STATE OF FLORIDA
DEPARTMENT OF JUVENILE JUSTICE

INTEROFFICE MEMORANDUM

DATE: January 15, 2016

TO: Christina K. Daly, Secretary

FROM: Robert A. Munson, Inspector General

SUBJECT: Final Report - #A-1415DJJ-003, *Audit of Mobile Devices Usage*

Please find enclosed a copy of our final audit report, *Audit of Mobile Devices Usage*. The Bureau of Internal Audit will conduct a follow-up review to determine the status of corrective actions taken to address the reported findings.

We would like to thank Administration for the support extended to our audit staff in the audit process. If you have any questions, please feel free to contact Michael Yu, Audit Director, at 850-717-2468.

RM/MY/kn

Attachment

Cc: Tim Niermann, Deputy Secretary
Fred Schuknecht, Chief of Staff
Vickie J. Harris, Director, Administration
Melinda M. Miguel, Chief Inspector General, Executive Office of the Governor
David W. Martin, CPA, Auditor General
Kathy DuBose, Director, Legislative Auditing Committee

Audit of Mobile Devices Usage
Report Number *A-1415DJJ-003*
January 15, 2016

By

The Office of the Inspector General
Bureau of Internal Audit

Robert A. Munson
Inspector General

Michael Yu, CIA, CIG
Director of Auditing

Kelly Neel
Auditor

Christina K. Daly, Secretary

Office of Inspector General
Bureau of Internal Audit
Audit of Mobile Devices Usage
Audit No. *A-1415DJJ-003*

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Department of Juvenile Justice (Department), Office of the Inspector General, Bureau of Internal Audit has performed an Audit of Mobile Devices Usage. The audit objectives were to provide management with an assessment of mobile devices security policies and procedures and their operational effectiveness; identify internal control deficiencies related to mobile device usage that could affect the Department; and identify information security control concerns that could affect the confidentiality, integrity, and availability of Department data due to weaknesses in mobile device controls.

The audit disclosed that, in general, the Department complied with applicable Florida Statutes, Florida Administrative Code, and Department policies and procedures. Effective controls were in place to mitigate the security risks posed from the use of mobile computing and mobile storage devices. However, we noted areas for improvement pertaining to the following:

- A number of employees not completing mandatory annual Information Security Awareness Training;
- Procedures related to Encrypted Mobile Device Acknowledgement Forms and Mobile Device Property Custody Logs not being followed;
- Procedures not being followed to ensure proper documentation was completed to verify the sanitization of all data storage media;
- Service fees being paid for Department issued cell phones with no usage;
- Cell phone security controls needing enhancement; and
- Weak controls for cell phone assignment justification and approval.

We recommend the Department implement processes to ensure staff are completing all mandatory annual training; and to ensure procedures for the Mobile Device Property Custody Log, Encrypted Mobile Device Acknowledgment Form, and Data Storage Media Sanitization/Destruction Form are followed. We also recommend the Department assign an employee a cell phone on an essential basis and analyze in depth cell phone usage to remove service from phones with little or no usage. We recommend procedures be enhanced for justification and approval for assigning a cell phone. We urge stronger smartphone security features be applied for greater protection of IT resources.

Audit of Mobile Devices Usage

Audit # A-1415DJJ-003

INTRODUCTION

The Office of the Inspector General conducted an audit of the Department's Mobile Devices Usage for the period July 1, 2013 through June 30, 2015, and related activities through the end of fieldwork. The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*, published by the Institute of Internal Auditors.

Background

Mobile device is a universal term describing both mobile computing and mobile storage devices. A mobile computing device is a laptop, notebook, tablet, personal digital assistant (PDA), smartphone, or other portable device that can process data. A mobile storage device is portable data storage media including external hard drive, memory card, thumb drive, floppy disk, recordable compact disc, recordable digital video disc, portable music player such as an iPod, media player, or tape drive that may be easily attached and detached from computing devices. Mobile devices used in the Department must be department owned or managed.

