AUDIT OF THE EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS' LAPTOP COMPUTER AND ELECTRONIC TABLET ENCRYPTION PROGRAM AND PRACTICES

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 14-15
March 2014

AUDIT OF THE EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS' LAPTOP COMPUTER AND ELECTRONIC TABLET ENCRYPTION PROGRAM AND PRACTICES

EXECUTIVE SUMMARY

Ensuring the proper encryption of laptop computers (laptops) and electronic tablets used by United States Attorney's Office (USAO) employees, contractors, and subcontractors is essential to the security of the information that is processed on those machines. While each U.S. Attorney is the chief federal law enforcement officer for their jurisdiction, it is the Executive Office for the United States Attorneys (EOUSA) that provides general executive assistance, direction, policy development, and management oversight of encryption policies and practices.

The Office of the Inspector General (OIG) performed this audit to determine whether EOUSA complies with Department of Justice (DOJ) policy regarding: (1) the use of whole disk encryption on employee, contractor, and subcontractor laptops processing sensitive and classified information; and (2) laptop encryption procedures for contractors and subcontractors. In the process, we also included electronic tablets because EOUSA received a waiver of certain encryption requirements from the Department to deploy this type of electronic tablet in a pilot program.[1]

According to EOUSA, it had 10,790 laptops and 1,044 electronic tablets in use during our audit period. We found that 111 of the 120 EOUSA-owned laptops that we tested that were used for unclassified processing were encrypted and 6 were not encrypted; we could not determine the encryption status for the remaining 3 laptops. The six unencrypted laptops were used for special purposes such as jury use, use by visiting EOUSA employees, and the production of employee identification cards. However, the six unencrypted laptops were not labeled to identify their special use, nor were there policies that explicitly limited their use.

[1] The electronic tablet waiver allows a manufacturer's electronic tablets to be used without complying with National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 "Security Requirements for Cryptographic Modules." Modules validated as conforming to FIPS 140-2 are accepted by the U.S. Federal Agencies for the protection of sensitive information. This waiver allows time for the manufacturer to complete the required FIPS validation with NIST.

We also reviewed a sample from three encryption monitoring scans completed by EOUSA's Information Systems Security staff as part of its encryption monitoring program. These scans are used to identify unencrypted laptops that should be encrypted. The first two scans identified approximately 60 unencrypted laptops that were resolved by EOUSA encrypting these laptops in a timely manner. The third scan, however, identified eight unencrypted laptops, the encryption status of which had gone unaddressed for over a year.

Our audit noted other issues regarding the management and monitoring of the devices we tested. For instance, we found that EOUSA's official equipment inventory was incomplete, contained inaccurate data entries, and was subject to delays in updating information. We further determined that EOUSA did not sufficiently track and monitor laptops used for classified processing, causing an increased risk of classified information loss. We also tested two classified laptops and three classified hard drives for encryption while on our site visits. We determined that one of the laptops was encrypted, but one laptop and one hard drive were not encrypted and the remaining two hard drives were inoperable.

We evaluated EOUSA's use of electronic tablets as part of its pilot program and found that EOUSA did not fully comply with JMD's electronic tablet waiver requirements. Further, EOUSA does not adequately monitor the use of the electronic tablets and does not have policies sufficient to minimize security risks.

In addition, we reviewed EOUSA's procedures for contractor use of DOJ data, specifically those of expert witnesses and litigation consultants, and found that the use of this data was not in compliance with the DOJ Procurement Guidance Documentation 08-04, which requires that external contractors' laptops be encrypted to process DOJ data. The Justice Management Division had previously granted a waiver to EOUSA from this encryption requirement but the waiver had expired in 2011, and no formal, written waiver was issued in its place. However, EOUSA continued to allow its contractors to process the DOJ data on their unencrypted equipment. When JMD issued a new waiver to EOUSA in February 2013, the waiver included a new requirement that all data transmitted to contractors must be encrypted, but EOUSA did not convey this new instruction to the USAOs. We also found that the oversight of these contractors and the contracting process was inconsistent among USAOs, and that the use of DOJ data in general was not sufficiently monitored by the USAOs we visited, thereby increasing the risk of DOJ data loss.

Our audit resulted in 13 recommendations to assist EOUSA in improving safeguards of DOJ data on laptops and electronic tablets, and in improving its management oversight to ensure compliance with DOJ policies.

AUDIT OF THE EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS' LAPTOP COMPUTER AND ELECTRONIC TABLET ENCRYPTION PROGRAM AND PRACTICES

TABLE OF CONTENTS

INTRODUCTION 1

Laptop Encryption Policy Within DOJ 1

Laptop Encryption Policy for Contractors 1

EOUSA's Use of Contractors for Litigation Support 4

OIG Audit Approach 5

Previous Audits on Laptop Encryption Programs and Practices 5

FINDINGS AND RECOMMENDATIONS 8

EOUSA'S EFFORTS TO ENSURE SAFEGUARDS OVER DOJ DATA ON LAPTOP COMPUTERS AND ELECTRONIC TABLETS NEED IMPROVEMENT 8

Laptop Computers and Electronic Tablets Owned by EOUSA 9

Encryption Requirements and Encryption Process 9

Laptop Encryption Testing 10

Encryption Installation Records Not Maintained 12

Laptop and Electronic Tablet Inventory 15

EOUSA Electronic Tablet Pilot Program 18

EOUSA Compliance with Electronic Tablet Waiver Conditions 19

Electronic Tablet Policies and Procedures 21

Electronic Tablet Password Testing 22

Electronic Tablet Risks and Observations 22

Laptop Computers Owned by Contractors and Subcontractors 23

OBD-47 Contractor Compliance with PGD 08-04 23

USAO, Expert Witness, and Litigation Consultant Compliance with Data Security Requirements 25

Conclusion 28

Recommendations 28

STATEMENT ON INTERNAL CONTROLS 30

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS..... 31

APPENDIX I: OBJECTIVES, SCOPE, AND METHODOLOGY 32

APPENDIX II: DOJ PROCUREMENT GUIDANCE DOCUMENT 08-04, CONTRACTOR-OWNED LAPTOP SECURITY REQUIREMENTS 35

APPENDIX III: DOJ'S CLARIFICATIONS ON THE DATA SECURITY IMPLEMENTATION OF THE PGD 08-04 PROCUREMENT GUIDE 37

APPENDIX IV: EOUSA'S RESPONSE..... 39

APPENDIX V: OFFICE OF INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO RESOLVE THE REPORT.....45

AUDIT OF THE EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS' LAPTOP COMPUTER AND ELECTRONIC TABLET ENCRYPTION PROGRAM AND PRACTICES

INTRODUCTION

Encrypting laptops used by EOUSA and United States Attorney's Office (USAO) employees, contractors, and subcontractors is essential to the security of the information that is processed on those machines. The Executive Office for United States Attorneys (EOUSA) Information Systems Security Staff is responsible for ensuring that EOUSA's IT systems, including those used by the USAOs, comply with all applicable laws and regulations; assisting the USAOs with information systems security needs; protecting USAO and EOUSA Information Systems data from unauthorized disclosure; and managing other IT security responsibilities, such as cyber incident response.

Laptop Encryption Policy Within DOJ

DOJ Order 2640.2F, issued in November 2008, established the laptop and data media encryption policy for the Department.[2] Chapter 2, section 12 states that "information on mobile computers/devices (for example, notebook computers, personal digital assistants) and removable media shall be encrypted using FIPS 140-2 validated or NSA [National Security Agency] approved encryption mechanism."[3]

Laptop Encryption Policy for Contractors

Contractors and subcontractors who use equipment accessing DOJ systems or containing DOJ data are subject to DOJ Procurement Guidance Document (PGD) 08-04, *Security of Systems and Data, Including Personally*

[2] The DOJ Order 2640.2F establishes uniform policy, responsibilities and authorities for protection of Information Technology systems that store, process or transmit the Department information.

[3] The National Institute of Standards and Technology (NIST) issued Federal Information Processing Standards (FIPS) 140-2 "Security Requirements for Cryptographic Modules." Modules validated as conforming to FIPS 140-2 are accepted by the U.S. Federal Agencies for the protection of sensitive information.

Identifiable Information. PGD 08-04, issued in March 2008, contains a security clause governing the use of laptops by contractors that must be included in all current and future contracts where a contractor handles "data that originated within the Department, data that the contractor manages or acquires for the Department, and/or data that is acquired in order to perform the contract and concerns Department programs or personnel." In addition, the contractor must comply with all security requirements applicable to Department systems, such as DOJ Order 2640.2F. The use of contractor-owned laptops or other media storage devices to process or store data covered by the clause is prohibited until the contractor provides a letter to the contracting officer certifying that the nine specific requirements related to the security of laptops and other media storage devices are met. See Appendix II for a complete listing of these requirements.

PGD 08-04 also required that all Department contracts that were already in existence as of the March 2008 issuance of the guidance be modified to include the applicable security clause within 60 days. After 60 days, laptops or devices not covered by certification letters could not be used on DOJ contracts. According to PGD 08-04, "a request for a waiver from the requirement to include these clauses, or any deviations from the language of these clauses (except those that are more stringent), must be made in writing to the DOJ Senior Procurement Executive." It further states that "permission for a deviation or waiver will only be granted in unusual circumstances."

A memorandum issued by the Justice Management Division (JMD) in June 2008 updated the above requirements and allowed a 60-day extension to implement PGD 08-04.[4] The June 2008 memorandum reiterated the protections set forth in the earlier March memorandum.

The June memorandum also referenced OMB M-07-16 and OMB M-06-16, which include the requirement to report PII-related incidents to US-CERT and requires that all data on mobile devices be encrypted unless the data is determined, in writing by the designated official, to be

[4] Senior Procurement Executive, Justice Management Division, memorandum for bureau procurement chiefs and executive officers, Implementation Guidance Regarding Security of Systems and Data, Including Personally Identifiable Information, June 17, 2008.

non-sensitive.[5] [6] The June 2008 memorandum also provided clarifications regarding: (1) encryption-related requirements; (2) certification of data extracts; (3) publicly available or previously released data; (4) the identification of compensating controls and plans of action and milestones; and (5) micro purchases.[7] [8] [9] See Appendix III for a complete listing of the clarifications.

Components can request a waiver from JMD for any of the June 2008 memorandum requirements that it has not or cannot meet. Such requests should include the following information:

1. The contract or contracts for which the waiver is being sought.

2. The type and amount of data involved in the contract or contracts, including the sensitivity of the data and whether PII is involved.

3. Which security requirements cannot be met and the reason(s) the contract or contracts cannot comply with the security requirements.

---

[5] OMB M-07-16: Deputy Director for Management, Office of Management and Budget, memorandum to heads of executive departments and agencies, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007. OMB M-06-16: Deputy Director for Management, Office of Management and Budget, memorandum to heads of departments and agencies, Protection of Sensitive Agency Information, June 23, 2006.

