



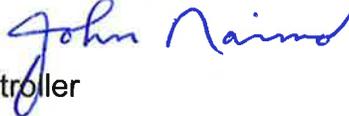
JOHN NAIMO  
AUDITOR-CONTROLLER

**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

July 1, 2015

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: **PROBATION DEPARTMENT – INFORMATION TECHNOLOGY AND SECURITY 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 Probation Department's (Probation or Department) compliance with the Policies, and related County standards and requirements. Probation has numerous critical systems, such as the Adult Probation System (APS) and Probation Case Management System (PCMS), which are used to manage adult and juvenile probationer case information, respectively; and the Probation Electronic Medical Records System (PEMRS), which contains medical records for detained juveniles. Probation also reported having over 17,000 IT devices, such as desktop computers, laptops, printers, servers, tablets, etc. Our review included testing access controls, IT equipment control, antivirus and encryption software, equipment disposition, and IT security awareness training.

**Results of Review**

Our review disclosed that Probation needs to significantly improve its controls over areas such as IT access, equipment control, computer encryption, and equipment disposition. The following are examples of areas for improvement:

*Help Conserve Paper – Print Double-Sided  
"To Enrich Lives Through Effective and Caring Service"*

- **Inappropriate Access** – Probation needs to restrict unneeded access to APS, PCMS, PEMRS, and their Virtual Private Network (VPN). We noted that Probation did not remove APS, PCMS, PEMRS, and VPN access for up to seven years for 695 users after they terminated from the Department. Thirty-three terminated employee accounts were used to access PCMS up to five years after the employees terminated. The access allows users to view, enter, and update probationer's personal and case information. However, we could not determine how the access was used because PCMS does not maintain an audit trail of users' activity as required by County Fiscal Manual Section 8.10.0.

Also, APS and PCMS, which are accessible by most of Probation's 5,500 active employees, maintain probationer Social Security Numbers (SSN), and all user accounts with access to APS and PCMS have access to the SSNs. Probation management confirmed that not all users need the full SSN to perform their job. Also, 173 (17%) of Probation's 1,049 VPN users have not used their access in over a year, including 99 users who have never used their access. Probation management confirmed that the unused access was not necessary. We estimate that Probation could have reduced VPN access token costs by at least \$19,000 over the past two years if they had removed the unnecessary access timely.

*Probation's attached response indicates that they have deactivated all terminated/unnecessary PCMS, PEMRS, and VPN users' access, and are working to deactivate terminated APS users' access. Probation's response also indicates that they agree with our recommendation to establish a system audit trail and to properly restrict and/or mask SSN's, and will evaluate incorporating these features into future system enhancements.*

- **IT Equipment Control** – Probation needs to significantly improve its controls over IT equipment. Staff could not locate 18 (45%) of the 40 items from Probation's equipment list, including desktop computers and laptops that may contain sensitive probationer data. Department management subsequently provided documentation to support that four of the missing laptops were donated and two other laptops were stolen, but Probation did not remove these six items from their inventory. In addition, the stolen laptops were not reported to the Auditor-Controller or County's Chief Information Officer as required by the Policies.

We also noted that 8,907 (52%) of the 17,180 items on Probation's IT equipment list were missing the required make, model, and/or asset custodian, or were assigned to individuals who no longer work for Probation. Probation also does not conduct annual physical inventories of their IT equipment at all locations.

*Probation's attached response indicates that they investigated the 12 missing computing devices and one was located, three were salvaged or stolen, and eight continue to be missing. Probation has or will complete the required paperwork for these devices in compliance with the Policies. Probation's response also indicates that they will conduct Department-wide annual physical inventories of their equipment and update their inventory system timely.*

- **Portable Computer Encryption** – Probation needs to encrypt its portable computers and improve encryption documentation. Two (18%) of the 11 laptops tested did not have encryption software installed. This includes one laptop used to access information in PCMS that may contain sensitive probationer data. We were also not able to determine whether 24 other laptops we selected were encrypted because they were either missing or disposed of during our review, and Probation does not maintain records to support computer encryption for each of their 1,853 portable computers.

