THE CRIMINAL DIVISION'S LAPTOP COMPUTER ENCRYPTION PROGRAM AND PRACTICES

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

Audit Report 10-23
March 2010

THE CRIMINAL DIVISION'S LAPTOP COMPUTER ENCRYPTION PROGRAM AND PRACTICES

TABLE OF CONTENTS

	Page
INTRODUCTION	1
OIG Audit Approach	2
OIG Results in Brief	3
Background	4
FINDING AND RECOMMENDATIONS	10
The Criminal Division's Efforts to Ensure Safeguards Over DOJ Data on Laptop Computers Need Improvement	10
Laptop Computers Owned by the Criminal Division	10
Laptop Computers Owned by Contractors and Subcontractors	17
Recommendations	19
STATEMENT ON INTERNAL CONTROLS	21
STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS	22
APPENDIX I: OBJECTIVES, SCOPE, AND METHODOLOGY	23
APPENDIX II: ACRONYMS	25
APPENDIX III: CRIMINAL DIVISION'S RESPONSE	26
APPENDIX IV: OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT	31

THE CRIMINAL DIVISION'S LAPTOP COMPUTER ENCRYPTION PROGRAM AND PRACTICES

INTRODUCTION

Significant losses of sensitive data and personally identifiable information have occurred in both the government and in the private sector over the past few years.[1] For example, in May 2006 the Department of Veterans Affairs reported that a laptop computer containing personal information on approximately 26 million veterans and active duty military personnel had been stolen, and an investigation determined that the laptop was not encrypted.[2] In February 2009 a federal judge approved the government's plans to pay $20 million for out-of-pocket expenses for credit monitoring or physical symptoms of emotional distress to veterans exposed to possible identity theft resulting from the laptop loss.

In 2009, the Department of Justice Office of the Inspector General (OIG) issued a report on the Civil Division's laptop computer encryption program and practices in which we found significant weaknesses concerning unencrypted laptop computers used by its contractors, subcontractors, and vendors and other issues.[3] The Civil Division concurred with our findings and is in the process of implementing corrective action, including ensuring that laptop computers used to process Department of Justice (DOJ) data are encrypted.

As a result of our findings in the Civil Division report, we initiated this audit to assess the adequacy of laptop computer encryption deployment practices in the Criminal Division. The Criminal Division is responsible for prosecuting significant criminal cases of national interests such as organized crime, money laundering and narcotics,

---

[1] The term "personally identifiable information" refers to information that can be used to distinguish or trace individuals' identity, such as their name and social security number.

[2] Encryption is the use of algorithms (i.e., mathematically expressed rules) to encode data in order to render it readable only for the intended recipient.

[3] 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).

and dangerous drugs, and it treats all work processed on DOJ laptops as sensitive.

OIG Audit Approach

Our audit objectives were to determine whether the Criminal Division complies with federal and DOJ policies regarding: (1) the use of whole disk encryption on the laptop computers that Criminal Division employees, contractors, subcontractors, and other vendors use to process DOJ sensitive and classified information; and (2) encryption certification procedures for the laptop computers of contractors, subcontractors, and other vendors providing services to the Criminal Division.

The scope of our audit included two types of laptop computers: (1) laptops owned by the Criminal Division, and (2) laptops owned by contractors, subcontractors, and other vendors working for the Criminal Division. The laptop computers owned by the Criminal Division are mostly "pooled" laptops that are loaned to Criminal Division employees and to contractors on an as-needed basis. All Criminal Division-owned laptop computers are authorized to process "sensitive but unclassified" information.

During our audit, we interviewed officials within the Criminal Division, Justice Management Division (JMD), and contractor personnel with responsibility for encryption policy development and deployment practices. Additionally, we interviewed Procurement and Contracting Staff at JMD. Within the Criminal Division, we interviewed Contracting Officer's Technical Representatives (COTR), Criminal Division contractors and subcontractors, and attorneys regarding laptop data security practices.

As of November 5, 2009, the Criminal Division had 799 laptops listed in ARGIS, the Department's official property management system. We selected a sample of 40 laptops for testing and required that the Section Laptop Managers, who are responsible for laptop computers within their section, log on to these laptops. For this sample, we verified that encryption software was completely installed and that the installation date was documented within the software. We also followed up on a DOJ Computer Emergency Response Team

(DOJCERT) incident report in May 2009 by the Criminal Division that related to the loss of a laptop computer.[4]

We also tested non Criminal Division-owned laptops on two major contract types used by the Criminal Division, Mega 3 and the Offices, Boards, and Divisions (OBD 47) contracts for litigation support. We visited two off-site facilities to verify data security practices by a Mega 3 contractor and subcontractor.[5] From three Criminal Division sections, we selected 9 of 18 OBD 47 contractors to test contractor-owned laptops for the installation of whole disk encryption software.

OIG Results in Brief

Criminal Division-Owned Laptop Computers

Our review found that of the 40 laptops we tested for encryption software, 10 did not have encryption, and 9 of those 10 did not have Windows passwords enabled. All of the unencrypted laptops were in one Criminal Division section, the International Criminal Investigative Training Assistance Program (ICITAP), and all of those laptops contained sensitive departmental data.

In addition to our testing of laptops for encryption, we found weaknesses in other areas of the Criminal Division's laptop encryption program. We determined that at least 43 laptops did not comply with DOJ standards and Criminal Division requirements for laptop security settings.[6] Also, documentation was not maintained to verify the successful installation of whole disk encryption software for all laptop computers. In addition, the Criminal Division was unable to produce an accurate inventory of the universe of laptop computers it owns from ARGIS, DOJ's official property management system.

---

[4] DOJCERT is a reporting and tracking system that provides support of the resolution of issues that could disrupt working operations of the Department of Justice's Information Technology (IT) systems. DOJCERT is responsible for coordination and support of all response activities.

