



THE CIVIL DIVISION'S LAPTOP COMPUTER ENCRYPTION PROGRAM AND PRACTICES

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

Audit Report 09-33
July 2009

TABLE OF CONTENTS

	<u>Page</u>
THE CIVIL DIVISION'S LAPTOP COMPUTER ENCRYPTION PROGRAM AND PRACTICES.....	1
Introduction.....	1
OIG Audit Approach	2
OIG Results in Brief.....	3
Background	4
Finding and Recommendations	
<i>Civil Division's Efforts to Ensure Safeguards Over DOJ Data on Laptop Computers Need Improvement</i>	13
Conclusion.....	20
Recommendations.....	20
STATEMENT ON INTERNAL CONTROLS.....	22
STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS	23
APPENDIX I: OBJECTIVES, SCOPE, AND METHODOLOGY ..	24
APPENDIX II: ACRONYMS	26
APPENDIX III: DOJ PROCUREMENT GUIDANCE DOCUMENT 08-04, SECURITY OF SYSTEMS AND DATA, INCLUDING PERSONALLY IDENTIFIABLE INFORMATION.....	27
APPENDIX IV: SAFEGUARDS AGAINST AND RESPONDING TO THE BREACH OF PERSONALLY IDENTIFIABLE INFORMATION.....	31
APPENDIX V: PROTECTION OF DEPARTMENT SENSITIVE INFORMATION ON LAPTOP AND MOBILE COMPUTING DEVICES.....	53
APPENDIX VI: CIVIL DIVISION MANAGEMENT'S RESPONSE	54
APPENDIX VII: OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT.....	59

THE CIVIL DIVISION'S LAPTOP COMPUTER ENCRYPTION PROGRAM AND PRACTICES

Introduction

Significant losses of sensitive data and personally identifiable information (PII) 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 (VA) 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 As a result, 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.

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.

The stolen laptops included PII of Civil Division attorneys, the consultant's employees, plaintiffs, and potentially litigation sensitive information in support of the government's defense of sensitive civil litigation.

As a result of this incident, the OIG initiated this audit to assess the adequacy of laptop computer encryption deployment practices in the Civil Division.

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.

OIG Audit Approach

Our audit objectives were to determine whether the Civil Division complies with federal and Department of Justice (DOJ) policies regarding: (1) the use of whole disk encryption on the laptop computers that Civil 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 Civil Division.

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

During our audit, we interviewed Justice Management Division (JMD), Civil Division, and contractor personnel with responsibility for encryption policy development and deployment practices. Additionally, we interviewed JMD’s Contracting Officer responsible for finalizing contractual agreements between service vendors and the Civil Division regarding security requirements for laptop computers. We also reviewed the Civil Division’s contract documents for litigation support services. Within the Civil Division, we interviewed the Contracting Officer’s Technical Representative and the Counsel to the Chief Information Officer. We also interviewed key Civil Division personnel responsible for the laptop computer loan process, security, incident reporting, and encryption installation.

In addition, we tested a judgmental sample of 49 of 244 Civil Division-owned laptop computers contained in the Civil Division’s official property management system, ARGIS. We tested whether these laptops were encrypted, were included in the Civil Division’s inventory system, and whether they displayed the required warning banners.

The Civil Division did not maintain an inventory of laptops owned by contractors, subcontractors, and vendors. Therefore, we performed testing to estimate the number of contracted litigation support providers that used non-Civil Division-owned laptop computers. We surveyed 107 (20 percent) of 540 vendors and received 83 responses. Thirty-nine of the respondents stated that they used their own laptops to process DOJ data on behalf of the Civil Division. We surveyed these 39 respondents on whether the laptops

were encrypted and whether they had received the required security instructions for protecting DOJ data. We also requested more information surrounding the Civil Division contractor's loss of the two unencrypted laptops that occurred in October 2008.

OIG Results in Brief

Civil Division-Owned Laptop Computers

We found that all 46 Civil Division-owned operational laptop computers we tested were encrypted and compliant with DOJ requirements.³ However, we identified weaknesses in the Civil Division's laptop inventory, documentation, and warning banners.

The Civil Division was unable to produce an accurate inventory of the universe of laptop computers it owns from ARGIS, the official property management system. During our review, we were provided two sets of substantially different data for the number of laptops the Civil Division owned. The Civil Division's data in the ARGIS database identified 244 Civil Division-owned laptop computers, while a laptop tracking database used by the Civil Division's Office of Litigation Support (OLS) identified 136 laptop computers.⁴ We performed limited testing of both data sources and found discrepancies between the two systems, although we found more discrepancies in ARGIS than in the OLS laptop tracking database. For example, two laptop computers listed on the OLS database printout were not contained in the ARGIS database. In addition, at least 57 of the laptop computers identified within ARGIS were previously exceded.

The Civil Division maintained four unencrypted, non-operational laptops for operating system re-imaging purposes. We found that these laptops were not appropriately labeled for this purpose. In our judgment, these laptops should be labeled to minimize the risk of having the unencrypted laptop computers inadvertently deployed for operational use.