*Probation's attached response indicates that they encrypted all laptops subsequent to our review. They also implemented a new encryption program that maintains records of all encrypted devices, which allows Probation staff to periodically monitor device encryption.*

- **Hard Drive Disposal** – Probation needs to ensure all data on County hard drives is rendered unreadable and unrecoverable (sanitized) before authorizing their disposal, as required by Board Policy 6.112. We noted that staff complete disposition forms indicating that hard drives were sanitized and management signs off on the forms to authorize their disposal before the hard drives are sanitized. After the forms are signed, the hard drives are placed in a storage room to be sanitized at a later time, unnecessarily creating a need for inventory and monitoring records that Probation does not maintain. As a result, there is no record that hard drives were ever successfully sanitized.

*Probation's attached response indicates that they have established a process to sanitize hard drives before authorizing their disposal. They have also updated the disposition form to include the make, model, and serial number of the hard drives taken from Probation computers to improve hard drive disposal records.*

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

### **Review of Report**

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

We thank Probation 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) 253-0100.

JN:AB:RS:MP

Attachments

c: Sachi A. Hamai, Interim Chief Executive Officer  
Jerry E. Powers, Chief Probation Officer  
Dr. Robert K. Pittman, Chief Information Security Officer, Chief Information Office  
Public Information Office  
Audit Committee

## PROBATION DEPARTMENT INFORMATION TECHNOLOGY AND SECURITY REVIEW

### Background

The Board of Supervisors' (Board) Information Technology (IT) and Security Policies (Policies) require all County departments to comply with minimum IT security standards. 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 Probation Department's (Probation or Department) compliance with the Policies, and related County standards and requirements. Probation has numerous critical systems, such as the Adult Probation System (APS) and Probation Case Management System (PCMS), which are used to manage adult and juvenile probationer case information, respectively; and the Probation Electronic Medical Records System (PEMRS), which contains medical records for detained juveniles. Probation also reported having over 17,000 IT devices, such as desktop computers, laptops, printers, servers, tablets, etc. Our review included testing access controls, IT equipment control, antivirus and encryption software, equipment disposition, and IT security awareness training.

### Access Controls

Board Policy 3.040 requires departments to safeguard personal or confidential information contained on their IT resources. County Fiscal Manual (CFM) Section 8.7.4.2 also requires departments to limit unneeded access by immediately updating user access rights when employees terminate or change job duties, and by periodically reviewing the propriety of users' access levels.

### Inappropriate Access

We reviewed Probation users' Virtual Private Network (VPN) access, Internet access, and system access for three of the Department's 12 mission-critical systems, including APS, PCMS, and PEMRS. We noted numerous instances of inappropriate access. Specifically:

- **Terminated Employees with Access** – Access for 695 users (three VPN, 95 APS, 580 PCMS, and 17 PEMRS users) remained active for up to seven years after they terminated from Probation. System records also showed that PCMS was accessed for 33 of these users between two days and up to five years after the employees terminated. The access allows users to view, enter, and update probationer's personal and case information. However, we could not determine how the access was used because PCMS does not maintain an audit trail of users' activity as required by CFM Section 8.10.0.

Probation needs to immediately cancel terminated and transferred employees' user access, and establish a procedure that ensures the removal of future terminated and transferred employees' access timely. Probation management should also evaluate modifying PCMS to maintain an audit trail of users' activity.

- **Unnecessary Access to Social Security Numbers (SSN)** – Probation's adult and juvenile probationer case tracking systems (APS and PCMS), which are accessible by most of Probation's 5,500 active employees, maintain probationer SSNs and all user accounts with access to APS or PCMS have access to the SSNs. Probation management confirmed that not all users need the full SSN to perform their job. To protect probationer information and ensure system users only access information necessary to perform their job duties, Probation should evaluate modifying APS and PCMS to restrict access to and/or mask SSNs.
- **Unused VPN Access** – 173 (17%) of Probation's 1,049 VPN users have not used their access in over a year, including 99 users who have never used their access. Probation management confirmed that the unused access was not necessary. We estimate that if the Department had removed the unnecessary access timely, including the three VPN users who terminated (from the section above), they could have reduced VPN access token costs by at least \$19,000 over the past two years. Probation needs to remove the unnecessary VPN access noted in our review.
- **Unauthorized Internet Access** – We reviewed five of the eight Probation users with higher-level Internet access and noted that four (80%) users were not authorized for their access. Two users had only been authorized for basic Internet access, and the other two users did not obtain the required Director's approval. Probation management needs to remove the unauthorized higher-level Internet access or obtain the Director's approval as required, and ensure that all Internet access is properly authorized.