[5] The Criminal Division COTR and Mega 3 contractors stated that Mega 3 contracted litigation support providers do not use laptop computers. Therefore, we did not have any Mega 3 laptops to test.

[6] As we explain in detail in the Baseline Configuration Section of this report, we confirmed with Information Technology Management that 43 laptops were not in compliance with DOJ requirements.

Non-Criminal Division-Owned Laptop Computers

We found serious deficiencies with the OBD 47 contractor-owned laptops. Specifically, seven out of nine OBD 47 contractors we tested processed sensitive Department data on laptops without encryption.

In addition to our testing of contractor laptops for encryption, we found weaknesses in oversight of data security policies for the Criminal Division's contractors. For both the Mega 3 and OBD 47 contracts, we found that these contracts did not have the required security clause requiring encryption, and the Criminal Division had not implemented alternative controls to compensate for the contract deficiencies.

Background

The Criminal Division develops, enforces, and supervises the application of federal criminal laws, except those specifically assigned to other components such as the Antitrust, Civil Rights, Environment and Natural Resources, and Tax Divisions. The Criminal Division and the 93 U.S. Attorneys have the responsibility for overseeing criminal matters under more than 900 statutes as well as certain civil litigation. In addition to its direct litigation responsibilities, the Criminal Division formulates and implements criminal enforcement policy.

The Criminal Division also approves or monitors sensitive areas of law enforcement, such as participation in the Witness Security Program and the use of electronic surveillance; advises the Attorney General, Congress, the Office of Management and Budget (OMB), and the White House on matters of criminal law; provides legal advice and assistance to federal prosecutors and investigative agencies; and provides help to coordinate international as well as federal, state, and local law enforcement matters.

As of January 2010, the Criminal Division had 747 full-time employees on-board. It is comprised of but not limited to the following sections: Organized Crime and Racketeering Section (OCRS); Asset Forfeiture and Money Laundering Section (AFMLS); Fraud Section (FRD); Computer Crime and Intellectual Property Section (CCIPS); International Criminal Investigative Training Assistance Program (ICITAP); Domestic Security Section (DSS); Child Exploitation and Obscenity Section (CEOS); Office of Overseas Prosecutorial Assistance, Development and Training (OPDAT); Narcotic and Dangerous Drug Section (NDDS); and Office of Enforcement Operations (OEO).

The Criminal Division's Information Technology Management group is responsible for the implementation and oversight of laptop security throughout the Division. The Information Technology Management staff installs encryption software for Criminal Division laptops and provides technical support.

In its work, the Criminal Division uses contractors, subcontractors, and other vendors (such as expert witnesses, specialists, and consultants) to assist with its wide range of duties. The two major contract types used by the Criminal Division to obtain litigation support services are the Mega 3 and the OBD 47 contracts.[7] Contracted litigation support providers help acquire, organize, develop, and present evidence throughout the litigation process.

During our audit, we requested from the Criminal Division a list of contractors supporting the Division. In December 2009, the Criminal Division provided us with a list of 168 full-time contractors. This list included some Mega 3 contractors, but the Criminal Division was unable to provide an accurate number of Mega 3 contractors from the list of 168 contractors during audit field work.

In order to identify an accurate number of OBD 47 contractors, we requested a list from the Criminal Division's Office of Administration (ADMIN). We also selected a sample of three sections (Fraud, Asset Forfeiture and Money Laundering, and Office of Special Investigations) to review OBD 47 contractor compliance with the DOJ Procurement Guidance Document (PGD) 08-04, and we received separate contracting lists from each of these three sections. However, we noted a material difference between the list provided by ADMIN and the section specific lists. Specifically, the three sections sampled for OBD 47 review provided us with 24 contracts, but 8 of those 24 contracts were not included on the list provided by ADMIN. These 24 contracts covered 18 distinct OBD 47 contracting entities.[8] Therefore, the ADMIN provided list is not a complete and accurate account of the OBD 47 contracts. Subsequently, the Criminal Division was unable to confirm an accurate number of OBD 47 contractors.

---

[7] The Mega 3 contracts provide automated litigation support services and the OBD 47 contracts are used to procure the services of expert witnesses or litigation consultants. See Appendix I, Objectives, Scope, and Methodology for more details.

[8] Our testing of OBD 47 contractors (individuals and companies) differs from the total number of contracts reviewed because an OBD 47 contractor may be responsible for working on multiple contracts.

Laptop Encryption Policy within the DOJ

DOJ Order 2640.2F establishes laptop encryption policy for DOJ employees and contractors. Chapter 2, section 12 states that information on mobile computers or devices (e.g., notebook computers, personal digital assistants) and removable media shall be encrypted using a National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) 140-2 validated or National Security Agency (NSA) approved encryption mechanisms.

Laptop Encryption Policy for Contractors

On March 20, 2008, the Department's Senior Procurement Executive issued DOJ PGD 08-04, Security of Systems and Data, Including Personally Identifiable Information. PGD 08-04 contains a security clause addressing Department systems and data, including provisions 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 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, and 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 the following requirements:

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;

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 Information Technology (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 DOJ Contracting Officer within 15 days of termination of contractor work.

These requirements also apply to all subcontractors who perform work in connection with Department contracts. For each subcontractor, the contractor must certify that it has required the subcontractor to adhere to all such security requirements. Any breach by a subcontractor of any of the provisions is attributable to the contractor.

According to PGD 08-04, all current Department contracts must be modified to include the applicable clause within 60 days of the date of the issuance of the guidance, which was March 20, 2008, after which, laptops or devices not covered by certification letters may not be used on DOJ contracts. 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.

According to the Senior Procurement Executive, permission for a deviation or waiver is only granted in unusual circumstances.

Civil Division's Request for a Waiver of Implementation of PGD 08-04, "Civil Waiver"

In July 2008, in response to the PGD 08-04 document, the Civil Division issued a memorandum to the Senior Procurement Executive requesting an exemption from the requirement to incorporate the security clause into the Mega 3 contractors on behalf of all litigating components, which includes the Criminal Division.