[6] United States Computer Emergency Readiness Team (US-CERT) is the Federal security incident handling center located within the Department of Homeland Security. It was established with the purpose of coordinating the response to security threats from the Internet for the nation.

[7] Compensating controls are controls intended to supplement/enhance ineffective or weak controls to reduce the associated risks.

[8] Plan of Action and Milestones is a document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

[9] According to the JMD Purchase Card Manual, in most cases the micro purchase threshold is set at $3,000 for goods and services.

4. A statement of any factors that mitigate the risk of harm from the contractors not meeting the security requirements, and whether there is an alternative solution to DOJ security requirements.

5. A statement of the time frame for which the waiver is needed, and any steps or long-term solutions planned.

6. If lack of resources is a reason for the need for a waiver, a brief statement of the component's funding needs to address contractor data security requirements.

7. A statement that the component official making the request accepts the risk of harm that could result from the contractor not meeting the security requirements, given the need for the contract or contracts.

EOUSA's Use of Contractors for Litigation Support

EOUSA uses several types of contractors for litigation support, including paralegals and expert witnesses. Contractors for litigation support, referred to as Mega-3 contractors, often work onsite in EOUSA and USAO offices using DOJ equipment, whereas expert witnesses, known as OBD-47 contractors, tend to work from offsite locations and use their personal computer equipment. All contractors are expected to follow PGD 08-04 or a current data security waiver for PGD 08-04.

At the USAO sites we visited, there were only two Mega-3 contractors in use and they both worked onsite. EOUSA's Office of Chief Information Officer (OCIO) and Contracting Office officials told us that because their Mega-3 contractors only process DOJ data onsite at EOUSA and USAO offices, they do not need to meet the Civil Division data security waiver requirements. We agree with EOUSA in this instance.

OBD-47 contractors perform services such as expert analysis, preparation for testimony, and litigation consulting for USAOs, and often perform these services offsite. The contractors often receive case information in printed documents or on flash drives or compact disks. Because the risk of data loss increases when using such media and hard copy documentation, it is essential that these contractors comply with data security requirements when processing information on personal equipment offsite.

OIG Audit Approach

The objectives of our audit were to determine whether EOUSA complies with DOJ policy regarding: (1) the use of whole disk encryption on employee, contractor, and subcontractor laptops processing sensitive and classified information; and (2) laptop encryption procedures for contractors and subcontractors.

To accomplish our objectives, we interviewed personnel and inspected equipment at EOUSA headquarters and six USAOs to determine whether equipment was properly encrypted, and to assess the effectiveness of policies and procedures related to encryption policy development, incident response, data security, and deployment practices.[10]

In addition, we met with the USAO procurement staff responsible for finalizing contractual agreements between expert witnesses and attorneys; legal assistants responsible for oversight of litigation support services; and expert witnesses and litigation contractors regarding contractual security requirements for laptop computers. We also reviewed EOUSA's efforts to safeguard DOJ data on other mobile devices such as electronic tablets. Appendix I contains a more detailed description of our audit objectives, scope, and methodology.

Previous Audits on Laptop Encryption Programs and Practices

On October 3, 2008, the Office of the Inspector General (OIG) received a Department of Justice Computer Emergency Readiness Team (DOJCERT) alert indicating that two unencrypted laptop computers were stolen from the offices of a consulting firm in Washington, D.C., that was performing litigation support work for the Civil Division.[11] The stolen laptops included

[10] The six USAOs that we judgmentally selected included an office from each of the four USAO size categories: (1) District of Maine (small), (2) Eastern District of Wisconsin (medium), (3) Eastern District of North Carolina (medium), (4) Western District of Washington (large), (5) Southern District of Florida (extra-large), and (6) Eastern District of Virginia (extra-large). We inspected laptops and electronic tablets at each location, with the exception of the Eastern District of Virginia, where we only inspected classified laptops.

[11] A DOJCERT alert is a notice that DOJCERT sends to components on pressing IT security issues such as network vulnerability.

Personally Identifiable Information (PII) of Civil Division attorneys, the consultant's employees, and plaintiffs, as well as potentially sensitive case information in support of the government's defense. As a result of this incident, the OIG initiated an audit of the Civil Division's Laptop Encryption Program and Practices, and our audit report was issued in July 2009.[12]

The July 2009 report concluded that the Civil Division complied with Department requirements by ensuring that its own laptop computers were encrypted to protect Department data. However, this audit also found that the Civil Division's efforts to ensure contractor safeguards over Department data on laptop computers owned by Civil Division contractors, subcontractors, and vendors needed significant improvement. Specifically, we found that an inventory of contractor laptops used to process Department data was not maintained, a large percentage of these laptops were not encrypted, and contractors had not received notification of Department laptop encryption requirements. We made seven recommendations to the Civil Division to enhance its safeguards over Department data on laptop computers. The Civil Division has implemented corrective actions to address the recommendations, which have been closed.

In March 2010 the OIG issued an audit of the Criminal Division's Laptop Encryption Program and Practices. During this audit, we tested for encryption on 40 of the 799 laptop computers owned by the Criminal Division. We found that 10 laptop computers did not have encryption software and 9 of the 10 did not have Windows passwords enabled, as required by Department policy. All of the unencrypted laptops, which were deployed to the Criminal Division's International Criminal Investigative Training Assistance Program, contained sensitive Department data. In addition, we determined that at least 43 laptop computers did not comply with Department standards and Criminal Division requirements for laptop security settings. Our audit also found that seven of the nine contractors tested had processed sensitive Department data on laptops that were not encrypted.

The March 2010 report also identified weaknesses in the oversight of data security policies for the Criminal Division's contractors. The two contracts under which most litigation support contractors were hired did not

[12] U.S. Department of Justice Office of the Inspector General, *The Civil Division's Laptop Computer Encryption Program and Practices,* Audit Report 09-33 (July 2009).

have the required security clause requiring encryption, and the Criminal Division had not implemented alternative controls to compensate for the contracts' deficiencies. We made 10 recommendations to the Criminal Division to enhance its safeguards over Department data on laptop computers. The Criminal Division has taken corrective actions to address the recommendations, which have been closed.

In April 2010, the OIG issued a memorandum to the Assistant Attorney General for Administration to inform him of the findings in the above mentioned OIG audit reports and to recommend that the Department re-emphasize the need for components to adhere to the Department's encryption policies for all laptop computers used to process Department data, including laptops used by contractors. Subsequently, in May 2010, the Department's Chief Information Officer (CIO) issued a memorandum to all component CIOs on the DOJ Data at Rest Program Implementation.[13] This document cited DOJ and Office of Management and Budget (OMB) encryption requirements for employees and contractors, and informed the component CIOs that recent audits conducted by the OIG had revealed instances of deficiency in meeting these mandates.

[13] Chief Information Officer, Department of Justice, memorandum to component Chief Information Officers, Department of Justice Data at Rest Program Implementation, May 19, 2010.

FINDINGS AND RECOMMENDATIONS

EOUSA's Efforts to Ensure Safeguards Over DOJ Data on Laptop Computers and Electronic Tablets Need Improvement

We found that 111 of the 120 EOUSA-owned laptops we tested that were used for unclassified processing were encrypted, 6 were not encrypted, and we could not determine the encryption status for 3 of the laptops. The six unencrypted laptops were used for special purposes such as jury use, use by visiting EOUSA employees, and the production of employee identification cards, but had not been labeled as such.

We reviewed three encryption monitoring scans completed by EOUSA for unencrypted laptops. We found that the first two scans identified approximately 60 unencrypted laptops that EOUSA subsequently encrypted in a timely manner. The third scan, however, identified eight unencrypted laptops whose encryption status has gone unaddressed for over a year.

In addition, we determined that EOUSA's official inventory of computer equipment, including laptops, was incomplete, contained inaccurate data entries, and was subject to delays in updating information. We further determined that EOUSA did not sufficiently track and monitor laptops used for classified processing. Our testing of two classified laptops and three classified hard drives for encryption determined that one laptop and one hard drive were not encrypted, and that two of the hard drives were inoperable. We also found that EOUSA is using more than 1,000 electronic tablets as part of its pilot program that do not fully comply with JMD waiver requirements, are not adequately monitored, and lack sufficient policies to minimize security risks.

We also reviewed EOUSA's procedures for contractor use of DOJ data and found that, despite a DOJ requirement that external contractors' laptops must be encrypted, EOUSA allowed contractors to use unencrypted equipment, relying on a "verbal waiver" extension from JMD. JMD officials disagreed that a

"verbal waiver" had been granted. EOUSA also failed to confirm that the unencrypted equipment met the conditions set out in the expired waiver. Finally, we found that the oversight of contractor data security is inconsistent among USAOs, increasing the risk of DOJ data loss.

Laptop Computers and Electronic Tablets Owned by EOUSA

Encryption Requirements and Encryption Process

DOJ Order 2640.2F Chapter 2 Section 12, Protection of Mobile Computers/Devices and Removable Media, notes that "information physically transported outside of the Department's secured physical perimeter is more vulnerable to compromise. The intent of this policy is to compensate for protections not provided by physical security controls when information is removed from the component location." The Order therefore requires that information on mobile computers/devices (notebook computers, personal digital assistants) and removable media must be encrypted using FIPS 140-2 validated or an NSA-approved encryption mechanism. In addition, the Order requires DOJ components to ensure that all security related updates are installed on mobile computers and devices.

EOUSA manages the encryption program for both EOUSA and the USAOs. In 2012, an EOUSA official stated that EOUSA planned to upgrade its personal computers and laptops throughout EOUSA and the USAOs, and the projected total number of laptops after their refresh would be 8,080.[14] During this computer refresh, all new laptops were expected to be encrypted as part of the imaging process.[15]

We found that EOUSA currently uses CheckPoint encryption software, formerly known as PointSec, instead of the Department's approved encryption software, GuardianEdge. CheckPoint does meet the FIPS 140-2 requirement of the DOJ Order, and according to EOUSA officials, CheckPoint offers implementation and performance advantages such as volume-based

[14] As of July 2013, the total number of refreshed laptops was 7,412.

[15] Imaging is the process of copying a computer's hard disk content to another computer. This is often used for a speedy and standardized installation to a large group of computers so that all the imaged computers have the same hard disk content and software configurations.

versus file-based encryption and centralized management software architecture. However, EOUSA is currently paying for both CheckPoint and GuardianEdge.[16] Although JMD is aware of EOUSA's desire to continue using CheckPoint, there is currently no waiver in place regarding its use. Therefore, we recommend that EOUSA either use the Department's encryption solution or obtain a waiver for the use of CheckPoint encryption.