We also noted that Probation does not have written policies and procedures to periodically review users' VPN access, Internet access, and APS and PCMS access as required by CFM Section 8.7.4.2. To ensure access is consistent with users' job duties, Probation needs to establish written policies and procedures to periodically review users' VPN access, Internet access, and APS and PCMS access.

### Recommendations

#### **Probation Department management:**

1. **Immediately cancel terminated and transferred employees' user access, and establish a procedure that ensures the removal of future terminated and transferred employees' access timely.**

2. Evaluate modifying the Probation Case Management System to maintain an audit trail of users' activity.
3. Evaluate modifying the Adult Probation System and Probation Case Management System to restrict and/or mask access to Social Security Numbers.
4. Remove the unnecessary Virtual Private Network access noted in our review.
5. Remove the unauthorized higher-level Internet access or obtain the Director's approval as required, and ensure all Internet access is properly authorized.
6. Establish written policies and procedures to periodically review users' Virtual Private Network access, Internet access, and Adult Probation System and Probation Case Management System access.

### User Authentication

We noted that critical Probation systems do not always require unique log-on identifications (IDs) and complex passwords, as required by Board Policy 6.101. Specifically:

- **Generic User IDs** – We noted ten PCMS and 41 PEMRS log-on IDs were not assigned to specific employees, including some with the ability to change probationers' personal or case information in PCMS or change physician and clinical notes in PEMRS. As a result, there is no record of who accessed system information with those IDs. Although most of the IDs have not been used for several years, to protect against unauthorized access and potential violations of privacy and security requirements over protected health information, Probation should ensure all IDs in PCMS and PEMRS are assigned to specific individuals.
- **Password Controls** – APS does not enforce password complexity as required by CFM Section 8.6.4, increasing the risk for unauthorized access. We also noted one staff who taped their computer user ID and password on their laptop. Probation should evaluate modifying APS to enforce password complexity requirements as defined in the CFM, and remind employees to keep their user ID and password secured.

## Recommendations

### Probation Department management:

7. **Ensure all log-on identifications in the Probation Case Management System and the Probation Electronic Medical Records System are assigned to specific individuals.**
8. **Evaluate modifying the Adult Probation System to enforce password complexity requirements as defined in the County Fiscal Manual.**
9. **Remind employees to keep their user identification and password secured.**

## IT Equipment Control

Board Policies 6.106 and 6.109 require departments to establish safeguards over IT equipment and to promptly report missing or stolen items to the Auditor-Controller's (A-C) Office of County Investigations (OCI) and the Chief Information Office (CIO), as applicable. CFM Section 6.8.0 also requires departments to inventory their IT equipment annually and maintain an up-to-date IT equipment list.

We reviewed Probation's IT equipment list, which includes servers, and sampled items at five Probation field offices. We noted significant control weaknesses that could allow County computers and their data to go missing or be stolen without being detected. Specifically:

- **Missing Equipment** – Staff could not locate 18 (45%) of the 40 items that we selected from the Department's equipment list. This includes one server, five desktop computers, and 12 laptops, which in some cases were used to access critical Probation systems and could contain sensitive probationer data. Based on our review, it appears the missing items would not have contained protected health information.

Department management subsequently provided documentation to support that four laptops were donated in 2013, and that two other laptops were stolen in 2008 and 2012, but these six items were not removed from their inventory. The stolen laptops were also not reported to the A-C or CIO. Weaknesses in Probation's security awareness training program, discussed further below, may have contributed to staff and managers' lack of knowledge about the need to report these incidents.