In January 2009, the Senior Procurement Executive granted a waiver to exempt the security clause from being incorporated into the Mega 3 contracts after the Civil Division provided the following requirements to ensure that data security measures were implemented and enforced for the Mega 3 contracts:

1. data security guidance and instructions that were issued to vendors;

2. written acknowledgement from the contractors that they have received and accepted that data security guidance and instructions;

3. a statement by contractors agreeing to provide the data security guidance and instructions to all applicable employees and subcontractors and to provide adequate security training; and

4. a more detailed description of the steps that were taken and would be taken to ensure that data security measures are implemented and enforced.

As requested, the Civil Division provided documentation to JMD on how the Civil Division would meet the IT security requirements for Mega 3 contracts only. The Senior Procurement Executive did not address any other contract vehicles other than Mega 3 contracts in his January 2009 memo. As a result, the waiver only applied to the Mega 3 contracts and did not apply to the OBD 47 contracts.

During our audit of the Criminal Division, JMD informed us that the waiver applied to all litigating divisions. However, the Criminal

Division officials were unaware of the PGD 08-04 security clause and the waiver.

Impact of the Waiver

Although the Civil Division was granted the waiver for the Mega 3 contracts on behalf of all litigating Divisions, including the Criminal Division, the revised Rules of Behavior for the Mega 3 contracts still required that contractors encrypt all Departmental data stored on laptops and on removable media being transported outside the Department's physical perimeter. Therefore, regardless of the waiver, Mega 3 contractors, subcontractors, and vendors are still required to encrypt all laptop computers processing DOJ data.

FINDING AND RECOMMENDATIONS

The Criminal Division's Efforts to Ensure Safeguards Over DOJ Data on Laptop Computers Need Improvement

We found that for laptops owned by the Criminal Division: (1) at one Criminal Division section, ICITAP, laptop computers used to process sensitive DOJ data were not encrypted; (2) at two Criminal Division sections (ICITAP and CCIPS), baseline configurations were not consistent with DOJ requirements for all laptop computers used to process DOJ data; (3) the Criminal Division did not maintain documentation to verify the successful installation of whole disk encryption software for all laptop computers; and (4) the Criminal Division did not maintain a complete and accurate laptop inventory in ARGIS.

In addition, the Criminal Division's efforts to ensure contractor safeguards over DOJ data need immediate attention to correct significant weaknesses. We found that: (1) contractor laptops used to process sensitive DOJ data were not encrypted; and (2) the Criminal Division did not provide sufficient oversight regarding the enforcement of data security measures for OBD 47 and Mega 3 contracts.

Laptop Computers Owned by the Criminal Division

Encryption Test Results

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. In accord with this Order, information on mobile computers/devices (e.g., notebook computers, personal digital assistants) and removable media must be encrypted using FIPS 140-2 validated or 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.

The Criminal Division's Standard Operating Procedures (SOP), Stand Alone Laptop PC Management Version 4.2, requires that the Division's laptop System Administrator install PointSec hard drive encryption software on each laptop.

To test the encryption of Criminal Division laptops, we sampled 40 laptop computers from 7 Criminal Division sections. Our tests found that laptops within the Criminal Division's International Criminal Investigative Training Assistance Program (ICITAP) section were not encrypted. However, each of the laptop computers we tested in the other six Criminal Division sections were encrypted.

We noted that all 10 of the sampled ICITAP laptops used to process DOJ Data were not encrypted.[9] In addition to not having whole disk encryption, the laptops contained DOJ documentation such as reports, a management video, and field notes for ICITAP work. For example, the laptops included the following data:

- Attorney General Weekly Submission-Iraq Program;
- International Development and Training Programs - Iraq Program Update, was marked for Internal Distribution Only;
- Iraqi Program Accomplishments report based on Police, Corrections, and Commissions on Public Integrity; and
- Pakistan Program Management Evaluation Report.

We asked ICITAP and Information Technology Management officials whether they were aware that sensitive DOJ data was stored on these laptops. ICITAP officials stated that these laptops were in use by ICITAP staff, but they were unaware of what files were stored on the laptops and the nature of their sensitivity. Information Technology Management officials stated that they were unaware that the laptops were unencrypted.

We also asked for the procurement documentation for the 10 ICITAP unencrypted laptops from the Criminal Division's ICITAP and Information Technology Management sections. However, they were unable to provide the OIG with information regarding the procurement

[9] These laptops were selected because we considered them to be high risk since they were not listed on Information Technology Management's laptop loaner pool inventory and therefore they may not have received Information Technology Management oversight.

of the 10 unencrypted laptops. ICITAP and Information Technology Management informed us that they would search for the purchase orders for the unencrypted laptops. However, we received an e-mail from a member of the Information Technology Management staff indicating that the purchase orders could not be found by either section.

Additionally, ICITAP officials informed the OIG that they believed the laptops went through Criminal Division's Information Technology Management as directed by Criminal Division policy. However, Information Technology Management was unable to determine whether the laptops came through their section prior to use for proper configuration including encryption. Although Information Technology Management is responsible for maintaining oversight of laptop security throughout the Division, it was unaware that these laptops did not receive the approved configuration baseline.

Baseline Configuration Non-Compliance

Criminal Division, Information Technology Management SOP, Stand Alone Laptop PC Management Version 4.2, requires that the laptop System Administrator keep laptop images up to date. If major hardware and software updates are needed, a Change For Request must be submitted and a new image must be created.

DOJ Order 2640, 2F Section 5, Technical Security Policy, states that in accordance with DOJ IT Security Standard – Identification and Authentication (IA) Control, component IT systems shall identify: IT system users; processes acting on behalf of users; or devices, and that component IT systems shall authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to component IT systems.

