not have up-to-date policies and procedures for maintaining equipment inventories, and staff who manage equipment inventories indicated that they did not receive adequate training in their job duties/responsibilities, as required by CFM 8.3.1.

RECOMMENDATIONS

Department of Public Social Services management:

1. Update equipment inventories for the inaccuracies noted in our review, ensure staff conduct accurate physical equipment inventories, and investigate and update inventory lists for any discrepancies.

2. Report the four missing equipment items through the County's computer incident response process, and remind all staff to report missing equipment to their Department Information Security Officer.

3. Ensure staff document approvals for all equipment disposals.

4. Update policies and procedures for maintaining equipment inventories, and train staff on their duties and responsibilities for managing equipment inventories.

DPSS RESPONSE TO 1:
DPSS agrees with the recommendation. However, subsequent to the review, it was confirmed that the 10 equipment items noted under Unrecorded Equipment (including the Xerox multi-function printer) were in DPSS' Asset Management System (AMS) and were overlooked by staff. The Inventory Control Unit received reinforcement training on conducting physical equipment inventories in August 2013. Refresher training will be conducted once the update of IT equipment policies and procedures is completed.

TARGET DATE: December 31, 2014

DPSS RESPONSE TO 2:
DPSS agrees with the recommendation. Three of the four missing equipment items were reported through the County's computer incident reporting procedures. The server referred to as missing was never missing and continues to be in use today. There was merely a mismatch of the serial number and asset tag in the AMS system. This data entry error was corrected in the AMS system.

COMPLETED: July 10, 2014

DPSS RESPONSE TO 3:
DPSS agrees with the recommendation. The Inventory Control Unit received reinforcement training on equipment disposal procedures in August 2013. Refresher training will be conducted once the update of IT equipment policies and procedures is completed.

TARGET DATE: December 31, 2014

DPSS RESPONSE TO 4:
DPSS agrees with the recommendation and is in the process of updating the policies and procedures.

TARGET DATE: December 31, 2014

INVENTORY SYSTEMS

CFM Chapter 6 requires departments to use the electronic Countywide Accounting and Purchasing System (eCAPS) to account for capital IT equipment with a useful life over one year and acquisition cost over $5,000.

We noted that DPSS accounts for capital IT equipment in their own asset management system and in eCAPS. As a result, staff perform duplicate data entry to update both systems when capital equipment is purchased, disposed, or transferred to a new custodian. DPSS' materials management staff indicated that tracking capital assets in DPSS' Asset Management System does not provide any significant benefit or control beyond the tracking that eCAPS provides. In addition, the duplicate data entry is time consuming and can result in discrepancies between the two systems.

To save staff time and improve the accuracy of capital equipment inventories, DPSS management should evaluate discontinuing duplicate capital equipment tracking in their Asset Management System.

RECOMMENDATIONS

5. DPSS management evaluate discontinuing duplicate capital equipment tracking in the Asset Management System.

DPSS RESPONSE TO 5:
DPSS agrees with the recommendation and will evaluate discontinuing duplicate capital equipment tracking in the Asset Management System.

TARGET DATE: December 31, 2014

PORTABLE COMPUTER ENCRYPTION

Board Policy 6.110 requires departments to encrypt all County owned portable computers. Encryption helps render data unreadable if a computer is lost or stolen, and protects against unauthorized disclosure of personal/confidential information such as recently occurred at a Health Services contractor.

DPSS could not locate encryption documentation for 613 (46%) of their 1,323 portable computers because their encryption records did not always have enough information, such as an asset tag or serial number, to identify the encrypted device. We analyzed 44 portable computers assigned to DPSS staff and noted that five (11%) did not have encryption software installed. This occurred in part because one field office bypassed DPSS' central receiving unit that is responsible for receiving and encrypting all portable computers. In addition, DPSS management does not periodically monitor the Department's portable computers to ensure that each has been encrypted.

To protect County data and software on portable computers, DPSS needs to implement the following recommendations.

RECOMMENDATIONS

DPSS management:

6. Enhance encryption documentation so staff can locate the encryption records for all portable computers.
7. Encrypt all portable computers, and ensure all portable computers are requested and processed through the Department's central receiving unit.
8. Periodically monitor to ensure all portable computers are encrypted.

DPSS RESPONSE TO 6:
DPSS agrees with the recommendation. DPSS was one of the first Departments to implement encryption of laptops following the adoption of that requirement in County policy. Reporting on encrypted devices was not robust in the prior solution implemented to meet the policy requirement. Effective May 2014, DPSS implemented new encryption software and policies for all computers and laptops. The new encryption solution now has robust reporting capabilities. It monitors the DPSS network for unencrypted devices and notifies DPSS IT personnel when a new device needs to be encrypted. DPSS has updated the computer build images in the central processing center for the Department to include the encryption software on all new computers prior to them being distributed. Furthermore, the new reports will be utilized to actively monitor encryption requirements on all devices on DPSS' networks in order to ensure compliance with the newly expanded County encryption policy.