Probation management needs to investigate the 12 missing computing devices noted in our review, update inventory records when items are donated or stolen, and report lost or stolen computers as required by the Policies and CFM.

- **Inaccurate Tracking** – The Department does not maintain a complete and accurate IT equipment list. For example, a server that we randomly selected during a site visit was not on the Department's equipment list. During these visits, we also confirmed that custodians, locations, and/or equipment descriptions on 42 (65%) of the 65 items reviewed were not accurate. In addition, using audit software we noted that 8,907 (52%) of the 17,180 items on the equipment list were missing the required make, model, and/or asset custodian, or were assigned to individuals who no longer work for Probation. Probation needs to update its IT equipment inventory for the inaccuracies identified in our review.
- **Asset Tags** – Probation generally does a good job of using asset tags to account for IT equipment. However, we noted that one (2%) of the 65 items reviewed did not have an asset tag to identify it as County property. Probation needs to ensure a County property tag is attached to all County IT resources as required by Board Policy 6.106.

We also noted the Department does not conduct annual physical inventories of their IT equipment at all locations. In addition, when physical inventories are performed, staff do not update equipment inventory records with the results of their physical counts, which render the inventories pointless. Probation needs to inventory all IT equipment immediately, and annually thereafter, and update inventory records with the results of the physical counts.

### Recommendations

#### **Probation Department management:**

- 10. Investigate the 12 missing computing devices noted in our review.**
- 11. Update inventory records when items are donated or stolen.**
- 12. Report lost or stolen computers as required by the Board of Supervisors Policy 6.109.**
- 13. Update its Information Technology equipment inventory for the inaccuracies noted in our review.**
- 14. Ensure a County property tag is attached to all County Information Technology resources as required by Board of Supervisors Policy 6.106.**
- 15. Inventory all Information Technology equipment immediately, and annually thereafter, and update inventory records with the results of the physical counts.**

### Portable Computer Encryption

Board Policy 6.110 requires departments to encrypt all County portable computers. Encryption helps render data unreadable if a computer is lost or stolen, and protects against unauthorized disclosure of personal/confidential information. A recent theft of computers from a County contractor highlighted the importance of a robust encryption program.

Probation staff generally encrypt laptops during the software setup process before laptops are assigned to departmental personnel. However, we noted unencrypted laptops and a lack of documentation to support and help monitor computer encryption. Specifically:

- Two (18%) of the 11 laptops tested did not have encryption software installed. One of the unencrypted computers is used to access information in PCMS and may store sensitive data, increasing the County's risk of exposure. The Department needs to encrypt all portable computers as required by the Policies.
- Twenty-four laptops selected for review were not available for testing and Probation did not maintain records to support that they were encrypted. Specifically, Probation provided documentation to support that 12 laptops were disposed of during our review, and 12 other laptops, that may contain sensitive probationer data, could not be located (as noted in the IT Equipment Control section above). The Department also did not maintain encryption records that include the computer's asset tag or serial number, to support and help monitor encryption on these and Probation's other 1,829 portable computers.

Probation management needs to maintain detailed encryption records and periodically monitor encryption on the Department's portable computers.

### Recommendations

#### **Probation Department management:**

- 16. Encrypt all portable computers as required by Board of Supervisors Policy 6.110.**
- 17. Maintain detailed encryption records and periodically monitor encryption on the Department's portable computers.**

### Hard Drive Disposal

Board Policy 6.112 requires departments to render unreadable and unrecoverable (sanitize) all data and software from computer hard drives before disposing of the devices from County inventory.

We reviewed Probation's procedures for sanitizing and disposing of hard drives and noted control weaknesses that increase the risk for the loss and unauthorized disclosure of information. Specifically:

- Probation does not sanitize hard drives before authorizing their disposal. We noted that staff complete disposition forms indicating that the hard drives were sanitized and management signs off on the forms to authorize their disposal from County inventory. However, the forms are completed and signed before the hard drives are sanitized, and the hard drives are placed in a storage room to be sanitized at a later time, unnecessarily creating a need for inventory and monitoring records that Probation does not maintain. As a result, there is no record that hard drives were ever successfully sanitized.