Each USAO System Manager is responsible for encrypting the laptops at its location. The encryption begins during the installation of EOUSA's server-based image and continues running in the background until the installation is complete. However, there is no documented confirmation that the encryption process is complete. Instead, we were told that some USAOs' IT staffs may perform a visual check on the encryption status, but this process is neither consistent nor mandatory. This may result in laptops being used without the hard drive being fully encrypted. Therefore, we recommend that EOUSA and USAOs should verify and document that full-disk encryption is installed on all laptops, including the classified laptops in accordance with DOJ policy, such as using a checklist during the imaging process.

Laptop Encryption Testing

In order to verify full disk encryption on laptops, we tested a total of 120 unclassified and 2 classified laptops, as well as 3 classified hard drives from EOUSA headquarters and the 6 districts we visited.[17] Our review consisted of verifying that full disk encryption was present on each laptop, including the date of encryption.

---

[16] According to EOUSA, Checkpoint maintenance combines several products so a specific cost for each product is not readily available, but EOUSA officials estimated that the cost of CheckPoint encryption software is about $30,000. According to JMD, EOUSA paid about $28,000 for its share of the GuardianEdge software to the Department in 2012 in addition to the money it paid for CheckPoint. JMD requires all components to share the cost of Guardian Edge.

[17] We tested unclassified laptops from the Eastern District of Wisconsin, Western District of Washington, Eastern District of North Carolina, Southern District of Florida, and District of Maine, and classified laptops from the Eastern District of Virginia and Western District of Washington. The three classified hard drives that we tested at the Western District of Washington were assembled using two classified laptop shells for testing.

Of the 120 unclassified laptops in our sample, we were able to verify that 111 laptops were encrypted. However, we were unable to determine the date of encryption for 9 of those 111 laptops, either due to incomplete logs or because an older version of PointSec encryption that did not log the date of encryption was used. For the remaining nine laptops, we were unable to determine the encryption status of three laptops because two did not have a hard drive to test and one laptop had been decommissioned with its barcode removed. We determined that the other six laptops were unencrypted and dedicated for special purposes, such as jury use, use by visiting employees, and for an employee identification station. None of these six laptops, however, were labeled to identify their special purposes, nor were there policies that explicitly limited their use. Therefore, we recommend that EOUSA develop policies on the use of non-encrypted laptops for special use if such laptops are deemed necessary, and label these laptops accordingly.

We tested two classified laptops and three classified hard drives from the sites we visited for encryption testing. We determined that one of the laptops was encrypted, one laptop and one hard drive were not encrypted, and the remaining two hard drives were inoperable. At one site, the unencrypted laptop was the result of an unsuccessful encryption process and the status of the encryption was not checked once completed, so the unsuccessful encryption went undetected. At another site, the IT staff told us that the unencrypted hard drive was very old, had not been used for several years, and had not been encrypted because the staff had begun the process of excessing the laptop. In our judgment, these are two examples of preventable situations where the security of data could have been properly safeguarded had verification of the encryption and DOJ order for full-disk encryption been followed. For example, if EOUSA had subjected these laptops to the Department's Security Authorization process, the vulnerabilities would likely have been remedied.[18]

[18] Security Authorization, previously known as Certification and Accreditation (C&A), is the process used to implement information security by determining the security posture, evaluating risks, and developing corrective actions to deficiencies of a system. The Authorization Official reviews the Security Authorization Package of the system, which contains evidence including, but is not limited to, the system security plan, security assessment report, plan of action and milestones, and the Security Authorization memorandum.

Encryption Installation Records Not Maintained

DOJ Order 2640.2F Information Technology Security, Audit and Accountability, Chapter 1, Section 5, states that DOJ components should create, protect, and retain IT system audit records to the extent needed to enable security monitoring, analysis, investigation and reporting of unlawful, unauthorized, or inappropriate IT system activity.

There are two types of controls to identify unencrypted laptops: (1) encryption status checks of lost laptops and (2) periodic encryption status scans of network laptops.

Encryption Status Checks of Lost Laptops

The EOUSA Security Operations Center (SOC) investigates and confirms incident information. For a lost laptop, the SOC may confirm with the encryption team at EOUSA the encryption of the laptop. However, we found that the SOC did not always verify the encryption status of lost laptops, nor did it record its verification of encryption with the EOUSA encryption team on all tickets reported on lost laptops.[19] Therefore, we were unable to determine if this verification of encryption is consistently completed. We recommend that EOUSA document encryption verification in all EOUSA incident response tickets and disclose the encryption status to the Justice Security Operations Center (JSOC).[20] JSOC's Incidence Response Plan handbook states that "the implications of the loss can extend beyond the scope of the data items that have been lost, and can lead to additional unauthorized disclosures, classified spills, or financial losses."[21] The Incidence Response Plan handbook requires components to report the encryption status of lost data. Whether the data on the lost IT device is encrypted is an important piece of information to help assess the severity of the data loss.

[19] A ticketing system uses electronic files to record incident information.

[20] JSOC monitors and protects the IT environment for the Department, and provides leadership and guidance to all DOJ components in the areas of incident response. JSOC assists components with the reporting, monitoring, and resolution of their incidents, and acts as the main reporting source to US-CERT based on US-CERT's guidelines.

[21] DOJ OCIO, Computer System Incident Response Plan, Version 1.6, January 2012.

We reviewed the completeness of reporting from EOUSA SOC to JSOC and found that during the period between January 1, 2011, and January 18, 2012, 2 of 18 EOUSA incidents did not have a corresponding DOJCERT number and 6 DOJCERT tickets did not appear to have an EOUSA incident number. We found that for the two EOUSA tickets that did not have the DOJCERT number, one was for a laptop destroyed in a vehicle fire and deemed not necessary to report to DOJCERT, and the other involved a lost laptop that was found more than 4 months later. Any lost DOJ IT device containing data must be reported to JSOC within 1 hour from discovery of the loss. Therefore, the lost laptop, should have been reported to DOJCERT and issued a corresponding DOJCERT number. The six DOJCERT tickets that did not appear on EOUSA's SOC incident list were reported during the transition between the EOUSA helpdesk monitoring incidents to the EOUSA SOC reporting incidents. Those six incidents were either recorded in the helpdesk ticketing system or reported directly by the EOUSA SOC manager to DOJCERT.

We also reviewed the 40 tickets received by DOJCERT from EOUSA regarding the status of 29 lost laptops, 2 lost hard drives, and 9 lost electronic tablets between October 1, 2010, and July 31, 2012, and found that only 1 ticket noted the encryption status. Therefore, we were unable to determine the encryption status of the 29 lost laptops, 9 lost electronic tablets, and 1 lost hard drive because encryption status was not consistently recorded.

Periodic Status Scans for Encryption

EOUSA also monitors computer encryption compliance by periodically reviewing network computer encryption status. To review the status, a report is run by an Information Systems Security (ISS) staff member from System Center Configuration Manager (SCCM) on an ad-hoc basis to detect the disk encryption status of computers on the network.[22] There are no policies regarding the frequency, retention, or management of the scan.

To determine the effectiveness of the encryption monitoring program, we reviewed a sample of the encryption monitoring work completed by ISS.

[22] System Center Configuration Manager (SCCM) is a Microsoft network management tool that provides services such as software deployment, compliance settings management, and assets management of servers, desktops, laptops, and mobile devices.

We obtained the encryption audit reports for the last two reviews conducted as of April 20, 2012, which took place on November 23, 2011, and April 5, 2012, and we assessed the status of the incident tickets for each district office. These tickets, issued by the SOC per district, may encompass multiple incidents of non-compliance with encryption requirements on multiple pieces of equipment.

The November 23, 2011, scan included 37 tickets for 72 laptops and the April 5, 2012, scan included 28 tickets for 41 laptops. In order to determine if laptops identified as unencrypted in the April scan had been encrypted, we requested an additional scan, which occurred on April 23, 2012. The April 23, 2012, scan identified 25 laptops as unencrypted, which included 17 laptops that had already been identified in the April 5, 2012, scan and 8 newly identified unencrypted laptops.

We reviewed the 65 incident tickets from the first two scans from November 2011 and April 2012 and found that they had all been closed because: (1) the laptops were found to be properly encrypted and may have just been a false positive or (2) encryption software on laptops that were unencrypted was reinstalled. Although the length of time between ticket issuance and ticket closure varied from 1 week to over 4 months, most tickets were closed within 2 weeks. The 65 tickets cover a total of 113 laptops and we found that approximately 60 of the 113 laptops were confirmed by the districts to be unencrypted. These laptops, which should have been identified during the laptop imaging process, posed a data security risk when they were unencrypted.

In addition, in May 2012 we followed up with EOUSA officials about the eight remaining unencrypted laptops identified in the third scan dated April 23, 2012, and learned that the scan results had not been sent to the EOUSA SOC, and that no further follow-up had been conducted by ISS on these laptops. As of July 2013, ISS had still not sent the scan results of these eight unencrypted laptops to the EOUSA SOC for ticket issuance in order to mitigate the security risks posed by these laptops. We contacted EOUSA in July 2013 to determine the status of these laptops and were told that seven of the eight laptops had been disposed of in July 2012 during the laptop refresh, and that one laptop had been sent back to the vendor for replacement in May 2012. Due to a lack of communication and information sharing between ISS and the EOUSA SOC, these eight laptops were in use in the field, unencrypted for several months, increasing the risk to security.

To improve data security and help ensure that laptops are encrypted, we recommend that EOUSA complete encryption scans on a routine basis and timely follow up on results of scans.

Laptop and Electronic Tablet Inventory

Office of Management and Budget (OMB) Circular A-130 requires that a complete inventory of information resources, including personnel, equipment, and funds devoted to information resource management and information technology, be maintained to an appropriate level of detail.

EOUSA's official inventory for tracking laptops and electronic tablets is maintained using JMD's Unicenter Asset Portfolio Management (UAPM).[23] However, EOUSA and some USAOs also maintain separate inventories for local use using Excel spreadsheets. As a result, in addition to analyzing EOUSA's UAPM inventory file, we also requested and analyzed inventories from five USAO offices. We also analyzed additional information, such as location information, about laptops from SCCM and about electronic tablets from a mobile device management tool. [24]

USAO district offices are only authorized to order laptops and electronic tablets from EOUSA's OCIO Store.[25] Unauthorized laptop models are detected through network scans by EOUSA and flagged for disposal. When a district receives new laptops, each item is required to be entered into UAPM by EOUSA's Assistant Property Custodian and then sent to the district System Manager who is responsible for imaging the machine and assigning it to a particular person. An Evaluation and Review Staff from EOUSA performs a review on a yearly basis to spot check a sample of

[23] EOUSA's UAPM inventory contains only unclassified laptops. We discuss classified laptops and their inventories later in this section.