DOJ Information Technology Security Standard, Access Control Version 2.2 (control AC-08), requires that all DOJ systems display an approved notification message before granting access to the system. The warning banner is required to be designed to remain on the laptop computers' screen until the user logs on to the information system. The warning banners are required to be designed to alert potential system users that they are about to access a federal government system. Additionally, the banner must warn the potential user of DOJ system access criteria and ramifications for illegal and unauthorized system use. The warning banner also should contain DOJ's privacy and security notices.

Baseline configurations provide information about the standard software loaded for a workstation or notebook computer including updated patch information. Also, baseline configurations provide minimum information system settings such as password length and composition.

We selected a sample of laptops for testing based on the number of laptops in each section and the sensitivity of the type of work performed in that section. Specifically, we tested 5 laptops each from the Computer Crimes and Intellectual Property section (CCIPS), Fraud, AFMLS, OPDAT, Office of Enforcement Operations, and Narcotics and Dangerous Drug Section, and 10 from ICITAP.

We found that laptops imaged at CCIPS and ICITAP do not have the Information Technology Management approved baselines installed. Specifically, we noted that of the 40 laptops we tested:

- 4 CCIPS and 10 ICITAP laptops did not display a warning banner.

- 9 ICITAP laptops did not require a Windows password to access the system.

During our testing, we noted that four of the five laptops selected for sampling at CCIPS did not display a warning banner. CCIPS stated that laptop computers are re-imaged between usages. However, we subsequently learned that the images that are used were not provided by the Criminal Division's Information Technology Management section as required by policy. Instead, CCIPS created an image used for their laptops that does not meet the approved DOJ configuration baselines.

During our testing, an Information Technology Management official became aware of this issue. Based on our results, Information Technology Management staff scanned the CCIPS laptops to review the configuration settings. The result of those scans concluded that the CCIPS image was not in compliance with DOJ requirements, including maintaining audit logs, password length, and password complexity. CCIPS informed us that 33 laptops were imaged incorrectly, including 4 of 5 we tested.

We were informed by a CCIPS official that the section had re-imaged its own laptops based on the need for its attorneys to access

particular applications and run programs that require administrative access that Information Technology Management's image does not allow. According to CCIPS, it received authorization from Information Technology Management to perform the re-imaging of its laptops. We requested verification of this authorization from Information Technology Management and CCIPS; however, neither was able to provide us with documentation to substantiate this agreement.

ICITAP also had configuration issues with each of the 10 laptops we tested. Information Technology Management officials informed us that they have removed all laptops from operation for further analysis, as directed by the Criminal Division's Chief Information Officer. After performing scans of the ICITAP laptop computers baseline configurations, an Information Technology Management official informed us that the laptops did not meet DOJ requirements such as whole disk encryption, audit logs, password length, and password complexity.

During our testing at ICITAP, we also found Limewire, an unauthorized software program, installed and running on one of the unencrypted ICITAP laptop computers. Limewire is a free peer-to-peer file sharing client that makes computers vulnerable by allowing unauthorized access. Limewire may also allow access to any file on a user's computer, including documents with personal information or DOJ sensitive data, and it allows the dissemination of potentially harmful viruses and malware.[10] For example, a laptop with Limewire may allow an unauthorized user to obtain confidential reports such as the International Development and Training Programs-Iraq Program Update discussed previously. Publicly accessible peer-to-peer file sharing technology is not permitted according to the DOJ IT Security Standards, Systems and Services Acquisitions.

ICITAP officials were unaware that the unauthorized Limewire software had been installed on the laptop computer. As a result of our testing, Information Technology Management recalled the 10 ICITAP laptops we tested for further analysis, and it plans to surplus or re-image the laptops.

[10] Malware refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, and availability of the victim's data, application, or operating system. Malware has become the most significant external threat to most systems, causing widespread damage and disruption, and requiring extensive recovery efforts.

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.

Based on our review of a DOJCERT incident that involved the theft of an unencrypted laptop computer in May 2009 from the trunk of an attorney's car from the Criminal Division's Fraud section, we found that Criminal Division laptop encryption records are not maintained. We met with Information Technology Management staff to determine the stolen laptop's level of encryption. Information Technology Management staff stated that it does not allow any unencrypted laptop computers to be deployed; however, they could not provide documentation showing evidence when or if the encryption software was installed on any laptop. As a result the Criminal Division is unable to provide sufficient evidence that encryption software was appropriately installed.

We contacted the attorney whose laptop was stolen in May 2009. The attorney reported that he believed the laptop was encrypted and that multiple layers of authentication were required to access the laptop, including PointSec encryption software. The attorney and Information Technology Management staff further stated that little to no DOJ data was stored on the laptop. The attorney stated that the data was saved to a U.S. Attorney-issued biometric thumb drive, which was not stolen and that any information left on the laptop was limited since the laptop was recently put into service.

Based on our results, Information Technology Management staff plan to add a field within their internal database to track laptop encryption installation on all Criminal Division laptops.

Laptop Inventory Discrepancies

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 resources management and information technology, be maintained to an appropriate level of detail.

We reviewed several laptop inventories from the Criminal Division during this audit. Information Technology Management staff provided us two lists: the first from their internal inventory, which includes its laptop loaner pool, and the second from ARGIS, which is the Department's official property management system. In addition, two out of the seven Criminal Division sections we reviewed maintained their own independent inventories and provided us with copies of the inventories. The other five sections did not maintain their own inventories. We noted several discrepancies between ARGIS and the two sections (ICITAP and CCIPS) that maintained internal inventories.

Initially, the Criminal Division provided the audit team with the DOJ's official inventory from ARGIS. As of November 5, 2009, we noted that the Criminal Division had 799 laptops.

We compared the ARGIS inventory to the Information Technology Management's internal laptop loaner pool inventory, which tracks specific laptops used by Criminal Division's employees, contractors and vendors performing work across all sections. All laptops on the Information Technology Management's laptop loaner pool inventory reconciled with ARGIS.