Probation management needs to ensure hard drives are sanitized before authorizing their disposal.

- Probation's disposition forms do not identify the make, model, and serial number of the hard drives taken from Probation computers, making it impossible for management to verify that the proper hard drives were sanitized. Probation needs to ensure disposition forms identify the make, model, and serial number of hard drives taken from Probation computers.

### **Recommendations**

#### **Probation Department management:**

- 18. Ensure hard drives are sanitized before authorizing their disposal.**
- 19. Ensure disposition forms identify the make, model, and serial number of hard drives taken from Probation computers.**

### **Capital IT Equipment**

CFM Section 6.1.1 requires departments to record assets that have a useful life of over one year and an acquisition cost of over \$5,000 (i.e., capital assets) in the electronic Countywide Accounting and Purchasing System (eCAPS). The asset information, which is used for financial reporting, must be recorded within 30 days after invoice payment.

We compared Probation's IT equipment list to their list of servers in eCAPS and noted that the Department has not recorded ten servers, totaling almost \$80,000, in eCAPS. These servers were purchased between 2010 and 2012, and as a result, have not been reflected in the County's financial statements for several years. To ensure the County has accurate records for financial reporting, Probation management should ensure staff record capital IT equipment within 30 days of invoice payment.

**Recommendation**

- 20. Probation Department management ensure staff record capital IT equipment in the electronic Countywide Accounting and Purchasing System within 30 days after invoice payment.**

**IT Security Awareness Training**

We noted that Probation management does not provide IT security awareness training to its IT resource users at the time they are hired and periodically thereafter, as required by Board Policy 6.111. The lack of training may have contributed to some of the weaknesses noted in our review, including instances where staff did not report stolen laptops or where they taped their user ID and password to the laptop. Probation management needs to ensure all IT resource users receive adequate IT Security Awareness Training.

**Recommendation**

- 21. Probation Department management ensure all Information Technology resource users receive adequate Information Technology Security Awareness Training.**

**Internet Usage**

Probation Directive 923 requires that employees store any sensitive or critical data on the Department's network drive. Probation management also indicated that staff should not save County data on Internet sites that provide storage space (i.e., Internet storage sites).

We reviewed a Department-level summary of Probation's Internet activity and noted that Internet storage sites were visited over 230 times during a one month period. Although this activity does not confirm that staff are storing County data online, it increases the risk for such inappropriate activity and should be investigated.

Probation management should work with the A-C's OCI to obtain Internet activity details and investigate the Internet storage activity noted in our review.

**Recommendation**

- 22. Probation Department management work with the Auditor-Controller's Office of County Investigations to obtain Internet activity details and investigate the Internet storage activity noted in our review.**

### IT Risk Assessment

Board Policy 6.107 requires that departments perform risk assessments on their critical IT services by properly completing the A-C's Internal Control Certification Program (ICCP). Departments must certify that proper controls are in place, or that action is being taken to correct any weaknesses or vulnerabilities.

We noted that Probation did not perform risk assessments on seven of their mission-critical systems, including the KIOSK system used by probationers to fulfill reporting requirements, and the Pretrial + system used by Deputy Probation Officers to evaluate whether inmates should be released from jail on their own recognizance. To help assess and improve controls over IT security, Probation management needs to perform risk assessments on all their mission critical systems by properly completing the ICCP.

### Recommendation

- 23. Probation Department management perform risk assessments on all mission critical systems by properly completing the Internal Control Certification Program.**



**COUNTY OF LOS ANGELES  
PROBATION DEPARTMENT**

9150 E. Imperial Hwy, Downey, CA 90242  
(562) 940-2501



**JERRY E. POWERS**  
Chief Probation Officer

--REVISED--

June 25, 2015

TO: John Naimo  
Auditor-Controller

FROM: Jerry E. Powers *JA*  
Chief Probation Officer

SUBJECT: **RESPONSE TO AUDITOR-CONTROLLER'S INFORMATION  
TECHNOLOGY AND SECURITY REVIEW**

Attached is the Probation Department's response to the recommendations made in the Auditor-Controller's report of its review of Information Technology and Security. We concur with and have taken or initiated corrective actions to address the recommendations contained in the report.