[24] This mobile device management tool can implement and enforce policies on mobile devices. EOUSA uses this tool to manage electronic tablets.

[25] The EOUSA OCIO Store is an intranet website operated by the OCIO's Office Automation Staff, where EOUSA and USAO management and procurement officials can order accredited IT systems, such as desktops, laptops, and electronic tablets. The intent of the store is to provide a simplified method to procure approved hardware, leverage the aggregate buying power, ensure USAOs procure accredited systems, and ensure USAOs receive standard equipment.

districts for resource and management compliance, including inventory management. In addition, when an item is excessed, USAOs request the removal of the item from UAPM. However, staff at some of the USAOs we visited informed us that the approval process for a disposal can take from 6 to 12 months and the actual disposal process itself may also take several months to complete. Therefore, USAO property records may not correctly reflect the status of disposed property.

We determined that obtaining an accurate number of laptops and electronic tablets from a system-generated listing from UAPM was problematic because there were multiple inconsistencies in the UAPM list, including the incorrect classification of items, duplicate entries, and incomplete and missing information. We also found delays in the entry and removal of inventory items, which caused inconsistencies in the inventory totals. In addition, our review of local USAO inventories found that while these inventories may be more current, they too included duplicate, incomplete, and inaccurate information, such as multiple barcodes for the same laptop.

Our analysis of a May 2012 UAPM listing required that we remove duplicate entries and correct device misclassifications, such as desktop computers classified as laptops. We determined that the total number of EOUSA laptops and electronic tablets was 10,790 and 166, respectively. In comparison, our review of the mobile device management tool file, which tracks electronic tablets, listed the total number of electronic tablets at 1,044, resulting in a material difference between the inventory information in UAPM and in the mobile device management tool of 878 electronic tablets. We determined that the discrepancies in the number of electronic tablets were caused by electronic tablets being identified in UAPM as computers, computer organizers, computer tablets, and laptops rather than electronic tablets; not all of these machine types were included in the UAPM file we analyzed. As a result, we selected the mobile device management tool data of 1,044 electronic tablets for our electronic tablet analysis, as it was more reliable.[26]

[26] As of July 18, 2013, according to the mobile device management tool, the electronic tablet inventory was 2,003.

In addition, our review of UAPM found listings for 14 laptop computers, the purchase of which is prohibited by EOUSA's laptop purchasing policy.[27] EOUSA officials stated that they believed these were procured before PortfolioStat – an agency-wide IT portfolio review - was in place, and that this PortfolioStat process should give EOUSA better insight into its IT procurements.[28] Nevertheless, these laptops may pose a risk to data security because they do not have Security Authorization and there are no security policies in place for monitoring their use. Therefore, we recommend that EOUSA identify unapproved laptops and remove them from use.

EOUSA officials told us that the UAPM does not keep an inventory of classified laptops. Therefore, we spoke with staff from EOUSA's Security and Emergency Management Office (SEMO) to discern how classified laptops are tracked. SEMO staff informed us that it tracks the location of classified laptops using a Microsoft Excel spreadsheet. We reviewed the inventory that SEMO staff provided and verified that the 24 classified laptops it listed were not included on the UAPM. While inspecting the two classified laptops and three classified hard drives as part of our encryption testing, however, we noted that one of the laptops was not listed on the SEMO classified laptop inventory spreadsheet. SEMO staff explained that the spreadsheet is updated when the USAOs contact their staff with changes in their classified laptop inventory and when EOUSA performs its annual "Call-Out" in which the USAOs are contacted to identify their classified laptops. This "Call-Out" process was described by SEMO staff as ineffective because some of the USAOs did not reply back to the "Call Out."

We also found that 23 of the 24 laptops listed for classified processing have not received a Security Authorization within the last 3 years as required by the Department security process. EOUSA's SEMO staff explained that it currently has no process for the certification of older classified laptops

[27] We gathered further information regarding 3 of the 14 laptops listed on the inventory. The three USAOs informed us that the laptops were not encrypted and stored no DOJ data. According to these USAOs, the laptops were used for video presentations.

[28] To reduce low priority and duplicative IT investments, OMB issued memorandum M-12-10 in March 2012, requiring agencies to, among other things, lead an agency-wide IT portfolio review (i.e., PortfolioStat) to establish a baseline of commodity IT investments (e.g., e-mail, mainframes and servers, financial systems), identify potential duplicative or wasteful investments, and finalize plans to consolidate their portfolio or move to shared services.

that may not meet Department requirements, but told us that it will develop a process in the future. EOUSA officials stated that the use of JCONS/TS has diminished its need for classified laptops and its goal is to reduce the number of classified laptops and standalone computers. In our judgment, proper oversight of classified laptops is necessary to mitigate the risk of classified data loss. Therefore, we recommend that EOUSA complete a Security Authorization package (formerly known as Certification & Accreditation package) for all classified laptops and standalone computers and reauthorize them every 3 years in accordance with DOJ policy.

We believe that EOUSA's lack of encryption on some of its classified devices, in addition to poor inventory management, allow for the potential loss of classified information. Further, without formal and enforced Security Authorization of classified laptops, EOUSA is not able to maintain appropriate oversight to prevent the unauthorized disclosure, modification, or destruction of classified information. We recommend EOUSA implement procedures to ensure that accurate, current, and reliable information is maintained in an official inventory for unclassified and classified equipment to help EOUSA to ensure that all required laptops are encrypted and deployed in compliance with DOJ policy.

EOUSA Electronic Tablet Pilot Program

On July 28, 2011, JMD issued to EOUSA a waiver approving the use of a manufacturer's smartphone and electronic tablet mobile devices for a pilot deployment program. The JMD waiver grants these mobile devices remote access to the DOJ network. Currently, electronic tablets are encrypted with a non-FIPS 140-2 compliant program through the manufacturer. Although the initial waiver expired on March 30, 2012, JMD approved a new waiver on May 24, 2012 on the use of up to 4,000 smartphone and electronic tablet mobile devices. The new waiver is effective through September 30, 2013, to allow time for the manufacturer to complete the required FIPS validation. The waiver specifies the following conditions:

1. Devices connected to the DOJ infrastructure shall use the Department's Trusted Internet Connection (TIC) and DOJ Connect infrastructure and be monitored by the Justice Security Operations Center.[29]

2. This deployment shall comply with DOJ Mobile Device Security Requirements, including Appendix A, the manufacturer's mobile device operating system Secure Implementation Instructions.[30]

3. Prior to pilot deployment, the EOUSA Authorizing Official shall formally accept all documented risks associated with tools not yet FIPS 140-2 validated.

4. All aspects of this pilot program, especially the security risks and mitigation, must be properly described in EOUSA's appropriate system security plan and included in all associated Security Authorization documentation.

EOUSA Compliance with Electronic Tablet Waiver Conditions

We evaluated EOUSA's compliance with the conditions specified by JMD in the waiver and found that while EOUSA met some of the requirements, it was not in full compliance with DOJ/EOUSA requirements.

We interviewed JMD officials for clarification on the requirement that the electronic tablets need to use the TIC because they are connected to the DOJ infrastructure. We also spoke with EOUSA officials regarding the connection of electronic tablets to both the DOJ Network and outside networks. We were informed that to access the DOJ network, devices must go through the TIC to be monitored. Electronic tablets use a VPN to access

[29] DOJ Connect infrastructure is the Department's remote access solution allowing users to connect through a Virtual Private Network (VPN).

[30] Appendix A of the DOJ Mobile Device Security Requirements provides the Department's configuration baselines for the manufacturer's mobile device operating system.

the DOJ network, which also goes through the TIC.[31] However, this does not address traffic that occurs outside the DOJ Network where the electronic tablets can connect to the Internet directly for personal use. Although we did not find evidence of inappropriate traffic outside the DOJ Network, we believe that this should be more thoroughly addressed in policy and guidance.

Regarding the requirement that the waiver comply with DOJ Mobile Device Security Requirements, including the manufacturer's mobile device operating system Secure Implementation Instructions, we found that EOUSA does not fully comply with Appendix A, the manufacturer's mobile device operating system Secure Implementation Instruction from JMD, which requires that all devices use a specified version number or higher of the operating system. When reviewing the applications installed on electronic tablets from the April 2012 mobile device management tool scan, we found that the mobile operating system of the devices were not up to date. Out of the total inventory of 1,044 electronic tablets, only 356 electronic tablets (34 percent) had the required operating system version or higher. Using devices with out-of-date mobile operating system versions may pose a higher security risk because older mobile operating system versions have more security vulnerabilities. EOUSA informed us that because the users manually update the electronic tablets, there is often a delay in the process. According to Appendix A, devices that are not running the latest approved versions should be restricted from connecting to DOJ services until they have been updated.

Finally, we found that EOUSA has not fully documented all aspects of this pilot program. Specifically, the security risks and mitigation that must be properly described in EOUSA's system security plan and included in all associated security authorization documentation was not present. While the documentation does include information on the mobile device architecture, it does not address security risks and mitigations, including those listed in Appendix A. Instead, EOUSA relies on Rules of Behavior that do not address issues that are specific to the mobile device operating system and the

[31] A VPN uses shared public telecommunication infrastructure, such as the Internet, to provide secure communication between two ends by using tunneling protocols, which encrypt the data at the sending end and decrypt data at the receiving end. A VPN provides secured access capabilities at a lower cost than the more expensive dedicated leased lines.

system security plan, thereby leaving potential security risks unidentified and unaddressed.

Electronic Tablet Policies and Procedures

Electronic tablets used at EOUSA are to be purchased through EOUSA's OCIO Store and are manually set up by IT personnel with a core set of applications. EOUSA uses a mobile device management tool to track and monitor these devices. The mobile device management tool also issues policies such as password and profile settings for the electronic tablet and updates EOUSA on the status of electronic tablets whenever they are connected to the EOUSA server, including their mobile operating system versions and any applications installed.

Electronic tablets enable users to download additional applications from the manufacturer's online application store. Although EOUSA's electronic tablets are pre-configured so that users have account access for EOUSA-approved applications from the online application store, there is no restriction that prevents users from downloading unapproved applications. Applications that are not approved can be requested and must go through a vetting process by EOUSA before being allowed to be downloaded.

While several electronic tablet-specific policies exist, such as mobile application approval and device loss and theft, we found that there is no clear policy governing actions that USAO and EOUSA IT staff should take when an employee leaves the organization, including when and if electronic tablets should be removed from the mobile device management tool list when electronic tablets are turned in from terminated users and reimaged before being assigned to new users. We also found that there is no policy regarding the consistent monitoring of electronic tablets, including the use of authorized applications.