We then reconciled ARGIS to ICITAP's two internal inventory lists, one for Information Technology Management-provided laptops for ICITAP Headquarters and another for laptops that are provided to foreign field offices through a State Department-funded program. While reviewing both ICITAP inventories, we noted initially that at least one laptop was not included in the ARGIS inventory. This one laptop was eventually found on the ARGIS inventory by the Criminal Division; it was documented erroneously on the list. However, after bringing this to ICITAP's attention, further inspection by ICITAP revealed that 11 of their laptops were not in the ARGIS inventory. To perform their inspection, ICITAP used a more updated list than the one we were originally provided. An ICITAP official explained that laptops may have been dropped from the ARGIS system due to system or operator error.[11]

We also reconciled ARGIS to CCIPS's internal inventory of laptops and found discrepancies. Specifically, nine laptops on the

[11] According to the Criminal Division, ARGIS is known to randomly purge records, resulting in inaccurate inventories. The Department is seeking to replace the ARGIS system in the near future.

CCIPS inventory were not listed in ARGIS. According to CCIPS, it does not have access to ARGIS and therefore did not reconcile their internal list to ARGIS.

Without an accurate accounting in the officially approved inventory, the Criminal Division is unable to ensure that all required laptop computers are encrypted and deployed compliant with DOJ policies.

Laptop Computers Owned by Contractors and Subcontractors

OBD 47 Contractor Compliance with PGD 08-04

As previously discussed in the background section of this report, the DOJ PGD 08-04 document requires that laptops must employ encryption using a FIPS 140-2 approved product. The document also states that the contractor agrees that in the event of any 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 COTR.

During our audit, we sampled laptops in 9 of 18 OBD 47 contractors in the Fraud Section, Asset Forfeiture and Money Laundering Section (AFMLS), and Office of Special Investigations located in Washington, DC; Boston; New York; and Miami. We found that:

- The OBD 47 contracts did not contain the required PGD 08-04 clause;
- Seven of the nine contractors we sampled processed DOJ data on laptops that were not encrypted;
- The Criminal Division did not provide sufficient oversight of data security on the contractors' laptops. The Criminal Division did not provide DOJ requirements to the OBD 47 contractors regarding standard policies and procedures regarding data security, including encryption requirements and procedures for addressing data breaches.

Specifically, on our testing of the OBD 47 contractors, we found unencrypted laptops that contained sensitive DOJ data such as case

related files containing information on financial corruption, medical records, and information involving genocide. We found that in some cases, the laptops may have been used by contractors' family members for personal use.

Furthermore, these OBD 47 contractors did not receive specific guidance and oversight from the Criminal Division regarding data security measures. By not enforcing the PGD 08-04 clause for its contract employees, we concluded that the Criminal Division is placing DOJ data at high risk to loss, corruption, or disclosure.

Mega 3 Contractor Compliance with PGD 08-04

The Criminal Division also uses three Mega 3 contractors: CACI International Incorporated, Labat-Anderson Incorporated, and Lockheed Martin. We reviewed the contracting documentation and waiver implementation for these contractors and performed interviews and site visits.

We found that the Criminal Division's Mega 3 contracts do not comply with the PGD 08-04 clause. As noted above, these contracts have a waiver; however, this waiver requires that alternate security measures be implemented. Although the Mega 3 contractors at the Criminal Division do not use non-DOJ laptops, they are still required to satisfy other requirements. For example, the Criminal Division should be issuing security guidance, maintaining signed rules of behavior, and conducting site visits of contractor facilities as a part of the provisions of the waiver. Based on our review, the Criminal Division is providing limited security guidance to the Mega 3 contractors and maintaining signed rules of behavior. However, we noted that the Criminal Division is not conducting site visits in accordance with the oversight procedures specific to the waiver for Mega 3 contractors.

When we asked the Criminal Division whether it had implemented measures to satisfy compliance with the waiver, the Criminal Division COTR was unaware that any oversight procedures were required.

We also conducted two site visits (one Mega 3 contractor and one subcontractor) to test Criminal Division's oversight of the Waiver provisions. We found that:

- The Criminal Division was not conducting site visits to determine compliance with DOJ requirements;
- There were no locks on the subcontractors' rooms where they process DOJ information; and
- Standalone computers used to process information were not secured via password-protected screensavers.

In sum, we found that contractors performing work for the Criminal Division are not securing data in accord with DOJ requirements. We believe that, by not enforcing the Waiver, the Criminal Division is placing DOJ data at high risk of loss, corruption, or disclosure.

Recommendations

As a result of the issues identified in this report, we make 1 recommendations to the Criminal Division to enhance its safeguards over DOJ data on laptop computers.

We recommend that the Criminal Division:

1. Ensure that all current Criminal Division-owned laptops are encrypted.
2. Provide all laptops to Information Technology Management staff for encryption prior to use.
3. Formalize laptop procurement procedures to ensure that laptops are appropriately inventoried, encrypted, and processed through Information Technology Management per Criminal Division policy.
4. Ensure that the Information Technology Management staff approves baseline configurations using DOJ standards on all laptops used for DOJ processing.
5. Ensure that a record of encryption is maintained for all Criminal Division-owned Laptops.

6. Enhance procedures for ensuring that the official inventory database, ARGIS, maintains accurate and reliable information for all Criminal Division-owned laptop computers.

7. Ensure that all contractor-owned laptop computers used to process DOJ data are encrypted or require contractors to use encrypted Criminal Division provided hardware.

8. Ensure that Criminal Division contract support providers are aware of security procedures for handling DOJ data in accordance with DOJ policy.