Information Security requires protecting employee and youth information and Department owned information technology (IT) resources (mobile devices) from unauthorized use, disclosure, alteration, or destruction. The Department's Information Security Handbook was developed based on Section 282.318 Florida Statues, 71A-1 Florida Administrative Code, National Institute of Standards and Technology (NIST) SP800 series, and International Standards Organization (ISO) 17799. Department employees shall receive Information Security Awareness training, which encompasses Mobile Computing/Storage Device Security, within 30 days of their employment start date and prior to accessing confidential information. Any Department employee who has a network account is required to complete an Information Security Awareness training program at least annually.

Mobile device security is centrally managed through Active Directory (AD) for laptops and tablets. Active Directory is a directory service that Microsoft developed for Windows domain networks, which authenticates and authorizes all users and computers assigning and enforcing security policies and installing or updating software. MobileIron manages iOS and Android devices. The MobileIron Management solution is a mobile security platform that secures data-at-rest on mobile devices, in applications, and in cloud storage, as well as data-in-motion as it moves between corporate networks and devices. The BlackBerry Exchange Server (BES) manages BlackBerry smart phones.

BES handles unique messaging elements such as attachments, device status, messaging, policies, and synchronization. Services can be installed and managed individually, allowing the Department to deploy the level of BlackBerry support and control that best suits Department requirements. The Department does not manage cell phones that do not store or transmit data.

The Department currently uses three cellular service providers for cell phone purchases and service. In FY 2014-2015, the Department paid $538,821.22 to cellular service providers.

Objective, Scope, and Methodology

The audit objectives were to provide management with an assessment of mobile device security policies and procedures and their operational effectiveness; identify internal control deficiencies related to mobile device usage that could affect the Department; and identify information security control concerns that could affect the confidentiality, integrity, and availability of Department data due to weaknesses in mobile device controls. The scope of the audit was the Department's mobile devices usage from July 1, 2013 through June 30, 2015, and related activities through the end of fieldwork.

To achieve the audit objective, we:

- reviewed applicable statutes and rules;
- reviewed Department policies and procedures;
- reviewed the Information Resource Security Handbook;
- reviewed mobile security best practices;
- interviewed the Bureau of Management Information Systems (MIS) management and staff;
- interviewed Department employees;
- examined cell phone usage; and
- conducted other activities deemed necessary.

Statistical sampling was used in order to infer the conclusions of test work performed on a sample to the population from which it was drawn and to obtain estimates of sampling error involved. When appropriate, judgmental sampling was used to improve the overall efficiency of the audit.

Because of inherent limitations associated with sample selection, errors or irregularities could have occurred but were not detected. As such, projection of the auditor's conclusions based on the selected sample may be different from that reached if all mobile devices were subject to the audit procedure.

RESULT OF AUDIT

The audit revealed policies and procedures exist for mobile devices. Mobile device policies, procedures, and internal control processes were generally in compliance with applicable laws and regulations. However, we noted areas for improvement pertaining to the following:

Details of Findings and Recommendations

Finding 1: Some department employees did not complete mandatory annual Information Security Awareness training in 2014

Florida Administrative Code 71A-1.008 Awareness and Training states, at minimum, agency workers shall receive annual security awareness training. According to the Department policy and procedure FDJJ-1215, Information Security Awareness (ISA) Training, ISA training will include such topics as protection of mobile devices, the Executive Leadership Team is responsible for ensuring staff complete ISA training on an annual basis, and Department employees with a network account are required to complete an ISA training program at least annually. Policies and procedures are in place for mobile device training through the Information Security Awareness Training required for new hires and annually for all employees.

We reviewed the Required Hours Remaining Report in the SkillPro on-line training system for employees under Executive Direction. For employees with less than 7 hours (the mandatory courses' credit hours) completed, we reviewed their course history. Our review indicated that 30 employees under Executive Direction had not completed Information Security Awareness training through SkillPro in 2014.

Incomplete annual information security awareness training could result in employees unaware of the latest security requirements thus opening the department up to security threats.

We recommend the Department implement processes to ensure that staff are completing all mandatory training.