In addition, while we found that EOUSA is capturing information from the mobile management tool scan that can be used for monitoring electronic tablets, it is not using the information for this purpose. For example, EOUSA is not actively monitoring the use of unauthorized applications unless the application is listed as unallowable by DOJ, such as Skype. During our review of electronic tablets and the applications installed on the devices, we found electronic tablets with unapproved applications including video games, TV programs, or file editing software. While these applications go through the manufacturer's security process, they may nevertheless pose a risk to

DOJ if they are not properly monitored and authorized. Therefore, we recommend that EOUSA monitor and take action on electronic tablets with unauthorized application downloads and with outdated versions of the mobile operating system.

Electronic Tablet Password Testing

We selected 12 electronic tablets for testing in 5 of the districts we visited and EOUSA headquarters based on inventories provided by each site. Our review consisted of verifying the password protection mechanisms on the electronic tablets. Of the 12 electronic tablets we tested, 11 were password protected using the manufacturer's non-FIPS 140-2 compliant software. We were unable to determine the status of one electronic tablet as it was slated for destruction.

Electronic Tablet Risks and Observations

As electronic tablets become more commonplace for business purposes, proper precautions need to be taken in order to protect DOJ information. The storage of DOJ information combined with a lack of FIPS 140-2 encryption, unapproved application usage, outdated mobile operating system versions, and the potential absence of traffic monitoring may increase the risk of improper or unobserved DOJ information dissemination. EOUSA is currently using over 1,000 electronic tablets, and comprehensive policies and procedures need to be in place to address the use of the devices. EOUSA's monitoring should be proactive to ensure that policies and procedures in place are being followed, such as for unauthorized applications or an out-of-date mobile operating system. Risks and any mitigating factors should also be appropriately documented by EOUSA to confirm an understanding of potential security issues and compliance with the electronic tablet waiver. Therefore, we recommend that EOUSA develop comprehensive security policies and procedures for monitoring and handling electronic tablets.

Laptop Computers Owned by Contractors and Subcontractors

OBD-47 Contractor Compliance with PGD 08-04

PGD 08-04 requires that laptops must employ encryption using a FIPS 140-2 approved encryption solution. PGD 08-04 also states that the contractor agrees that in the event of an actual or suspected breach of DOJ data (such as loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), the contractor will immediately (and in no event later than within 1 hour of discovery) report the breach to the DOJ Contracting Officer and the Contracting Officer's Technical Representative.

On February 24, 2010, JMD granted EOUSA a limited, 12-month waiver of PGD 08-04 to allow EOUSA time to comply with the above clauses and implement an encryption solution. As a result, on February 24, 2010, the USAOs received guidance from EOUSA to use a data security waiver for OBD-47 contractors, including expert witnesses and litigation consultants who, "in many cases, may be self-employed or have small staff, may not be technologically savvy or have no in-house IT employees to enable compliance with these clauses."[32] The waiver eliminated the need for these contractors to abide by PGD 08-04 when reviewing Personally Identifiable Information (PII) of 25 or fewer individuals. However, if the contractor would be reviewing PII of more than 25 individuals, the full requirements of PGD 08-04, including encryption on contractors' computers, was expected to be enforced. In addition, the waiver required contractors to follow an alternative set of data security procedures.

On February 16, 2011, JMD sent a memorandum to EOUSA regarding EOUSA's request for an extension of the waiver. The memorandum expressed concern that EOUSA was seeking another 12-month extension of the waiver without making progress towards implementation of the Department-wide encryption solution (GuardianEdge). However, JMD granted a 3-month waiver extension, until May 17, 2011, pending receipt of EOUSA's plan for implementing the Department-wide encryption solution,

[32] Assistant Director of Acquisitions Staff, EOUSA, memorandum to Contracting Officers, Administrative Officers, Security Managers, Civil Chiefs, Criminal Chiefs, and First Assistant U.S. Attorneys, Temporary Waiver of Security Clauses, February 24, 2010.

including the timeframe for each phase of deployment of GuardianEdge over the next year.

On May 6, 2011, EOUSA's OCIO office sent an e-mail to EOUSA staff noting that a verbal conversation had taken place between JMD and EOUSA regarding an extension of the waiver, and EOUSA subsequently informed the USAOs that EOUSA had received a "verbal waiver" extension from JMD. As a result, USAOs continued to implement this waiver for contractors processing the PII of 25 or fewer individuals. However, when we asked JMD officials about the waiver, they acknowledged that a discussion of the waiver had been held but they disputed that a verbal extension had been granted. We followed up with JMD again in September 2013 and were informed by the JMD officials that JMD does not give out verbal waivers and that components should follow the formal waiver application process as specified in the DOJ Security Authorization Handbook.[33] Therefore, neither JMD nor we consider the verbal waiver for PII of 25 or fewer individuals, as described by EOUSA, to be an official extension of the waiver.

In July 2013, JMD officials told us that EOUSA had received a waiver from the Department dated February 11, 2013, allowing EOUSA to deviate from PGD-08-04 with respect to its contractors. However, EOUSA operated without a formal, written, or documented waiver in place for almost 2 years, from May 17, 2011, to February 11, 2013.

JMD granted the February 11, 2013, waiver through September 30, 2013, and stated:

> Given the unique circumstances, but recognizing the need to encrypt all sensitive data at rest and in transit, the waiver requested is granted based on the following conditions:
>
> - EOUSA will continue to use FIPS 140-2 encrypted solutions for transmitting case and investigation information via mail and email to their consultants and expert witnesses.

[33] Department of Justice OCIO Information Technology Security Staff, Security Authorization Handbook, V. 8.3, June 2011.

- By February 28, 2013, EOUSA will develop and submit contract policy changes that identify specific clauses that address data handling requirements for the consultants and expert witnesses.

- EOUSA will research and test additional technical solutions for securing and sharing case and investigation information with all of their consultants and expert witnesses. These include secure file hosting services and digital rights management technologies. EOUSA should report back the outcomes of these efforts by September 30, 2013.

Previously, EOUSA's waiver eliminated the need for these contractors to abide by PDG 08-04 when reviewing PII of 25 or fewer individuals. In contrast, based on its language, we believe that the February 11, 2013, waiver offers the same exemption from PGD 08-04 while not having the limitation of PII of 25 or fewer listed among its conditions. The new waiver requires EOUSA and USAOs to encrypt the data in transmission to the contractors.

On June 17, 2013, EOUSA communicated the current February 11, 2013, waiver to its District offices in an email. However, EOUSA specifically stated in the email that there was no change from the current contracting procedures for vendors handling electronically stored information containing the PII of 25 or fewer individuals. In our opinion, EOUSA did not fully communicate to its offices the conditions of the February 11, 2013, waiver because it did not specify the new requirement that a FIPS 140-2 encryption solution is to be used for transmitting case information to the contractors. We recommend that EOUSA implement each of the conditions of the February 11, 2013, waiver to ensure that all sensitive data are encrypted between USAOs and their consultants and expert witnesses.

USAO, Expert Witness, and Litigation Consultant Compliance with Data Security Requirements

Each USAO maintains and manages its own contracts and contracting process, including contractor oversight. Therefore, we were unable to determine the specific number of contractors that USAOs employ. However, EOUSA officials estimated that the total number of contractors and subcontractors it oversees is in the thousands. We selected a sample of five USAOs (Southern District of Florida, District of Maine, Eastern District of North Carolina, Western District of Washington, and Eastern District of

Wisconsin) and interviewed attorneys, contracting officers, and legal assistants in order to evaluate USAO supervision of contractors' waiver compliance and data security.

We found that there are inconsistent processes and a lack of formal guidelines and requirements regarding: securing data for transmission to, from, and between USAOs and the contractors, including whether information should be encrypted and the appropriate methods of transmission (such as compact discs or e-mails); who was responsible for sending information or ensuring information was secured; and when to send information and what circumstances under which information may be shared before a contract is in place. Therefore, we recommend that EOUSA define the roles of attorneys, legal assistants, and contracting officers within the USAOs regarding contractor data security responsibility.

We also found that the USAOs we visited, which at the time were operating under the expired waiver described above, did not have a process in place to determine whether the case data contained PII relating to 25 or fewer individuals. Rather, it was generally assumed to be less than 25 PII so the data security waiver would be applicable.[34]

We reviewed 82 contracts of various performance types for signed data security waivers at the five USAOs we visited to determine whether waivers were returned in a timely manner. We determined that 62 of the 82 (or 76 percent) contracts received a waiver. However, 23 of these 62 waivers (or 37 percent) were signed and sent back after the invoices for the contract work were submitted, which does not provide reasonable assurances that the contractors were fully aware of the data security procedures before starting the contract work. Additionally, the collection rate of the signed waivers at these five USAOs varied significantly, from 50 to 100 percent. Overall, it appears that each site managed contracts differently regarding the enforcement of signing the data waiver and performance of work after waiver signature. Therefore, there is inadequate assurance from contractors before the start of the contracts that contractors

[34] By comparison, the new February 2013 waiver requires encrypting all data in transmission to the contractors; however, USAOs have not been instructed by EOUSA to implement this condition of the new waiver. See the discussion in the previous section on EOUSA's implementation of the new waiver.

are aware of, understand, and will comply with the requirements of the waiver.

We also interviewed a total of 32 expert witness and litigation support consultants in the Eastern District of Wisconsin and the Western District of Washington to assess their compliance with EOUSA data security requirements. We found that these contractors provided services, using their personal computer equipment, for a variety of professions, including the medical professions of gerontological nurse practitioner, psychiatrist, neurosurgeon, and interventional cardiologist. These medical contractors have processed medical records on their personal computer equipment while contracting for the Department.

We interviewed contractors about anti-virus software, encryption, password protection, the amount of PII and PII safeguarding, incident reporting awareness, and the use of sub-contractors. We found that the contractors received case information in multiple ways, such as printed documents, flash drives, or compact discs, and often the information was unencrypted. We also found that contractors did not always meet the requirements in the expired waiver for anti-virus software, password protection, and pass-through data security requirements to sub-contractors. Some contractors also informed us that they had not been instructed on data destruction requirements. While these requirements are not explicitly stated in the new waiver, in our judgment they are sound business practices to minimize DOJ data loss.

While the USAOs need an efficient and expeditious process for hiring contractors to provide litigation consultants and expert witness services, they must simultaneously ensure that the process provides an appropriate level of data security. Due to the large number of contractors employed by the USAOs, the potential for data breaches is greatly increased when DOJ policy is not followed. Therefore, the contract process should be closely monitored and managed to minimize the risk of data loss and the associated harm it will cause.

We therefore recommend that EOUSA increase its oversight of contractors to ensure that contractors: (1) are aware of and adhere to any security provisions required by the USAOs prior to starting work; (2) receive case information in an encrypted format; (3) implement sound business practices such as anti-virus software, password protection, and data

destruction when the case data are not needed; and (4) instruct the sub-contractors about pass-through data security provisions.