If you have any questions or require additional information, please contact me or Benny Chacko, Chief Information Officer, at (562) 940-2515.

JEP: bc

Attachment

## RESPONSE TO AUDITOR-CONTROLLER'S INFORMATION TECHNOLOGY AND SECURITY REVIEW

### AUDITOR-CONTROLLER RECOMMENDATION #1

Immediately cancel terminated and transferred employees' user access, and remind staff to remove future terminated and transferred employee's access timely.

#### Probation Response:

The Probation Department agrees with the Auditor-Controller's recommendation. Regarding terminated employees who still have access, the following information has been confirmed:

- PCMS – All 580 identified user accounts were deactivated as of May 3, 2015.
- PEMRS – 17 user accounts were deactivated as of January 20, 2015.
- APS – The Information Systems Bureau's Client Support Section is working to deactivate the identified user accounts.

Staff have been reminded to remove future terminated and transferred employees' access in a timely manner.

Estimated Task Completion Date: June 30, 2015

### AUDITOR-CONTROLLER RECOMMENDATION #2

Evaluate modifying the Probation Case Management System (PCMS) to maintain an audit trail of users' activity.

#### Probation Response:

The Probation Department agrees with the Auditor-Controller's recommendation. However, the Information System Bureau (ISB) evaluated and determined that in order to comply, PCMS will need to be redesigned or replaced. The current architecture of the application is not designed to handle detailed tracking of user activity. For future enhancements, the Probation Department will evaluate incorporating this feature into PCMS.

### AUDITOR-CONTROLLER RECOMMENDATION #3

Evaluate modifying the Probation Case Management System and Adult Probation System (APS) to restrict access to and/or mask Social Security Numbers.

**Probation Response:**

The Probation Department agrees with the Auditor-Controller's recommendation. However, ISB evaluated and determined that in order to comply, the PCMS and APS applications will need to be redesigned or replaced. The current architecture of the applications is not designed to carry out the recommended functionality. For future enhancements, the Probation Department will evaluate incorporating these features into PCMS and APS.

**AUDITOR-CONTROLLER RECOMMENDATION #4**

Remove the unnecessary Virtual Private Network (VPN) access noted in our review.

**Probation Response:**

The Probation Department agrees with and implemented the Auditor-Controller's recommendation. Unnecessary RSA SecurID VPN access has been deactivated and removed. A process is already in place to deactivate and remove unnecessary RSA hard tokens from use.

Estimated Task Completion Date: June 30, 2015

**AUDITOR-CONTROLLER RECOMMENDATION #5**

Remove the unauthorized higher-level Internet access or obtain the Director's approval as required, and ensure all Internet access is properly authorized.

**Probation Response:**

The Probation Department agrees with the Auditor-Controller's recommendation. Unauthorized higher-level Internet access has been removed, and a process is already in place to obtain Bureau Chief approval for higher-level Internet access. This process will be emphasized to the Client Support Section's System Registration Unit to ensure this process is being followed as documented.

A Probation Directive is being drafted to designate that a Bureau Chief's signature is required to permit higher-level Internet access.

**AUDITOR-CONTROLLER RECOMMENDATION #6**

Establish written policies and procedures to periodically review users' Virtual Private Network access, Internet access, Probation Case Management System access and Adult Probation System access.

**Probation Response:**

The Probation Department agrees with the Auditor-Controller's recommendation. Policy and procedures will be drafted to periodically review users' virtual Private Network, Internet, Probation Case Management System and Adult Probation System access.

Estimated Task Completion Date: June 30, 2016

**AUDITOR-CONTROLLER RECOMMENDATION #7**

Ensure all log-on identifications in the Probation Case Management System and the Probation Electronic Medical Records System are assigned to specific individuals.