COMPLETED: August 29, 2014

DPSS RESPONSE TO 7:
DPSS agrees with the recommendation. DPSS was one of the first Departments to implement encryption of laptops following the adoption of that requirement in County policy. Reporting on encrypted devices was not robust in the prior solution implemented to meet the policy requirement. Effective May 2014, DPSS implemented new encryption software and policies for all computers and laptops. The new encryption solution now has robust reporting capabilities. It monitors the DPSS network for unencrypted devices and notifies DPSS IT personnel when a new device needs to be encrypted. DPSS has updated the computer build images in the central processing center for the Department to include the encryption software on all new computers prior to them being distributed. Furthermore, the new reports will be utilized to actively monitor encryption requirements on all devices on DPSS' networks in order to ensure compliance with the newly expanded County encryption policy. Additionally, all portable computer requests require approval by the Department's Information Technology Division (ITD) and are then processed through the Department's central receiving unit. All portable computers are subsequently released by the Department's central receiving unit to ITD for proper encryption before they are issued to end users.

COMPLETED: August 29, 2014

DPSS RESPONSE TO 8:
DPSS agrees with the recommendation. DPSS ensures all portable computers are encrypted through the use of encryption reports and conducts a 100% review during the annual physical inventory.

COMPLETED: January 30, 2014

HARD DRIVE DISPOSAL

Board Policy 6.112 requires departments to erase all data and software from computer hard drives before disposing the hard drives from County inventory. The County's Hard Drive Cleaning Standard requires departments who contract for hard drive erasing services to obtain a certification from the vendor. The vendor certification should include the serial number of every hard drive erased or destroyed, the date/method of destruction, and name/signature of the person who performed the destruction.

We reviewed ten computing devices that DPSS disposed and noted that they could not adequately document that any of the hard drives were successfully removed and destroyed. While DPSS provided some lists of hard drives that they sent to their vendor for destruction, they could not document which of the hard drives, if any, came from the ten computing devices reviewed. DPSS also did not require the vendor to provide a certificate of destruction that includes:

- Hard drive serial number of every device destroyed
- Date and method of hard drive destruction
- Printed name and signature of the person who performed the destruction

DPSS indicated that they dispose of approximately 300-400 computing devices a year that contain confidential information. To reduce the risk of inappropriately disclosing confidential information, DPSS needs to implement the following recommendations.

RECOMMENDATIONS

DPSS management:

9. Document the serial number of every hard drive removed from a computing device for destruction, and the device that each hard drive was removed from.

10. Require vendors who dispose of computer hard drives to provide certificates of destruction that include the serial number of every hard drive destroyed, date/method of destruction, and printed name/signature of the person who performed the destruction.

DPSS RESPONSE TO 9 AND 10:
DPSS agrees with the recommendations. Per DPSS' hard drive destruction policy, a listing of each hard drive removed from a computing device is prepared that includes the serial number and the asset tag information of the specific computer from which the hard drive was removed. This list accompanies the hard drives to the destruction vendor who is required to certify the destruction based on the identifying information contained on the listing.

COMPLETED: July 31, 2014

SYSTEMS ACCESS

Board Policy 3.040 requires departments to safeguard personal and confidential information on their IT systems. CFM 8.7.4.2 requires departments to limit unneeded systems access by immediately updating user access when employees terminate or change job duties.

Inappropriate Access

We reviewed user access for three of 59 mission critical DPSS systems; the Los Angeles Eligibility Automated Determination, Evaluation and Reporting System (LEADER), the Greater Avenues for Independence Employment Activity and Reporting System (GEARS), and the In-Home Support Services Case Assignment and Management System (CAMS), and noted the following unneeded access:

- One CAMS, two GEARS, and 439 LEADER system users terminated or transferred from DPSS but continued to have access for 15 days to three years after termination. We reviewed system activity reports for seven of these LEADER user accounts, and noted that one account (14%) was used after the employee's transfer date to view personal and confidential information for clients in the CalWORKs program.

Subsequent to our review, DPSS indicated that they investigated the transferred user's activity and determined that the account was not used after the employee left DPSS. The Department indicated that there was an error in the user activity report generated during the audit, and that the error made it appear that the user had accessed the system. DPSS needs to resolve errors in the LEADER user activity reports to ensure the Department can identify any inappropriate system activity.