Conclusion

To ensure that all required laptops are encrypted and deployed in compliance with DOJ policy, EOUSA needs to implement a more accurate and reliable inventory for all laptops. In addition, EOUSA should create appropriate policies and procedures to verify, validate, and monitor encryption for the processing of both unclassified and classified laptops, as well as electronic tablets, to minimize the risks that result from unwanted exposure of DOJ data.

We also found that EOUSA needs to strengthen its oversight of contractors who use laptops to process DOJ data. Specifically, EOUSA should implement each of the conditions of the February 11, 2013, waiver of the requirements of PGD 08-04, including the requirement that all data transmitted to contractors is encrypted. It should also take other steps to strengthen contractor oversight at the USAOs, including ensuring that USAOs receive reasonable assurances that contractors understand, are able to implement, and have agreed to implement all applicable DOJ data security requirements before receiving DOJ data and beginning contract work.

Recommendations

We recommend that EOUSA:

1. Use the Department's encryption solution or obtain a waiver for the use of CheckPoint encryption.

2. Verify and document that full-disk encryption is installed on all laptops, including the classified laptops, in accordance with DOJ policy, such as using a checklist during the imaging process.

3. Develop policies on the use of non-encrypted laptops for special use if such laptops are deemed necessary, and label these laptops accordingly.

4. Document encryption verification in all EOUSA incident response tickets and disclose the encryption status to JSOC.

5. Complete encryption scans on a routine basis and timely follow up on results of scans.

6. Identify unapproved laptops and remove them from use.

7. Complete a Security Authorization package (formerly known as Certification & Accreditation package) for all classified laptops and standalone computers and re-authorize them every 3 years in accordance with DOJ policy.

8. Implement procedures to ensure that accurate, current, and reliable information is maintained in an official inventory for unclassified and classified equipment to help EOUSA to ensure that all required laptops are encrypted and deployed in compliance with DOJ policy.

9. Monitor and take action on electronic tablets with unauthorized application downloads and with outdated versions of the mobile operating system.

10. Develop comprehensive security policies and procedures for monitoring and handling electronic tablets.

11. Implement each of the conditions of the February 11, 2013, waiver to ensure that all sensitive data are encrypted between USAOs and their consultants and expert witnesses.

12. Define roles of the attorneys, legal assistants, and contracting officers within the USAOs regarding contractor data security responsibility.

13. Increase its oversight of contractors to ensure that contractors: (1) are aware of and adhere to any security provisions required by the USAOs prior to starting work; (2) receive case information in an encrypted format; (3) implement sound business practices such as anti-virus software, password protection, and data destruction when the case data are not needed; and (4) instruct the sub-contractors about pass-through data security provisions.

STATEMENT ON INTERNAL CONTROLS

As required by the Government Auditing Standards, we tested, as appropriate, internal controls significant within the context of our audit objectives. A deficiency in an internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to timely prevent or detect: (1) impairments to the effectiveness and efficiency of operations, (2) misstatements in financial or performance information, or (3) violations of laws and regulations.

Our evaluation of the EOUSA's internal controls was not made for the purpose of providing assurance on its internal control structure as a whole. The EOUSA's management is responsible for the establishment and maintenance of internal controls.

As noted in the Finding section of this report, we identified deficiencies in the EOUSA's internal controls that are significant within the context of the audit objectives and, based upon the audit work performed, that we believe adversely affect the EOUSA's ability to ensure that DOJ data is appropriately protected from unauthorized access, use, disclosure, disruption, modification, or destruction.

Because we are not expressing an opinion on the EOUSA's internal control structure as a whole, this statement is intended solely for the information and use of the EOUSA and the Department of Justice. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

As required by the *Government Auditing Standards* we tested, as appropriate given our audit scope and objectives, selected transactions, records, procedures, and practices to obtain reasonable assurance that the EOUSA's management complied with federal laws and regulations, for which non-compliance, in our judgment, could have a material effect on the results of our audit. The EOUSA's management is responsible for ensuring compliance with federal laws and regulations applicable to the information security controls. In planning our audit, we identified the following laws and regulations that concerned the operations of the EOUSA and that were significant within the context of the audit objectives:

- Senior Procurement Executive Procurement Guidance Document (PGD) 08-04,
- Protection of Department Sensitive Information on Laptop and Mobile Computing Devices, DOJ Memorandum
- OMB M-07-16,
- OMB Circular A-130,
- DOJ Order 2640.2F, and
- DOJ IT Security Standards

Our audit included examining, on a test basis, the EOUSA's compliance with the aforementioned laws and regulations that could have a material effect on EOUSA's operations. We interviewed key personnel within the EOUSA and performed a physical review on select laptop computers owned by EOUSA and contractors. Additionally, we interviewed a select group of vendors contracted to provide litigation support services to the EOUSA.

APPENDIX I

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The OIG performed this audit to assess EOUSA's laptop computer encryption program and practices. Specifically, the audit objectives were to determine whether EOUSA complies with federal and Department of Justice policies regarding: (1) the use of whole disk encryption on employee, contractor, and subcontractor laptops that process DOJ sensitive and classified information; and (2) laptop encryption procedures for contractors and subcontractors providing litigation support services.

Scope and Methodology

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit scope was an 11-month period, from December 2011 through October 2012. To assess EOUSA's laptop computer encryption program and practices, we interviewed EOUSA and United States Attorneys' Office (USAO) personnel with responsibilities related to incident response, encryption policy development, data security, and deployment practices. We also interviewed JMD staff responsible for encryption policy development and data security. In addition, we reviewed EOUSA laptop and electronic tablet inventories, electronic tablet application scans, laptop encryption monitoring scans, and incident response reports. We also performed follow-up interviews and analyses from November 2012 to September 2013.

Because USAOs vary in size - small (under 25 attorneys), medium (25-44 attorneys), large (45-99 attorneys), and extra-large (100 or more attorneys) - we judgmentally selected at least one USAO from each size category, in addition to EOUSA, for our field work. The six USAOs we visited were the: (1) District of Maine (small), (2) Eastern District of Wisconsin

(medium), (3) Eastern District of North Carolina (medium), (4) Western District of Washington (large), (5) Southern District of Florida (extra-large), and (6) Eastern District of Virginia (extra-large).

From a total population of 1,100 unclassified laptops at 5 of the 6 sites, according to local inventory lists, we randomly selected a sample of 120 laptops for full encryption installation testing. In addition, we tested a total of 12 electronic tablets at EOUSA and USAO offices to determine if the use of these electronic tablets was in compliance with current encryption policy. We tested unclassified laptops from the Eastern District of Wisconsin, Western District of Washington, Eastern District of North Carolina, Southern District of Florida, and District of Maine. We tested two classified laptops from the Eastern District of Virginia and three classified hard drives at the Western District of Washington. The hard drives that we tested were assembled using two classified laptop shells for testing. These non-statistical sample designs do not allow projection of the test results to all laptops and electronic tablets.

We also identified a total of two classified laptops and three classified hard drives at the six sites we visited and reviewed them for encryption status. Two classified laptops were in the Western District of Washington and the three hard drives were in the Eastern District of Virginia.

We also selected a sample of expert witness laptops to test and considered the diverse work performed in support of litigation, such as medical evaluations, economic analysis, and environmental surveys. In addition, we interviewed USAO procurement staff, responsible for finalizing contractual agreements between expert witnesses, about contractual security requirements for laptop computers. Further, at five of the sites we visited (Western District of Washington, Eastern District of Wisconsin, Eastern District of North Carolina, Southern District of Florida, and the District of Maine), we reviewed USAO contract documents for litigation support services and interviewed attorneys and legal assistants regarding the oversight of litigation support services. At the Western District of Washington and the Eastern District of Wisconsin, we also interviewed 32 expert witnesses contracted to provide litigation support, to determine the levels of data security compliance and oversight they received from USAOs.

Finally, we met with the EOUSA Contracting Officer's Technical Representative and two Mega 3 contractors who work onsite at EOUSA and

use EOUSA laptops. These two Mega 3 contractors did not process DOJ data offsite, therefore there were no Mega 3 contractor laptops to test.

APPENDIX II

DOJ Procurement Guidance Document 08-04, Contractor-Owned Laptop Security Requirements[35]

Section A of the PGD 08-04 memorandum lists the requirements for the contractor-owned laptops to process or store DOJ data. They are as follows:

(1) Laptops must employ encryption using a FIPS 140-2 approved product;

(2) The contractor must develop and implement a process to ensure that security and other applications software is kept up-to-date;

(3) Mobile computing devices must utilize anti-viral software and a host-based firewall mechanism;

(4) The contractor must log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required. All DOJ information is considered sensitive information unless designated as non-sensitive by the Department;

(5) Contractor-owned removable media, such as removable hard drives, flash drives, CDs, and floppy disks, containing DOJ data, must not be removed from DOJ facilities unless encrypted using a FIPS 140-2 approved product;

(6) When no longer needed, all removable media and laptop hard drives shall be processed (sanitized, degaussed, or destroyed) in accordance with security requirements applicable to DOJ;

(7) Contracting firms shall keep an accurate inventory of devices used on DOJ contracts;

---

[35] Senior Procurement Executive, Department of Justice, memorandum to component procurement chiefs, DOJ Procurement Guidance Document 08-04, Security of Systems and Data, Including Personally Identifiable Information, March 20, 2008.

(8) Rules of behavior must be signed by users. These rules must address at a minimum: authorized and official use; prohibition against unauthorized users; and protection of sensitive data and personally identifiable information; and

(9) All DOJ data will be removed from contractor-owned laptops upon termination of contractor work. This removal must be accomplished in accordance with DOJ IT Security Standard requirements. Certification of data removal will be performed by the contractor's project manager and a letter confirming certification will be delivered to the CO within 15 days of termination of contractor work.

APPENDIX III

DOJ's Clarifications on the Data Security Implementation of the PGD 08-04 Procurement Guide[36]

The Department's June 17, 2008, memorandum from the Senior Procurement Executive provided clarification on the implementation of data security requirements, including PII for the PGD 08-04 Guidance. It states that:

(1) Any documents filed with or produced to the courts do not need to be encrypted, as courts will not accept encrypted data;

(2) Documents that cannot be altered for "chain of custody" reasons need not be encrypted, but rather may be treated as evidence and controlled through delivery tracking;

(3) Documents produced to opposing counsel generally needs to be protected in transit via encryption. Once documents are in opposing counsel's custody, they are no longer DOJ's responsibility;

(4) As long as data extracts are still needed, there is no need to certify such need every 90 days;

(5) If data is provided to a contractor on an encrypted thumb drive, hard drive, or laptop AND data is not downloaded to a personal computer or network, most requirements regarding system security, such as testing, will not apply;

(6) Data that is publicly available or that has previously been released (e.g., via FOIA) is presumed to be non-sensitive;

(7) OCIO is available to assist in identifying compensating controls and/or plans of action and milestones (POAMs) where appropriate; and

[36] Senior Procurement Executive, Department of Justice, memorandum to component procurement chiefs, Implementation Guidance Regarding Security of Systems and Data, Including Personally Identifiable Information, June 17, 2008.