9. Implement the PGD 08-04 clause in all OBD 47 contracts.

10. Implement the conditions of the waiver pertaining to the PGD 08-04 clause for Mega 3 contracts.

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 Criminal Division's internal controls was not made for the purpose of providing assurance on its internal control structure as a whole. The Criminal Division'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 Criminal Division'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 Criminal Division'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 Criminal Division's internal control structure as a whole, this statement is intended solely for the information and use of the Criminal Division 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 Criminal Division'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 Criminal Division'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 Criminal Division 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 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 Criminal Division's compliance with the aforementioned laws and regulations that could have a material effect on the Criminal Division's operations. We interviewed key personnel within the Criminal Division, as well as performed a physical review on selected Criminal Division-owned laptop computers. Additionally, we contacted a select group of vendors contracted to provide litigation support services to the Criminal Division.

As noted in the Finding section of this report, we found that some of the tested Criminal Division-owned laptop computers were not encrypted as required by DOJ policy. Also, improvements are needed with the Criminal Division's laptop computer program and practices in the areas of laptop inventory and warning banners. Finally, significant improvements are required on the use of non-Criminal Division laptop computers by litigation support providers.

OBJECTIVES, 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.

This audit was performed to assess the Criminal Division's laptop computer encryption program and practices. Specifically, our audit objectives were to determine whether the Criminal Division complies with federal and DOJ policies regarding: (1) the use of whole disk encryption on employees', contractors', subcontractors', and other vendors' laptop computers used to process DOJ sensitive and classified information; and (2) laptop computers' encryption certification procedures for contractors, subcontractors, and other vendors providing services to the Criminal Division.

Our audit covered a 6-month period from July through December 2009. We performed our fieldwork on-site at the Criminal Division's offices in Washington, D.C. and conducted site visits at contractor offices in Washington, D.C.; New York, NY; Boston, MA; and Miami, FL. During the audit period, we interviewed Criminal Division contractor personnel with responsibilities related to encryption policy development, data security, and deployment practices.

In addition, we met with the COTR responsible for finalizing contractual agreements between service vendors, JMD staff, and Criminal Division procurement and asked questions regarding contractual security requirements for laptop computers. We also reviewed the Criminal Division's contract documents for litigation support services.

Our testing of Criminal Division laptop computers was conducted by selecting a sample of 40 of the 799 Criminal Division's laptop computers identified within the official ARGIS database. This non-statistical sample design does not allow projection of the test results to all laptops.

We also met with Criminal Division's Mega 3 contractors and OBD 47 contractors that perform litigation support services to determine if the Criminal Division is performing contractor oversight.

The Mega 3 contracts were awarded to three primary contractors: CACI International Inc., Labat-Anderson Incorporated, and Lockheed Martin. In addition to meeting with these three contractors, we also met with Lockheed Martin's subcontractor L-Discovery. The Criminal Division COTR and Mega 3 contractors stated that Mega 3 contracted litigation support providers do not use laptop computers. Therefore, we did not have any Mega 3 laptops to test.

We interviewed 9 of 18 OBD 47 contractors, which covers 15 of 24 DOJ contracts, and reviewed their laptops. The Criminal Division informed the audit team that OBD 47 contractors did not use Criminal Division-owned laptop computers to process Criminal Division data.

ACRONYMS

ADMIN	Office of Administration
AFMLS	Asset Forfeiture and Money Laundering Section
CCIPS	Computer Crime and Intellectual Property Section
CEOS	Child Exploitation and Obscenity Section
COTR	Contracting Officer's Technical Representative
DOJ	Department of Justice
DOJCERT	Department of Justice Computer Emergency Readiness Team
DSS	Domestic Security Section
FIPS	Federal Information Processing Standards
ICITAP	International Criminal Investigative Training Assistance Program
JMD	Justice Management Division
NDDS	Narcotic and Dangerous Drug Section
NSA	National Security Agency
OBD	Offices, Boards, and Divisions
OEO	Office of Enforcement Operations
OIG	Department of Justice Office of the Inspector General
OMB	Office of Management and Budget
OPDAT	Office of Overseas Prosecutorial Assistance, Development and Training
PGD	Procurement Guidance Document
SOP	Standard Operating Procedures

CRIMINAL DIVISION'S RESPONSE

U.S. Department of Justice

Criminal Division

Washington, D.C. 20530

March 26, 2010

MEMORANDUM

TO: Raymond J. Beaudet
Assistant Inspector General
Office of the Inspector General

FROM: Karl Maschino
Acting Executive Officer
Criminal Division

SUBJECT: Responses to OIG Draft Audit Report: *The Criminal Division's Laptop Computer Encryption Program and Practices*

This memorandum outlines the Criminal Division's response to the recommendations set forth in the Draft Audit Report issued by the Office of the Inspector General (OIG) on March 10, 2010. The Criminal Division appreciates all of the work undertaken by OIG in auditing the Criminal Division's encryption policies and practices, and agrees with the recommendations set forth in the draft Report, subject to the clarifications detailed below. The Division recognizes the importance of safeguarding Department information and, for that reason, has taken immediate mitigative steps to address the issues identified in this Audit.

As an initial matter, the Criminal Division wishes to emphasize that less than two percent of all Division-owned laptops were found to be non-compliant with encryption requirements, and the Division believes that this limited encryption-related non-compliance was confined entirely to one section as a result of an isolated occurrence several years ago. Moreover, with respect to the other information security issues identified in the draft Report, including those pertaining to baseline configurations and procurement, the Division believes the incidence of such issues was similarly limited. Regardless, steps have been taken to bring all identified non-compliant laptops into full compliance and to ensure full compliance going forward. Our efforts in this regard are outlined below.

Responses to Recommendations

The OIG made 10 recommendations to the Criminal Division to enhance the Division's safeguards over Department data on laptop computers. The OIG's recommendations reflect and build upon the longstanding policies of the Criminal Division, and consistent with the OIG's

recommendations, the Division has recently taken additional steps to improve its ability to protect and secure Department information on Division-owned and contractor-owned laptops.

Recommendation 1. Ensure that all current Criminal Division-owned laptops are encrypted.

The Criminal Division has a longstanding policy of encrypting Division-owned laptops prior to use. The Criminal Division believes that the unencrypted laptops found in one Criminal Division section were the result of an isolated purchase that took place years ago. All laptops identified during the OIG Audit as unencrypted have since been reimaged and encrypted, or excised.