Finding 2: Procedures were not being followed for completing the Encrypted Mobile Device Acknowledgement Form and tracking Department owned mobile devices with the Mobile Device Property Custody Log

According to FDJJ 1230P, Mobile Devices Procedures, supervisors are responsible for ensuring the Encrypted Mobile Device Acknowledgment Form is completed and signed by the recipient of mobile computing and/or mobile storage devices, and the original form is submitted to the Office of Personnel with a copy to the Information Security

Manager (ISM). Employees and supervisors should retain copies of the form for their records. Supervisors are responsible for tracking agency owned mobile computing devices with the Mobile Device Property Custody Log. Property Custodians/General Service Liaisons are responsible for maintaining the Mobile Device Property Custody Log to record the identity of temporary users of unassigned (shared) mobile devices, including laptops, and for retaining Mobile Device Property Custody Logs for two-year retention periods and ensuring their availability for auditing purposes.

During the audit process, we inquired of 14 areas within Department Headquarters to assess if the Encrypted Mobile Device Acknowledgment Form and Mobile Device Property Custody Log were used to record and track the mobile devices assignment. Among the 14 areas, only one area was aware of the Encrypted Mobile Device Acknowledgment Form and Mobile Device Property Custody Log. Staff in this area provided documentation of the Mobile Device Property Custody Logs but indicated that its personnel did not turn in all Encrypted Mobile Device Acknowledgment Forms.

When interviewed, the Office of Personnel staff stated that they were not aware the Encrypted Mobile Device Acknowledgment Form existed.

Without using the Encrypted Mobile Device Acknowledgment Form and Mobile Device Property Custody Log as required by Department policy, the Department would not be able to record employee acknowledgement of mobile device encryption requirements and to track the mobile devices assigned to employees. This could result in Department employees unaware of mobile device encryption requirements and consequently opening the Department up to security threats, and the Department losing control of the mobile devices assigned to employees.

We recommend the Department ensure procedures are followed to track mobile devices within each area of the Department through the Mobile Device Property Custody Log and employees are aware of encryption requirements by signing the Encrypted Mobile Device Acknowledgment Form.

Finding 3: Procedures were not being followed to ensure proper documentation was completed in order to verify the sanitization of all data storage media

Mobile devices procedures state that applicable MIS staff shall inspect all office machines with data storage capability during the disposition and disposal process to ensure that all data storage media (hard drives, flash drives, USB devices, optical disks, memory, etc.) is removed from the device and securely sanitized before the device/media leaves Department facilities. MIS staff shall complete the Data Storage Media Sanitization/Destruction Form (1260-1) to document and verify the sanitization of all data storage media. If the device is being surplused, a Surplus Certification of State Property (Form 25) must also be completed and attached to form 1260-1.

During our audit process, MIS was unable to provide documentation of form 1260-1. MIS provided its staff a PowerPoint training on Storage Media Disposal in July 2015 in response to the Auditor General's (AG) Operational Audit 2014-015 that found neither Form 1260-1 nor Form 25 had been completed for 6 of 25 records examined. Form 1260-1 was revised in September 2015 due to the AG audit.

Without following the procedures for the documentation and verification of sanitization/destruction of media, the Department would not be able to verify the sanitization of all data storage media.

We recommend MIS ensure its employees follow procedures to document and verify the sanitization of all data storage media.

Finding 4: A number of Department issued cell phones were found to have little or no usage

Our review indicated that in August 2015, 1804 out of 3265.5 Department positions had Department issued cell phones (55%). Our examination of cell phone usage and charges from June 2015 through August 2015 revealed that over the three-month period, a cost of $11,575.37 was for cell phones with no cellular minute usage and no data usage. An estimated annual cost would be $46,000 for cell phones with no usage. In August 2015, there were 329 out of 1804 Department issued cell phones (18%) that had no usage.

Our examination also revealed that, for the same three-month period, a cost of $20,032.96 was for cell phones that used less than 30 cellular minutes and less than 0.5 gigabytes (GB) of data monthly. An estimated annual cost would be $80,000 for cell phones with monthly usage less than 30 minutes and less than 0.5 GB of data. In August 2015, 295 out of 1804 department issued cell phones (16%) used less than 30 cellular minutes and less than 0.5 GB data usage.

We recommend the Department analyze in depth cell phone usage and consider updating the service plans according to use, suspending service when an employee is out for extended periods, and removing service from phones with little use for a more cost effective approach.