(8) Micro purchases are not covered by PGD 08-04 at this time; however, components should examine their controls for ensuring data security for those types of purchases.

APPENDIX IV

EOUSA'S RESPONSE

U.S. Department of Justice

Executive Office for United States Attorneys

Office of the Director

950 Pennsylvania Ave., N.W. *(202) 252-1000*
Room 2261, RFK Main Justice Bldg.
Washington, D.C. 20530

DATE: January 23, 2014

TO: Reginald F. Allen
Director, Computer Security and Information Technology Office
Office of the Inspector General

FROM: Norman Wong /S/
Deputy Director and Counsel to the Director
Executive Office for United States Attorneys

SUBJECT: Response to OIG Audit of EOUSA "Laptop Computer and Electronic Tablet Encryption Program and Practices"

The Executive Office for United States Attorneys (EOUSA) appreciates the audit undertaken by the Department of Justice, Office of the Inspector General (OIG), regarding the encryption of laptop computers and electronic tablets used by EOUSA and the 94 United States Attorneys' Offices (USAOs). The goal of the OIG audit was to assess whether laptops and tablets used by USAO employees, contractors, and subcontractors contain adequate security controls to protect sensitive data processed on those devices.

EOUSA places a high priority on computer security and has established wide-ranging procedures to safeguard United States Attorney information technology (IT) assets. To that end, the Information Systems Security Staff, in EOUSA's Office of the Chief Information Officer (OCIO), coordinates encryption protocols and security training for all USAO personnel nationwide. EOUSA's Security Operations Center in Columbia, SC, provides 24/7 intrusion

detection monitoring and vulnerability management. And each USAO has a Systems Manager and District Office Security Manager available to coordinate security issues locally. EOUSA places a commensurately high priority on the usability of IT assets so that they may be employed most effectively by a wide range of geographically dispersed users – including attorneys, support staff, joint task force personnel, litigative consultants and expert witnesses – and thereby best achieve the success of the Department's investigatory, prosecutorial, and litigation mission.

With this framework in mind, we next address each of the 13 recommendations contained in the OIG draft audit report. Id. at 26-27.

Recommendation 1. Use the Department's encryption solution or obtain a waiver for the use of CheckPoint encryption.

Response 1. EOUSA's CheckPoint encryption solution complies with DOJ Order No. 2640.2F, "Information Technology Security," because CheckPoint is FIPS 140-2 compliant. Accordingly, no waiver is required by the Order, which directs that: "Components shall … [e]ncrypt sensitive and classified information transported outside of the agency's secured, physical perimeter in digital format … using FIPS 140-2 validated or NSA approved encryption, as appropriate." See DOJ Order No. 2640.2F (Nov. 26, 2008) at 8, Chapter 1, §4(g)(2) ("Media Protection").[1]

Recommendation 2. Verify and document that full-disk encryption is installed on all laptops, including the classified laptops, in accordance with DOJ policy, such as using a checklist during the imaging process.

Response 2. Accepted and being implemented, e.g.:

(a) In January 2012, EOUSA began implementing its "Trusted Network Access" (TNA) solution – comprised of ForeScout's CounterAct network access appliances – to centrally monitor the encryption status of all online systems within the unclassified United States Attorney computer network.

(b) In addition, as of March 2013, EOUSA's Security Operations Center (SOC) verifies the encryption status of laptops in connection with all lost/stolen laptop incident reports.

(c) Further, in July 2013, EOUSA's Office Automation Staff (OAS) updated its Microsoft System Center Configuration Manager (SCCM) to enhance the imaging of all Windows-based systems, including the installation of encryption software. Previously, SCCM could allow an image to be pushed to a laptop and not inform if the encryption application had

[1] With respect to encryption costs, the Audit Report states that "EOUSA paid about $28,000 for its share of the GuardianEdge software to the Department in 2012 in addition to the money it paid for CheckPoint" (id. at 10, n.15). This is an apparent reference to EOUSA's share of DOJ's IT Working Capital Fund (WCF). While components currently have no ability to "opt-out" of WCF costs, we have found CheckPoint technically superior to, and more user-friendly than, GuardianEdge for reliable encryption.

failed. As enhanced, SCCM now verifies the completion of all applications prior to a laptop being released for use. EOUSA Information Bulletin 136,"*Image 2012 Update 03 (SCCM 2007 Task Sequence).*"

(d) With respect to classified data, EOUSA laptop computers used for processing National Security Information ("NSI" or "classified information") comply with the pertinent provisions of DOJ Information Technology Security Standard 1.6, "Classified Laptop and Standalone Computers Security Policy" (www.justice.gov/oig/reports/plus/a0532/app3.htm). In pertinent part, this DOJ policy calls for "[e]ncryption of the hard drive … on classified computer systems." Id. §3.13; see also Attachment 7 to Security Standard 1.6 ("Technical Checklist" ¶8, regarding "configuration and logs of the classified computer").

Recommendation 3. Develop policies on the use of non-encrypted laptops for special use if such laptops are deemed necessary, and label these laptops accordingly.

Response 3. Accepted and being implemented, e.g.:

In order to meet the United States Attorneys' law enforcement and litigation mission, EOUSA makes available to USAOs certain "special use" laptops containing specialized hardware and software designed to facilitate electronic discovery and litigation support (such as for audio/video processing and courtroom presentations), as well as a "standalone" image for processing unclassified data on laptops unconnected to internal DOJ networks. Insofar as such laptops are not equipped with whole-disk encryption capabilities (e.g., to improve processing performance), they should be labeled accordingly.

Recommendation 4. Document encryption verification in all EOUSA incident response tickets and disclose the encryption status to JSOC.

Response 4. Accepted and being implemented; see Response 2(b) above, noting that this OIG recommendation became a standard procedure at the EOUSA SOC as of March 2013 for all reported lost/stolen laptops.

Recommendation 5. Complete encryption scans on a routine basis and timely follow up on results of scans.

Response 5. Accepted and being implemented; see Response 2(a) above, noting that EOUSA's new TNA solution centrally monitors the encryption status of all online systems within the unclassified United States Attorney computer network.

Recommendation 6. Identify unapproved laptops and remove them from use.

Response 6. Accepted and being implemented, e.g.:

EOUSA's SOC monitors the entire unclassified United States Attorney computer network on a routine and ongoing basis for intrusion detection, malware, and other unauthorized usage. Among the SOC's tools is the TNA solution discussed above, which detects devices on

the network that do not contain an authorized configuration. When an unapproved laptop is detected, the SOC immediately coordinates the shutdown of affected ports and follows-up on the security incident to promptly remove the laptop from the network.

Recommendation 7. Complete a Security Authorization package (formerly known as Certification & Accreditation package) for all classified laptops and standalone computers and re-authorize them every 3 years in accordance with DOJ policy.

Response 7. Accepted and being implemented, e.g.:

EOUSA is working with the Justice Management Division (DOJ) to enhance compliance with DOJ Information Technology Security Standard 1.6, "Classified Laptop and Standalone Computers Security Policy," which states in pertinent part:

> [E]ach classified laptop and standalone computer must be certified and accredited prior to use and re-certified and re-accredited every three years or whenever a major system change occurs. To limit the unnecessary duplication of certification and accreditation activities, the Justice Management Division performed a "type accreditation" for classified laptop and standalone computers. Components are encouraged to implement computers consistent with the type accreditation.

Id. §3 (www.justice.gov/oig/reports/plus/a0532/app3.htm) (emphasis added).

Recommendation 8. Implement procedures to ensure that accurate, current, and reliable information is maintained in an official inventory for unclassified and classified equipment to help EOUSA to ensure that all required laptops are encrypted and deployed in compliance with DOJ policy.

Response 8. Accepted and being implemented, e.g.:

Newly purchased laptops contain no DOJ data or desktop image. Following acquisition, all laptops – both those intended for unclassified and classified use – are subject to inventory controls and logging in the Department's Unicenter Asset Portfolio Management (UAPM) system. It is expected that all laptops in each USAO's inventory will be electronically stored by UAPM in a central location.

In addition, once a laptop receives an image via EOUSA's SCCM system, SCCM logs that laptop's status and last known image. While SCCM is not used to image or track classified laptops, the existence of a classified laptop will be captured in UAPM following acquisition as noted above.

Recommendation 9. Monitor and take action on electronic tablets with unauthorized application downloads and with outdated versions of the mobile operating system.

Response 9. Accepted and being implemented, e.g.:

Electronic tablets with outdated versions, as mentioned in the Audit Report, have been targeted for updating, respectively, to versions dated September 2012, May 2013, and November 2013. In addition, since December 2012, EOUSA has begun daily reporting of non-approved electronic tablet applications, version lists, and inventories. These reports are generated each day at 3:00 a.m. (Eastern) and made available to all USAO Systems Managers and EOUSA electronic tablet management, as well as EOUSA's Information Systems Security (ISS) Staff, which audits the reports and takes action to have non-approved electronic tablet applications removed.

Recommendation 10. Develop comprehensive security policies and procedures for monitoring and handling electronic tablets.

Response 10. Accepted and being implemented, e.g.:

As noted in Response 9 above, EOUSA has strengthened its internal management controls for maintaining electronic tablets up-to-date with the latest mobile operating system and keeping them free of unauthorized applications. In addition, a formal United States Attorneys' Procedure (USAP No. 3-16.200.006, "Requesting Mobile Application Approval") has been issued to outline procedures by which users may request electronic tablet apps to be evaluated by EOUSA for approval. The USAP is currently in the process of being updated to emphasize that requests are required to clearly support the mission of the United States Attorneys' Offices. USAPs apply to all EOUSA and USAO network users nationwide and provide a uniform body of procedural guidelines to facilitate the establishment of, and compliance with, sound management principles.

Recommendation 11. Implement each of the conditions of the February 11, 2013, waiver to ensure that all sensitive data are encrypted between USAOs and their consultants and expert witnesses.

Response 11. EOUSA and the Department's Information Technology Security Staff (ITSS) are currently working on an updated waiver from PDG 08-04 to ensure that litigative consultants and expert witnesses needed to support USAO cases can continue to securely share data with Assistant United States Attorneys. EOUSA's position is that it has properly operated under a waiver (written or oral) at all material times.

Recommendation 12. Define roles of the attorneys, legal assistants, and contracting officers within the USAOs regarding contractor data security responsibility.

Response 12. Accepted and being implemented, e.g.:

As noted above, EOUSA maintains a system of United States Attorneys' Procedures (USAPs) to provide a uniform body of sound management principles nationwide. Potential modifications to the following USAPs are being considered in connection with this recommendation:

- USAP No. 3-13.000.001, "Government-Contractor Relationship Guidelines."