To help facilitate and achieve one hundred percent compliance going forward, the Division has recently developed Standard Operating Procedures (SOPs) for laptops. The SOPs clearly define the steps necessary to ensure that the Division's laptops are 1) inventoried appropriately in the Department's inventory system (ARGIS);[1] 2) loaded with baseline configurations using DOJ standards; and 3) running encryption software. In addition, the SOPs also require that the Information Technology (IT) Security Manager validates the encryption of each laptop and keeps a record of this action. Each of these steps is completed prior to deploying the laptop for Division use.

Recommendation 2. Provide all laptops to Information Technology Management staff for encryption prior to use.

All IT equipment is purchased in coordination with Information Technology Management (ITM) staff. The Criminal Division's practice in this regard is structured so that ITM can exercise control over laptops that are purchased by the Division, thereby ensuring minimum requirements and baseline configurations are applied. Recently, Criminal Division leadership has strongly re-emphasized this policy. Further, as stated above, the recently developed SOPs also require that all laptops be provided to ITM staff for encryption prior to use.

Recommendation 3. Formalize laptop procurement procedures to ensure that laptops are appropriately inventoried, encrypted, and processed through Information Technology Management per Criminal Division policy.

The new SOPs ensure that Department policy and security requirements are followed for the implementation, administration, maintenance, and support of laptop management.

---

[1] ARGIS, the Department's official property management system, is known to randomly purge records, resulting in inaccurate inventories. For this reason and others, the Department is seeking to replace the ARGIS system with a more user-friendly and reliable system in the near future. In the meantime, to address this systemic problem with ARGIS, Criminal Division staff will conduct routine inventory verifications to identify and correct any inconsistencies that result from this problem with ARGIS.

Recommendation 4. *Ensure that the Information Technology Management staff approves baseline configurations using DOJ standards on all laptops used for DOJ processing.*

The recently developed SOPs ensure that laptops are encrypted and imaged using the minimum requirements and baseline configuration in accordance with DOJ standards. These actions will be validated by the IT Security Manager when he/she reviews each laptop prior to its deployment, ensuring this baseline configuration and encryption.

To remedy the baseline configuration-related departures from policy identified in the draft Report, a one hundred percent inventory was completed. All identified non-compliant laptops have now been re-imaged and verified to be consistent with DOJ requirements, including the Criminal Division Minimum Configuration Checks, v1.0.

Recommendation 5. *Ensure that a record of encryption is maintained for all Criminal Division-owned laptops.*

The recently developed laptop SOPs require that each Criminal Division-owned laptop receives a validation of its encryption when the laptop is deployed. Going forward, Criminal Division-owned laptops will also be subject to random checks annually, and a record of those checks will be maintained by ITM staff.

Recommendation 6. *Enhance procedures for ensuring that the official inventory database, ARGIS, maintains accurate and reliable information for all Criminal Division-owned laptop computers.*

As stated above, Criminal Division administrative management is re-emphasizing that all IT purchases must be made in consultation with ITM staff. In keeping with the recently developed SOPs regarding laptop management, all IT equipment will be inventoried in ARGIS and will receive baseline configurations, using DOJ standards and encryption, prior to being deployed. In addition, the ARGIS inventory will be checked on a periodic basis to audit system counts and correct any random purges, as discussed above. The Criminal Division also encourages the Department to continue to explore the identified issues presented by the ARGIS system.

Recommendation 7. *Ensure that all contractor-owned laptop computers used to process DOJ data are encrypted or require contractors to use encrypted Criminal Division provided hardware.*

As outlined in the Department's PGD 08-04 Guidance, all work performed by off-site contractors for the Criminal Division is required to be stored on an encrypted device. To facilitate compliance with this requirement, the Division has adopted a new practice involving

the issuance of an encrypted USB storage device by ITM staff to each contractor who needs computer resources to process Department information. In order to comply with the Department's encryption requirements, all contractors must abide by the following rules when using encrypted USB storage devices:

- all information being produced for the Criminal Division must be stored on the USB-encrypted storage device issued by the Division's ITM staff;
- no information may be copied from the device to the computer being used;
- timely notice of any inadvertent departure from the above rules must be made to the ITM staff.

Finally, off-site contractors working for the Criminal Division must sign and return (within 10 business days) a consent form, whereby the contractor agrees to the terms and conditions set forth in the form and DOJ's PGD 08-04 Order. These contractors also receive a detailed memo from the Criminal Division's Contracting Officer containing rules, instructions, and the signature sheet to be returned, as well as an attachment outlining the PGD 08-04 guidance.

Recommendation 8. *Ensure that Criminal Division contract support providers are aware of security procedures for handling DOJ data in accordance with DOJ policy.*

As stated above, off-site contractors working for the Criminal Division must sign and return (within 10 business days) a consent form, whereby the contractor agrees with the terms and conditions set forth in the form and DOJ's PGD 08-04 Order. These contractors also receive a detailed memo from the Criminal Division's Contracting Officer containing rules, instructions, and the signature sheet to be returned, as well as an attachment outlining the PGD 08-04 guidance.

Recommendation 9. *Implement the PGD 08-04 clause in all OBD 47 contracts.*

As stated above, the Criminal Division has issued guidance that all work performed by off-site contractors for the Division is required to be stored on an encrypted device. This guidance also outlines the rules of behavior by which the off-site contractors must abide when using the encrypted devices. Before beginning work for the Division, contractors are asked to certify that they understand and will comply with these rules of behavior. This change will ensure that all OBD 47 contracts are in compliance with the PGD 08-04.

Recommendation 10. Implement the conditions of the waiver pertaining to the PGD 08-04 clause for Mega 3 contracts.