Finding 5: Smartphone security controls need enhancement

Our review indicated that the Department has policy and practice in place to ensure that only Department approved software are installed on Department owned or Department managed mobile computing devices. MIS centrally manages applications through security policies that limit or block third party software for mobile devices. However, this practice was not applied to the Department's BlackBerry devices. Our review indicated that BlackBerry devices allow installation of third party software without Department

approval. In addition, our review revealed that the BlackBerry devices require only a four-digit pin, which does not provide strong security control.

We recommend the Department strengthen security controls over BlackBerry devices to block the ability to install third party software and to increase security by using stronger passwords.

Finding 6: Policy and procedures are weak for cell phone assignment justification and approval

Our review indicated policy and procedures were not in place for formally documenting justification and approval for assigning an employee a Department issued cell phone. Currently the Information Resource Request (IRR) form requires employees to explain the need for a smart phone through the *Business Requirements and Benefits Statement* section. An ELT Member, Regional Director, or Designee signature is required on the IRR, but this form is being used for technical approval from MIS for smart phones only, not justification and approval for acquiring any Department issued cell phone.

We recommend the Department develop guidelines for justification and implement a formal approval process for issuing a Department cell phone.

APPENDIX:

MANAGEMENT RESPONSE

Department of Juvenile Justice
Audit of Mobile Devices Usage, Audit No. A-1415DJJ-003 - Response

Finding 1: Some department employees did not complete mandatory annual Information Security Awareness training in 2014

1. *Florida Administrative Code 71A-1.008 Awareness and Training states, at minimum, agency workers shall receive annual security awareness training. According to the Department policy and procedure FDJJ-1215, Information Security Awareness (ISA) Training, ISA training will include such topics as protection of mobile devices, the Executive Leadership Team is responsible for ensuring staff complete ISA training on an annual basis, and Department employees with a network account are required to complete an ISA training program at least annually. Policies and procedures are in place for mobile device training through the Information Security Awareness Training required for new hires and annually for all employees.*

   We reviewed the Required Hours Remaining Report in the SkillPro on-line training system for employees under Executive Direction. For employees with less than 7 hours (the mandatory courses' credit hours) completed, we reviewed their course history. Our review indicated that 30 employees under Executive Direction had not completed Information Security Awareness training through SkillPro in 2014.

   Incomplete annual information security awareness training could result in employees unaware of the latest security requirements thus opening the department up to security threats.

   We recommend the Department implement processes to ensure that staff are completing all mandatory training.

   Response:
   We concur. We will implement a process to produce a report including each program area and providers annually on October 1st. This report will be tailored to give MIS insight as to which DJJ employees and providers have yet to complete the training. With information from the report MIS will generate email messages to all employees and will ask contract managers to notify providers as a reminder to complete the annual requirement for security awareness training. After the initial notification, MIS will follow up at 30 and 60 day intervals in a continued effort to inform staff that training should be completed by December 31st. The MIS report will reflect the staff that have not completed training and Assistant Secretaries of each program area will be notified so they can follow up in their program area.

   Action Item:
   On-going. Will need to design a report which meets the requirements listed above.

Department of Juvenile Justice
Audit of Mobile Devices Usage, Audit No. A-1415DJJ-003 - Response

Finding 2: Procedures were not being followed for completing the Encrypted Mobile Device Acknowledgement Form and tracking Department owned mobile devices with the Mobile Device Property Custody Log

2. *According to FDJJ 1230P, Mobile Devices Procedures, supervisors are responsible for ensuring the Encrypted Mobile Device Acknowledgment Form is completed and signed by the recipient of mobile computing and/or mobile storage devices, and the original form is submitted to the Office of Personnel with a copy to the Information Security Manager (ISM). Employees and supervisors should retain copies of the form for their records. Supervisors are responsible for tracking agency owned mobile computing devices with the Mobile Device Property Custody Log. Property Custodians/General Service Liaisons are responsible for maintaining the Mobile Device Property Custody Log to record the identity of temporary users of unassigned (shared) mobile devices, including laptops, and for retaining Mobile Device Property Custody Logs for two-year retention periods and ensuring their availability for auditing purposes.*

   During the audit process, we inquired of 14 areas within Department Headquarters to assess if the Encrypted Mobile Device Acknowledgment Form and Mobile Device Property Custody Log were used to record and track the mobile devices assignment. Among the 14 areas, only one area was aware of the Encrypted Mobile Device Acknowledgment Form and Mobile Device Property Custody Log. Staff in this area provided documentation of the Mobile Device Property Custody Logs but indicated that its personnel did not turn in all Encrypted Mobile Device Acknowledgment Forms.