- USAP No. 3-15.111.001, "Contractor Security Approval Procedures for Sensitive but Unclassified (SBU) Contracts."
- USAP No. 3-15.120.002, "Handling and Safeguarding Federal Tax Information."
- USAP No. 3-15.120.004, "Safeguarding Grand Jury Information."

Recommendation 13. Increase its oversight of contractors to ensure that contractors: (1) are aware of and adhere to any security provisions required by the USAOs prior to starting work; (2) receive case information in an encrypted format; (3) implement sound business practices such as anti-virus software, password protection, and data destruction when the case data are not needed; and (4) instruct the sub-contractors about pass-through data security provisions.

Response 13. Accepted and being implemented, e.g.:

Increased oversight is being considered in connection with this recommendation so as to better ensure contractor and subcontractor awareness of, and adherence to, all applicable USAPs and Departmental directives regarding laptop and tablet security/encryption requirements. This may include training vehicles, such as the annual Computer Security Awareness Training (CSAT), which is required of all DOJ employees, contractors, and other network users. For example, CSAT modules could be developed to provide refresher training on the requirement in EOUSA's "Rules of Behavior" that users may "not transmit … sensitive information … over the Internet unless encrypted" absent a waiver.[2] With respect to anti-virus software, password protection, and data destruction, EOUSA's Security Operations Center (SOC) monitors the United States Attorney network on a continuous basis to ensure up-to-date antivirus software protection, guard against computer malware, and deter unauthorized network intrusions. And, whenever security issues are detected, Security Incident Reports are promptly generated and processed for timely resolution. Moreover, USAP 3-13.200.004, "Media Disposal," not only sets forth detailed guidance on how to securely dispose of electronic media, but also culminated in the establishment of an in-house "Data Destruction Center," co-located near the SOC at EOUSA's Network Operations Center (NOC) in Columbia, SC, for use by all 94 USAOs nationwide.

[2] The Rules of Behavior applicable to all United States Attorney network users are contained in USAP No. 3-16.200.003, "Network Account Security Management" (Attachment 5); see also DOJ Order No. 2640.2F, at 8, Chapter 1, §4(g)(2) ("Encrypt sensitive … information transported outside of the agency's secured digital perimeter in digital format"). It should also be noted that USAP No. 3-13.200.005, "Secure Shipping of Information," prescribes a number of special packaging and tracking requirements for all physical shipments containing sensitive information.

APPENDIX V

OFFICE OF INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO RESOLVE THE REPORT

The OIG provided a draft of this audit report to EOUSA. EOUSA's response is incorporated in Appendix IV of this final report. The following provides the OIG analysis of the response and summary of actions necessary to resolve the report.

Recommendations:

1. Use the Department's encryption solution or obtain a waiver for the use of CheckPoint encryption.

Closed. This recommendation is closed. Subsequent to receiving EOUSA's response to the draft, JMD issued EOUSA a waiver that will allow it to use CheckPoint through December 31, 2014. We reviewed the waiver and determined that it adequately addressed our recommendation.

2. Verify and document that full-disk encryption is installed on all laptops, including the classified laptops, in accordance with DOJ policy, such as using a checklist during the imaging process.

Resolved. EOUSA concurred with our recommendation. EOUSA stated in its response that (a) its "Trusted Network Access" (TNA) solution centrally monitors the encryption status of all online unclassified systems; (b) since March 2013, EOUSA's SOC verifies the encryption status of lost/stolen laptops; (c) it has enhanced its System Center Configuration Manager (SCCM) to verify the completion of the laptop imaging process, including encryption, described in EOUSA Information Bulletin 136; and (d) its classified laptops comply with DOJ IT Security Standard 1.6, "Classified Laptop and Standalone Computers Security Policy."

This recommendation can be closed when we receive evidence of EOUSA's: (a) implementation of the TNA solution and samples of corrective actions taken on unencrypted laptops from this solution, also applicable to Recommendation 5; (b) implementation of the encryption verification procedure for the lost/stolen laptops at EOUSA's SOC since March 2013, also applicable to Recommendation 4; (c) sample screenshots of SCCM's

verification of completion of all applications prior to a laptop being released for use, as well as a copy of EOUSA Information Bulletin 136; and
(d) encryption verification of the 24 classified laptops in the classified laptop inventory.

3. Develop policies on the use of non-encrypted laptops for special use if such laptops are deemed necessary, and label these laptops accordingly.

Resolved. EOUSA concurred with our recommendation. EOUSA stated in its response that the special use laptops for its litigation support should be labeled accordingly as not encrypted.

This recommendation can be closed when we receive evidence of policies for the non-encrypted laptops for special use and the labeling of those special use laptops, such as pictures of the special use laptops with labels alerting users of their unencrypted status.

4. Document encryption verification in all EOUSA incident response tickets and disclose the encryption status to JSOC.

Resolved. EOUSA concurred with our recommendation. EOUSA stated in its response that it has implemented the encryption verification check at the EOUSA SOC as of March 2013.

This recommendation can be closed when we receive evidence of the implementation of the encryption verification procedure for incident response tickets for lost/stolen laptops and disclosure to JSOC.

5. Complete encryption scans on a routine basis and timely follow up on results of scans.

Resolved. EOUSA concurred with our recommendation. EOUSA stated in its response that its new TNA solution, mentioned in its response 2(a), centrally monitors the encryption status of all online systems on its network.

This recommendation can be closed when we receive evidence of the implementation of the TNA solution and samples of corrective actions taken, such as service tickets, on laptops identified as unencrypted from TNA's monitoring.

6. Identify unapproved laptops and remove them from use.

Resolved. EOUSA concurred with our recommendation. EOUSA stated in its response that its TNA solution detects devices on the network that do not contain an authorized configuration.

This recommendation can be closed when we receive evidence of actions taken on the unapproved laptops noted during the audit.

7. Complete a Security Authorization package (formerly known as Certification & Accreditation package) for all classified laptops and standalone computers and re-authorize them every 3 years in accordance with DOJ policy.

Resolved. EOUSA concurred with our recommendation. EOUSA stated in its response that it is working with JMD to enhance compliance with DOJ IT Security Standard 1.6.

This recommendation can be closed when we receive a copy of the completed Security Authorization package for the classified laptops and classified standalone computers.

8. Implement procedures to ensure that accurate, current, and reliable information is maintained in an official inventory for unclassified and classified equipment to help EOUSA to ensure that all required laptops are encrypted and deployed in compliance with DOJ policy.

Resolved. EOUSA concurred with our recommendation. EOUSA stated in its response that following acquisition all laptops are subject to inventory controls and recorded in DOJ's Unicenter Asset Portfolio Management (UAPM) system, and the SCCM tracks the laptops' status after imaging. In addition, the UAPM will track the classified laptops.

This recommendation can be closed when we receive evidence of (1) efforts to clean up the existing UAPM data file, such as removing duplicated serial numbers and machine names, correcting classification information, and filling in missing information; (2) formalized inventory control procedures that include how information from SCCM is to be reconciled to UAPM, and the role of districts in maintaining the inventory information in UAPM; and (3) the formalized procedure for maintaining the classified laptop inventory in UAPM.

9. Monitor and take action on electronic tablets with unauthorized application downloads and with outdated versions of the mobile operating system.

Resolved. EOUSA concurred with our recommendation. EOUSA stated in its response that it has started targeting electronic tablets with older mobile operating systems for upgrade and it has begun daily reporting of unapproved applications to USAO Systems Managers and EOUSA electronic tablet management, as well as to EOUSA's Information Systems Security team, which audits the reports and takes actions to have unapproved electronic tablet applications removed.

This recommendation can be closed when we receive evidence of EOUSA's actions in removing unauthorized application downloads and updating outdated mobile operating systems on electronic tablets, such as policies and service tickets for such corrective actions.

10. Develop comprehensive security policies and procedures for monitoring and handling electronic tablets.

Resolved. EOUSA concurred with our recommendation. EOUSA stated in its response that in addition to its response to Recommendation 9, where it has strengthened its internal management controls to maintain electronic tablets up-to-date, it is updating the United States Attorneys' Procedure (USAP) No. 3-16.200.006, "Requesting Mobile Application Approval," to emphasize that requests for new applications are required to clearly support the missions of the USAOs.

This recommendation can be closed when we receive a copy of updated USAP No. 3-16.200.006, as well as new policies on electronic tablet user termination and electronic tablet monitoring.

11. Implement each of the conditions of the February 11, 2013, waiver to ensure that all sensitive data are encrypted between USAOs and their consultants and expert witnesses.

Resolved. Although EOUSA stated in its response its position that it has properly operated under a waiver (written or oral) at all material times, it also stated that it is currently working with DOJ's Information Technology Security Staff on an updated waiver from PDG 08-04. Subsequent to receiving EOUSA's response to the draft report, JMD issued EOUSA a waiver, valid through December 31, 2014, that will allow it to develop and test a file

sharing solution for securing DOJ data between the USAOs and expert witnesses.

This recommendation can be closed when we receive evidence of the implemented file sharing solution.

12. Define roles of the attorneys, legal assistants, and contracting officers within the USAOs regarding contractor data security responsibility.

Resolved. EOUSA concurred with our recommendation. EOUSA stated in its response that it is considering making modifications to four USAPs in connection with this recommendation.

This recommendation can be closed when we receive the updated USAPs that clarify and define the roles of attorneys, legal assistants, and contracting officers within the USAOs regarding contractor data security responsibility, as well as notices to the USAOs for the implementation of these changes.

13. Increase its oversight of contractors to ensure that contractors: (1) are aware of and adhere to any security provisions required by the USAOs prior to starting work; (2) receive case information in an encrypted format; (3) implement sound business practices such as anti-virus software, password protection, and data destruction when the case data are not needed; and (4) instruct the sub-contractors about pass-through data security provisions.

Resolved. EOUSA concurred with our recommendation. EOUSA stated in its response that it is considering increasing the oversight of contractors to include the possibility of the use of training vehicles such as the annual Computer Security Awareness Training with Rules of Behaviors content for the contractors. EOUSA responded that its SOC monitors the use of antivirus software in its internal environment. EOUSA also cited USAP 3-13.200.004, "Media Disposal," which provides guidance for the secure disposal of electronic media and resulted in an in-house Data Destruction Center.

This recommendation can be closed when we receive evidence of (1) instruction to the USAOs for enhanced collection of signed contractor data waiver forms from the contractors prior to the start of contract work, (2) implementation of data protection requirements according to the new waiver for PGD 08-04, and (3) the implementation of training for the

contractors and sub-contractors for security awareness including the use of antivirus software, password protection, and proper data destruction.