The Criminal Division requires that each of its Mega 3 contractors sign rules of behavior agreements that outline the DOJ security requirements as they apply to processing Division information. The Division re-emphasized these requirements to all of its current Mega 3 contractors. As for issues pertaining to site visits, it is stated in the temporary waiver that any site visits will be performed and overseen by the Civil Division. The Criminal Division is thus working in conjunction with both the Civil Division and the Department more broadly to ensure compliance with regulations related to site visits.

Note: Appendix A of the Criminal Division Management's response was omitted at the request of the Criminal Division because it contained sensitive information.

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

The OIG provided a draft of this audit report to the Criminal Division and their comments on the findings and recommendations were considered in preparing this Analysis and Summary of Actions Necessary to Close the Report. The Criminal Division's response is incorporated as Appendix III of this report. In its response, the Criminal Division concurred with our recommendations and discussed the actions it will implement in response to our findings.

We address later in this appendix the specific responses to each of our recommendations and the actions necessary to close the recommendations. First, however, we respond to comments in the Criminal Division's response that did not pertain to a specific recommendation.

Analysis of the Criminal Division Response

In response to our draft audit report, the Criminal Division stated that less than 2 percent of all Division-owned laptops were found to be non-compliant with encryption requirements and that it believed that this limited encryption-related non-compliance was confined entirely to one section as a result of an isolated occurrence several years ago. We do not agree that our audit found that less than 2 percent of all Division-owned laptops were non-compliant. We tested 40 of the 799 Criminal Division-owned laptops and found that 10 out of 40 laptops (25 percent) were not encrypted. The Criminal Division is correct that all 10 of the non-compliant laptops were in one section, and it may also be correct that this was the result of an isolated occurrence several years ago. However, our report is careful not to project the results of our non-statistical sample to the universe of 799 Criminal Division-owned laptops. Similarly, it cannot be assumed that the 759 Criminal Division-owned laptops we did not test are in fact encrypted.

The Criminal Division's response does not discuss the more significant lack of encryption issue we identified with respect to contractor-owned laptops. We reported that seven of the nine contractors we tested processed DOJ data on unencrypted laptops. This is a troubling issue that must be quickly addressed. In addition, our finding on improper baseline configurations was not limited to an isolated occurrence. In fact, two sections were found to have baseline configuration issues.

Summary of Actions Necessary to Close the Recommendations

1. **Resolved.** The Criminal Division concurred with the OIG's recommendation to ensure that all current Criminal Division-owned laptops are encrypted. This recommendation can be closed when the Criminal Division provides relevant SOPs to the OIG for review and evidence of encryption validation for the unencrypted laptops we tested.

2. **Resolved.** The Criminal Division concurred with the OIG's recommendation to provide all laptops to Information Technology Management staff for encryption prior to use. This recommendation can be closed when the Criminal Division provides relevant SOPs to us for review and evidence of implementation.

3. **Resolved.** The Criminal Division concurred with the OIG's recommendation to formalize laptop encryption procedures to ensure that laptops are appropriately inventoried, encrypted, and processed through Information Technology Management pursuant to Criminal Division policy. The Criminal Division has stated that it has a plan to correct systemic problems and will conduct routine inventory verifications. This recommendation can be closed when the Criminal Division provides relevant SOPs to us for review and evidence of implementation.

4. **Resolved.** The Criminal Division concurred with the OIG's recommendation to ensure that the Information Technology Management staff approves baseline configurations using DOJ standards on all laptops used for DOJ processing. The Criminal Division stated that the laptops we identified have been re-imaged and verified to be consistent with DOJ requirements. This recommendation can be closed when the Criminal Division provides relevant SOPs to us for review, evidence of implementation, and evidence that the indentified non-compliant laptops have been re-imaged in accord with DOJ requirements.

5. **Resolved.** The Criminal Division concurred with the OIG's recommendation to ensure that a record of encryption is maintained for all Criminal Division-owned laptops. This recommendation can be closed when the Criminal Division provides relevant SOPs and documentation of encryption record implementation.

6. **Resolved.** The Criminal Division concurred with the OIG's recommendation to enhance procedures for ensuring that the official inventory database, ARGIS, maintains accurate and reliable information for all Criminal Division-owned laptop computers. This recommendation

can be closed when the Criminal Division provides relevant SOPs and evidence of the Criminal Division's ARGIS inventory audit.

7. **Resolved.** The Criminal Division concurred with the OIG's recommendation to ensure that all Contractor-owned laptop computers used to process DOJ data are encrypted or require contractors to use Criminal Division provided hardware. The Criminal Division stated that it would provide encrypted USB storage devices to contractors and have the contractors sign a consent form agreeing to the terms and conditions of the PGD-08-04 guidance. This recommendation can be closed when the Criminal Division provides evidence that the procedures have been implemented to include: (1) contractor receipt of encrypted USB storage devices; (2) contractor-signed consent forms; and (3) the Contracting Officer's memo with signature page regarding rules and instructions outlining the PGD 08-04 guidance.

8. **Resolved.** The Criminal Division concurred with the OIG's recommendation to ensure that Criminal Division contract support providers are aware of security procedures for handling DOJ data in accordance with DOJ policy. This recommendation can be closed when the Criminal Division provides evidence of contractor-signed consent forms and the Contracting Officer's memo with signature page regarding rules and instructions outlining the PGD 08-04 guidance.

9. **Resolved.** The Criminal Division concurred with the OIG's recommendation to implement the PGD 08-04 clause in all OBD 47 contracts. This recommendation can be closed when the Criminal Division provides evidence of the contractors' certification that they understand and will comply with the rules of behavior prior to performing DOJ work and guidance regarding Division work being stored on the encrypted USB storage device.

10. **Resolved.** The Criminal Division concurred with the OIG's recommendation to implement the conditions of the waiver pertaining to the PGD 08-04 clause for Mega 3 contracts. This recommendation can be closed when the Criminal Division provides evidence of that it has re-emphasized the DOJ security requirements to all the Mega 3 contractors and evidence that site visits are regularly conducted.