   When interviewed, the Office of Personnel staff stated that they were not aware the Encrypted Mobile Device Acknowledgment Form existed.

   Without using the Encrypted Mobile Device Acknowledgment Form and Mobile Device Property Custody Log as required by Department policy, the Department would not be able to record employee acknowledgement of mobile device encryption requirements and to track the mobile devices assigned to employees. This could result in Department employees unaware of mobile device encryption requirements and consequently opening the Department up to security threats, and the Department losing control of the mobile devices assigned to employees.

   We recommend the Department ensure procedures are followed to track mobile devices within each area of the Department through the Mobile Device Property Custody Log and employees are aware of encryption requirements by signing the Encrypted Mobile Device Acknowledgment Form. JJIS access privileges. Similar instances were noted in our report No. 2014-015.

Department of Juvenile Justice
Audit of Mobile Devices Usage, Audit No. A-1415DJJ-003 - Response

Response:
We concur. The Department has made significant progress in aggressively applying encryption and managed device functionality to USB drives, smartphones, tablets, and laptops. By default, every USB drive that has data written to it forces the device to be encrypted. MIS encrypts all Department laptop computers, and MobileIron Mobile Device Management manages the mobile security policies on smartphones and iPad tablets. The forms referenced in the finding are no longer required due to the aforementioned default configuration for encryption and mobile device management. The forms will be removed as an attachment to the policy, along with updates to policy 1230.

Action Item:
Update DJJ Policy and Procedure 1230.

Department of Juvenile Justice
Audit of Mobile Devices Usage, Audit No. A-1415DJJ-003 - Response

Finding 3: Procedures were not being followed to ensure proper documentation was completed in order to verify the sanitization of all data storage media

3. *Mobile devices procedures state that applicable MIS staff shall inspect all office machines with data storage capability during the disposition and disposal process to ensure that all data storage media (hard drives, flash drives, USB devices, optical disks, memory, etc.) is removed from the device and securely sanitized before the device/media leaves Department facilities. MIS staff shall complete the Data Storage Media Sanitization/Destruction Form (1260-1) to document and verify the sanitization of all data storage media. If the device is being surplused, a Surplus Certification of State Property (Form 25) must also be completed and attached to form 1260-1.*

   During our audit process, MIS was unable to provide documentation of form 1260-1. MIS provided its staff a PowerPoint training on Storage Media Disposal in July 2015 in response to the Auditor General's (AG) Operational Audit 2014-015 that found neither Form 1260-1 nor Form 25 had been completed for 6 of 25 records examined. Form 1260-1 was revised in September 2015 due to the AG audit.

   Without following the procedures for the documentation and verification of sanitization/destruction of media, the Department would not be able to verify the sanitization of all data storage media.

   We recommend MIS ensure its employees follow procedures to document and verify the sanitization of all data storage media.

   Response:
   We concur. Although this was addressed during the time of the audit, MIS will follow-up with Regional MIS Managers and staff whose duties include sanitizing and surplusing equipment to ensure compliance. The ISM will review related training to verify that it covers applicable policy. The ISM will offer repeated training opportunities to applicable staff.

   Action Item:
   The ISM will conduct bi-annual training on media sanitization requirements in order to refresh applicable staff on policy and procedure.

Department of Juvenile Justice
Audit of Mobile Devices Usage, Audit No. A-1415DJJ-003 - Response

Finding 4: A number of Department issued cell phones were found to have little or no usage

4. *Our review indicated that in August 2015, 1804 out of 3265.5 Department positions had Department issued cell phones (55%). Our examination of cell phone usage and charges from June 2015 through August 2015 revealed that over the three-month period, a cost of $11,575.37 was for cell phones with no cellular minute usage and no data usage. An estimated annual cost would be $46,000 for cell phones with no usage. In August 2015, there were 329 out of 1804 Department issued cell phones (18%) that had no usage.*

   Our examination also revealed that, for the same three-month period, a cost of $20,032.96 was for cell phones that used less than 30 cellular minutes and less than 0.5 gigabytes (GB) of data monthly. An estimated annual cost would be $80,000 for cell phones with monthly usage less than 30 minutes and less than 0.5 GB of data. In August 2015, 295 out of 1804 department issued cell phones (16%) used less than 30 cellular minutes and less than 0.5 GB data usage.