- Seven (47%) of 15 GEARS user accounts reviewed have more access than they need for their job duties. Specifically, six employees with accounting and staff support duties can view confidential client information they do not need for their job duties. Another user changed job duties in 2008, but DPSS never restricted access that he no longer needed for his job duties, such as access to approve metro card payments.

Most of the inappropriate access noted above occurred because DPSS staff did not follow the Department's procedures for immediately updating or removing systems access when employees terminate or transfer job duties.

RECOMMENDATIONS

DPSS management:

11. Immediately cancel terminated and transferred employees' systems access, limit unneeded GEARS access, and remind staff to update or remove systems access when employees terminate or transfer.

12. Periodically monitor all users' access for appropriateness.

13. Resolve errors in LEADER user activity reports to ensure the Department can identify any inappropriate system activity.

DPSS RESPONSE TO 11:
DPSS agrees with the recommendation. DPSS issued a memo to District Directors and GAIN Regional Directors to reiterate the Exit Procedures to immediately update or remove systems access when employees terminate or transfer job duties. Access to GEARS is automatically suspended after 30 days when users do not log onto the system. In addition, Bureau of Contract and Technical Services (BCTS) receives a monthly listing from the Human Resources Division (HRD) of employees who have left the Department to ensure that system(s) access is terminated.

COMPLETED: June 26, 2014

DPSS RESPONSE TO 12:
DPSS agrees with the recommendation. An instructional memo, Management Review of Employee Access to Information Technology Systems, dated 10/21/14, was issued to all departmental managers. The memo addressed the County Fiscal Manual Section 8.7.4.2 requirement for a quarterly review of

employee access levels by managerial and Program Integrity Compliance Officer staff. The memo also emphasized the responsibilities for taking timely action in terminating and disabling employee system access(es) due to employee job changes, transfers, retirements, etc.

COMPLETED: October 21, 2014

DPSS RESPONSE TO 13:
DPSS agrees with the recommendation. DPSS will work with Unisys to resolve errors in the LEADER user activity reports.

TARGET DATE: February 28, 2015

Access Controls

Board Policy 6.101 requires that systems have appropriate user authentication such as log-on identifications and complex passwords that reset every 90 days.

We noted 38 LEADER users with high-level system administrator access are never forced to reset their passwords, increasing the risk that a compromised password could be used to access sensitive system information. We also noted that GEARS passwords are not case-sensitive, making them easier to guess.

RECOMMENDATION

DPSS management:

14. Ensure all LEADER users are forced to reset their password every 90 days.

15. Evaluate modifying GEARS to require case-sensitive passwords.

DPSS RESPONSE TO 14:
DPSS agrees with the recommendation. All LEADER users are now required to reset their password every 90 days.

COMPLETED: May 30, 2014

DPSS RESPONSE TO 15:
DPSS agrees with the recommendation. An analysis was completed by the vendor and GEARS will be modified to require case-sensitive passwords.

TARGET DATE: November 28, 2014

ANTIVIRUS SOFTWARE

Board Policy 6.102 requires departments to ensure they have functioning up-to-date antivirus software protection for all County computers. Departments must update antivirus software regularly to protect against the most current threats.

Nine (25%) of 36 computers reviewed had antivirus software protection that was outdated from nine days up to 14 months. The computers with outdated antivirus software are assigned to units processing critical and sensitive information such as LEADER technology management and Medi-Cal services sections.

DPSS management should ensure all computers have current antivirus protection.

RECOMMENDATION

16. DPSS management ensure all computers have current antivirus protection.

DPSS RESPONSE TO 16:
DPSS agrees with the recommendations. DPSS utilizes and closely manages the centralized McAfee Enterprise Anti-Virus Management service (which is a County Preferred platform, supported by the Office of the Chief Information Officer) that ensures departmental computers and laptops connected to the DPSS network have fully functioning and up-to-date anti-virus software protection. DPSS has utilized this County's standard anti-virus management solution for well over ten years to keep our systems highly protected from virus, malware penetrations or incidents. The McAfee ePO software consists of anti-virus agents installed on each DPSS computing device to ensure that they receive the latest anti-virus definitions whenever the device connects to the network.

The Department has many devices that do not connect to the DPSS network frequently, such as some of the laptops. Therefore, the versions of anti-virus software present on the laptops can become out of date while they remain in a disconnected state. However, when they do connect to the DPSS network, the McAfee ePO software updates their anti-virus definitions and other components. This approach is in compliance with best County practices and the expectations of the Office of the Chief Information Officer. DPSS verified that the devices cited in the audit with outdated anti-virus software subsequently received the latest updates when the users connected to the network. DPSS will also be sending out a reminder notice to all users of the need to connect to the network with more frequent regularity to receive all the security patches and anti-virus updates, especially with portable devices like laptops.