**Probation Response:**

The Probation Department agrees with and implemented the Auditor-Controller's recommendation. A process is already in place to ensure that access is assigned to specific individuals. Regarding Generic User IDs:

- 8 generic PCMS IDs were deactivated as of May 3, 2015, except for two user IDs which are needed for PCMS to interface with the CBO application.
- 36 generic PEMRS IDs were deactivated as of January 20, 2015, except for five user accounts.

These accounts are system service accounts needed for PEMRS application processes and workflows to function correctly and automate data exchanges with other systems, such as PCMS.

**AUDITOR-CONTROLLER RECOMMENDATION #8**

Evaluate modifying the Adult Probation System to enforce password complexity requirements as defined in the County Fiscal Manual.

**Probation Response:**

The Probation Department agrees with the Auditor-Controller's recommendation. However, per the Internal Service Department's Security Applications Support Section, there is a technology limitation for APS to comply with the password policy. APS is a legacy mainframe system; Probation is working to replace APS and will include this finding as part of the application requirements for said replacement.

**AUDITOR-CONTROLLER RECOMMENDATION #9**

Remind employees to keep their user identification and password secured.

**Probation Response:**

The Probation Department agrees with the Auditor-Controller's recommendation. Directive 1345 and a Departmental email was sent to Probation employees reminding them to secure their user names and passwords.

We also agree that training is essential. All Probation employees will take IT/Data Security and HIPAA Awareness training at determined intervals by executive management. This will be implemented once the County Chief Information Office's IT/Data Security courses are offered online (Saba/LMS).

**AUDITOR-CONTROLLER RECOMMENDATION #10**

Investigate the 12 missing computing devices noted in our review.

**Probation Response:**

The Probation Department agrees with and implemented the Auditor-Controller's recommendation. Probation conducted another walkthrough after the audit and was able to identify all the servers; therefore, there are no missing servers. Probation investigated the 11 missing computing devices and the findings are as follows:

- Two (2) of the eleven (11) missing computing devices were salvaged laptops. The required paperwork was completed.
- One (1) of the laptops was stolen and the required paperwork was completed per Board of Supervisors (BOS) Policy 6.109.
- Three (3) laptops and five (5) desktops are missing. Probation will document the lost items per BOS Policy 6.109.

A new process is in place to ensure all Departmental equipment is accounted for.

**AUDITOR-CONTROLLER RECOMMENDATION #11**

Update inventory records when items are donated or stolen.

**Probation response:**

The Probation Department agrees with the Auditor-Controller's recommendation. The Bar Scan Inventory System is used to update Probation's hardware inventory as items are salvaged or stolen. Probation will monitor the process

closely to ensure that personnel update the inventory to accurately reflect equipment that is salvaged or stolen.

**AUDITOR-CONTROLLER RECOMMENDATION #12**

Report lost or stolen computers as required by the Board of Supervisors Policy 6.109.

**Probation response:**

The Probation Department agrees with the Auditor-Controller's recommendation. An email will be drafted and sent to all Probation employees for notification that all lost or stolen IT equipment must be reported to the Probation Help Desk to both open a ticket and inform the Departmental Information Security Officer (DISO).

The DISO will communicate with end users, supplemented by IT Security Training online, to reiterate the importance of reporting lost or stolen computers as mandated by BOS Policy 6.109. ISB management will ensure lost or stolen computer equipment is also reported per BOS Policy 6.109.

Estimated Task Completion Date: June 2016

**AUDITOR-CONTROLLER RECOMMENDATION #13 and #15**

Update its IT equipment inventory for the inaccuracies noted in our review. Inventory all IT equipment immediately, and annually thereafter, and update inventory records with the results of the physical counts.

**Probation Response:**

The Probation Department agrees with the Auditor-Controller's recommendation. Probation will conduct a physical inventory Department-wide to account for all computer devices, and then update the Bar Scan Inventory System in a timely manner to establish an accurate baseline. Thereafter, the Department is committed to conduct an annual physical inventory to verify the accuracy of the inventory.