   We recommend the Department analyze in depth cell phone usage and consider updating the service plans according to use, suspending service when an employee is out for extended periods, and removing service from phones with little use for a more cost effective approach.

   Response:
   We concur. MIS will work with General Services to recommend specific department policy changes which will define periodic monitoring of cellular phone/smartphone usage. MIS will also conduct periodic monitoring of aircards/mifi/cellular tablet data usage with a report to leadership on little or no usage. Data learned from the monitoring process will be used to ensure that users do in fact require such a device and to promote monetary efficiency.

   Action Item:
   Update existing policy to describe process for periodic reviews of cell phones/smartphone usage. MIS will work with General Services on maintaining efficiency of phone usage.

Department of Juvenile Justice
Audit of Mobile Devices Usage, Audit No. A-1415DJJ-003 - Response

Finding 5: Smartphone security controls need enhancement

5. *Our review indicated that the Department has policy and practice in place to ensure that only Department approved software are installed on Department owned or Department managed mobile computing devices. MIS centrally manages applications through security policies that limit or block third party software for mobile devices. However, this practice was not applied to the Department's BlackBerry devices. Our review indicated that BlackBerry devices allow installation of third party software without Department approval. In addition, our review revealed that the BlackBerry devices require only a four-digit pin, which does not provide strong security control.*

   We recommend the Department strengthen security controls over BlackBerry devices to block the ability to install third party software and to increase security by using stronger passwords.

   Response:
   We concur. Prior to migrating to Office 365, Blackberry devices were managed by the Blackberry Enterprise Server management platform. As a requirement of migrating to Office 365, the Blackberry devices have policy enforcement and are managed through the Microsoft Exchange Online portal as part of the Office 365 offering. The capability of blocking downloads through the management features of the MDM is not available in the current offering. MIS is working with the Phone Administrator in General Services to try and block this at the individual carrier level. Also, the Department is quickly migrating away from Blackberry devices to standardize on Apple iPhones, which will be managed with MobileIron MDM.

   Action Item:
   This finding will be mitigated through attrition as Blackberry devices are replaced with iPhones, which will be managed by the MobileIron MDM. General Services has provided a report which indicates 175 Blackberry devices in use. These Blackberry devices will be replaced with iPhones by the end of the fiscal year.

Department of Juvenile Justice
Audit of Mobile Devices Usage, Audit No. A-1415DJJ-003 - Response

Finding 6: Policy and procedures are weak for cell phone assignment justification and approval

6. *Our review indicated policy and procedures were not in place for formally documenting justification and approval for assigning an employee a Department issued cell phone. Currently the Information Resource Request (IRR) form requires employees to explain the need for a smart phone through the Business Requirements and Benefits Statement section. An ELT Member, Regional Director, or Designee signature is required on the IRR, but this form is being used for technical approval from MIS for smart phones only, not justification and approval for acquiring any Department issued cell phone.*

   We recommend the Department develop guidelines for justification and implement a formal approval process for issuing a Department cell phone.

   Response:
   We concur. MIS will modify the existing IRR policy to state the approval process required for cell phone, smartphone, tablets, air cards, or any device with monthly cellular service required for usage. Such devices purchased for DJJ-HQ staff will have approval from a Bureau Chief or higher. DJJ locations outside of HQ will require Regional Director or higher approval.

   Furthermore, the instructions for IRR submittal will state that supporting documentation in the form of an e-mail message listing the approvals must be attached to the automated IRR before being approved.

   Action Item:
   Modify existing policy and instructions for IRR submittal. MIS will be responsible for technical requirements related to smartphone/device justification.

Vickie Jo Hains
Director of Administration
Jan 14, 2016