COMPLETED: May 30, 2014

PHYSICAL SECURITY

Board Policy 6.106 requires departments to physically safeguard IT resources from tampering, damage, theft, or unauthorized physical access. These controls help prevent data breaches such as the recent breach at a Health Services contractor.

We conducted interviews and walk-throughs at seven DPSS offices that house critical IT resources such as data centers, computers, multifunction printers, etc., and noted that DPSS generally does a good job physically securing its IT resources. However, we also noted that one of DPSS' most critical data centers containing confidential data does

not have surveillance cameras in place to deter/detect intruders. Another facility containing confidential data has functioning surveillance cameras, but the footage is recorded-over after 48 hours of filming, increasing the risk that a security incident on a Friday could be recorded-over if it was not discovered until the following Monday.

Board Policy 6.106 does not specifically require surveillance cameras. However, to deter intruders and increase the likelihood of DPSS recovering any stolen IT equipment or data, DPSS should evaluate implementing the following recommendations.

RECOMMENDATION

DPSS management evaluate:

17. Implementing surveillance cameras at facilities containing critical Information technology resources or confidential client data.

18. Increasing the retention period for recorded surveillance footage to increase the likelihood that security incidents can be captured.

DPSS RESPONSE TO 17:
DPSS agrees with the suggested recommendation. The reference to a "DPSS data center" in the finding is not accurate, as DPSS hosts and/or co-locates its mission critical systems at the Internal Services Department (ISD) data center. The site referenced as a DPSS data center is merely a location where a portion of the Department's IT staff is housed. DPSS completed the installation of surveillance cameras at the three locations mentioned: Information Technology Division, DPSS Headquarters and Materials Management Section with an expanded video retention schedule of 60 days.

COMPLETED: June 30, 2014

DPSS RESPONSE TO 18:
DPSS agrees with this recommendation. The Information Technology Division, Materials Management Section and DPSS Headquarters now have surveillance cameras installed. All surveillance videos are saved for 60 days and are reviewed on a monthly basis for any suspicious activity.

COMPLETED: June 30, 2014

INFORMATION SECURITY TRAINING

Board Policy 6.111 requires departments to provide Training to all IT resource users at the time they are hired and periodically thereafter. Training should be documented to assist management in determining employee awareness and participation.

We noted that DPSS does a good job providing Training at new employee orientation, but can improve their process for Training thereafter. DPSS management provides ongoing Training to staff through bulletins and newsletters on security topics. However, DPSS does not have a plan that outlines the frequency and type of content that they

need to deliver to staff. As a result, we could not determine whether DPSS delivered all the intended Training content through the bulletins and newsletters. In addition, DPSS could not document that IT users received and were aware of the Training materials.

After the start of our audit, DPSS conducted a comprehensive classroom Training. We reviewed Training documentation at six field offices and could not determine if the Department trained all necessary staff due to a lack of information. For example, DPSS did not have a list of all required attendees so that we could verify that each was on a sign-in sheet. In addition, many of the sign-in sheets did not include enough information to identify the attendee, such as an employee identification number and work location.

Board Policy 6.111 does not specify IT training content or how it should be documented. However, DPSS can improve their Training delivery by developing a plan that outlines the Training content that staff need to receive, and the documentation needed to evaluate staff participation and awareness.

RECOMMENDATION

19. Department of Public Social Services management develop a plan that outlines the information technology security awareness training content staff need to receive, and the documentation needed to evaluate staff participation and awareness.

DPSS RESPONSE TO 19:
DPSS agrees with the recommendation. When DPSS provided Security Awareness training via classroom-based sessions, DPSS collected attendance via sign-in sheets across multiple locations (which is a common practice throughout the County). Staff were able to register and attend at numerous locations across the Department. Also, staff were accommodated to attend alternative sessions in locations other than their original registration location when conflicts occurred. Their attendance at alternative locations was captured by allowing them to handwrite their name and signature and append it to the registration/sign-in magistrate. While their names were captured at the alternative locations, their names were not simultaneously removed from the registration magistrates of their originally selected session locations, which may have contributed to this finding.

As a result, DPSS has placed the security awareness training modules on the Learning Management System (LMS), where they can be taken by Department staff directly from their own desks. The Department continues to provide additional security reminders and awareness tips via regular newsletters, alerts, email blasts, and focused trainings to increase staff knowledge and awareness of potential security threats. Any future security awareness training that is deemed to be 'mandatory' for all employees will be placed on the LMS to provide improved attendance tracking capabilities. Furthermore, the Chief Information Security Office established the Security Awareness Security Engineering Team. This team has now drafted the Information Security Awareness program and training standards document, which defines the plan and outlines the detail of what DPSS will follow going forward.

COMPLETED: May 31, 2014