Estimated Task Completion Date: June 2016

**AUDITOR-CONTROLLER RECOMMENDATION #14**

Ensure a County property tag is attached to all County IT resources as required by Board of Supervisors Policy 6.106

**Probation Response:**

The Probation Department agrees with the Auditor-Controller's recommendation. Designated Probation management will ensure all equipment has County property tags prior to receiving equipment at the warehouse for distribution to users as part of the annual inventory process.

**AUDITOR-CONTROLLER RECOMMENDATION #16**

Encrypt all portable computers as required by Board of Supervisors Policy 6.110.

**Probation Response:**

The Probation Department agrees with and implemented the Auditor-Controller's recommendation. All laptops have been encrypted since this audit was conducted. ISB management will continue to monitor and ensure all new laptops are encrypted prior to distribution.

**AUDITOR-CONTROLLER RECOMMENDATION #17**

Maintain detailed encryption records and periodically monitor encryption on the Department's portable computers.

**Probation Response:**

The Probation Department agrees with and implemented the Auditor-Controller's recommendation. Probation changed its laptop encryption program from PointSec to McAfee to standardize desktop and laptop encryption. McAfee requires devices to connect to the network to register prior to encryption configuration. All encrypted devices are recorded in the database and periodically monitored.

The Department is committed to periodically monitoring the encrypted devices against the database.

**AUDITOR-CONTROLLER RECOMMENDATION #18**

Ensure hard drives are sanitized before authorizing their disposal.

**Probation Response:**

The Probation Department agrees with the Auditor-Controller's recommendation. The hard drives designated for disposal are corrupted hard drives; therefore, sanitization through a software program is not possible. Probation staff drill multiple holes through these hard drives to ensure the devices are no longer accessible. For those hard drives that are reusable, Probation runs the

sanitization program prior to donating to other entities. Hard drives designated for sanitization are stored in a secure area with limited personnel access.

Probation has changed the process to sanitize the hard drives first, prior to signing off on the hard drive disposition form.

**AUDITOR-CONTROLLER RECOMMENDATION #19**

Ensure disposition forms identify the make, model and serial number of hard drives taken from Probation computers.

**Probation Response:**

The Probation Department agrees with and implemented the Auditor-Controller's recommendation. The disposition form has been updated to include the make, model, and serial number of hard drives taken from Probation computers.

**AUDITOR-CONTROLLER RECOMMENDATION #20**

Probation Department management ensure staff record capital IT equipment in the Electronic Countywide Accounting and Purchasing System within 30 days after invoice payment.

**Probation Response:**

The Probation Department agrees with the Auditor-Controller's recommendation. However, the ISB Administration Unit does not have access to eCAPS. Probation will work with its Procurement and Property & Supply Units to ensure the recommended process will be carried out in a timely manner.

**AUDITOR-CONTROLLER RECOMMENDATION #21**

Probation Department management ensure all IT resource users receive adequate IT Security Awareness Training.

**Probation Response:**

The Probation Department agrees with the Auditor-Controller's recommendation. All Probation employees will take IT/Data Security Awareness Training at determined intervals by executive management. This will be implemented once the County Chief Information Office's IT/Data Security courses are offered online (Saba/LMS).

**AUDITOR-CONTROLLER RECOMMENDATION #22**

Probation Department management work with the Auditor-Controller's Office of County Investigations to obtain Internet activity details, including the individuals who visited the sites, and investigate the Internet storage activity noted in our review.

**Probation Response:**

The Probation Department agrees with the Auditor-Controller's recommendation. Probation will work with the Auditor-Controller and the Office of Investigation (OCI) to identify and implement an efficient process for obtaining internet activity details, including the individuals who visited the sites, and investigate the internet storage activity noted in the Auditor-Controller's review.

**AUDITOR-CONTROLLER RECOMMENDATION #23**

Probation Department management perform risk assessments on all critical systems by properly completing the Internal Control Certification Program.

**Probation Response:**

The Probation Department agrees with the Auditor-Controller's recommendation. Probation will complete the Internal Control Certification Program (ICCP) in an accurate and timely manner as requested.

The Probation Department's ICCP for FY 14-15 was submitted by Fiscal Services to Auditor-Controller on May 19, 2015.