³ Our test sample also included three of the four Civil Division-owned non-operational, unencrypted laptops that were used for operating system re-imaging purposes.

⁴ As we explain later in the report, Civil Division officials stated that ARGIS, which is a system developed by the Department's Justice Management Division, was not reliable. Therefore, they developed their own database to track Civil Division laptop computers.

Further, 37 of the 49 laptop computers we tested did not employ a DOJ-required system warning banner.⁵ Warning banners are important safeguards because they alert potential system users that they are about to access a federal computer system and that there are ramifications for illegal and unauthorized system use.

Non-Civil Division-Owned Laptop Computers

We found a serious weakness concerning unencrypted laptop computers used by Civil Division contractors, subcontractors, and vendors. Thirty-one of 39 (79 percent) of the contractor, subcontractor, and vendors responding to our survey stated that their laptops used for processing DOJ data on behalf of the Civil Division were not encrypted.

We also found that the Civil Division was not providing security instructions to contractors, subcontractors, and other vendors for protecting DOJ data on their laptop computers. Specifically, 48 percent of the survey respondents stated that vendors had not received security instructions for protecting DOJ data.

Background

The DOJ's Civil Division, which has approximately 1,370 employees, represents the United States, its departments and agencies, members of Congress, Cabinet officers and other federal employees in federal litigation. Its litigation efforts involve national security issues; benefit programs; energy policies; commercial issues such as contract disputes, banking, insurance, patents, fraud, and debt collection; accident and liability claims; and violations of the immigration and consumer protection laws. As a result, the Civil Division handles sensitive data containing PII.

In its work, the Civil Division also 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 methods used by the Civil Division to obtain litigation support services are the Mega 3 and

⁵ DOJ Information Technology Security Standard, Access Control (AC) 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 takes explicit actions to log on to the information system. It warns the potential user of DOJ system access criteria and ramifications for illegal and unauthorized system use. The warning banner also contains information to relay privacy and security notices.

the Offices, Boards, and Divisions (OBD 47) contracts.⁶ Contracted litigation support providers help acquire, organize, develop, and present evidence throughout the litigation process. As of November 2008, approximately 540 contractors, subcontractors, and other vendors provided litigation support to the Civil Division.

The Civil Division reported to us that most of its Mega 3 contracted litigation support providers do not use laptop computers. However, when laptop computers are needed by contractors, subcontractors, and other vendors, the Civil Division often supplies Civil Division-owned laptop computers for their use. In some cases, however, due to time constraints brought on by fast-approaching trial dates, contractors and subcontractors are allowed to use their own laptops, subject to DOJ's security requirements, including encryption standards.

Loss of Two Unencrypted Laptop Computers

Regarding the two stolen laptop computers from the Civil Division consultant that occurred in October 2008, the Civil Division provided us with detailed information identifying the types of Civil data stored on the stolen laptops. Specifically, the laptops contained personally identifiable information (PII) such as:

- For Civil Division attorneys - names, cell and home phone numbers, and e-mail addresses.
- For the consultant's employees – names, home addresses, cell phone numbers, e-mail addresses, and possibly social security numbers.
- For plaintiffs in Civil Division litigation – names and e-mail addresses of personnel to the extent the information may have been on a source document image.

In addition to the PII, the Civil Division ascertained that both laptops contained the consultant's work product and other potentially litigation sensitive information (nothing higher than SBU) in support of the government's defense of two cases that are currently before the U.S. Court of Federal Claims in Washington, D.C. The laptops also contained a significant number of source documents from several other Civil Division cases.

⁶ 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.

The consultant had signed the Civil Division's Rules of Behavior for General Users, to obtain access to the Civil Division's central file sharing system, Omega, in June and July 2008 – 3 months prior to the incident.⁷ The Rules of Behavior specifically stated:

"In the event data is downloaded from the system, ensure that it is stored upon an OLS [Office of Litigation Support - Civil Division] issued laptop or an appropriately encrypted device pursuant to OMB Memorandum 07-11."

However, the consultant did not comply with the Rules of Behavior requirement to encrypt its laptop computers. Moreover, its employees failed to adequately secure the laptop computers at the end of their work day. The consultant explained to the Civil Division that its employees worked until 4 a.m. the morning of the incident. The employees then went home for a few hours and returned to work around 8 a.m. to find that the laptop computers had been stolen from the office. According to the police report, unknown suspects gained entry into the office by breaking the locked handle of the front interior door.

The Civil Division took several steps after this breach, including meeting with the consultant to discuss actions to ensure adequate controls are implemented to protect DOJ information. As a result of the meeting, the consultant started using encryption software on its laptop computers to meet the Civil Division Rules of Behavior requirement that was previously signed by its employees. The consultant also discussed additional physical security requirements with its building managers to assist with preventing future thefts.

The Civil Division provided us with a memo dated March 17, 2009, that documented the Civil Division's impact assessment activities related to the data loss. This document states that the Civil Division was able to quickly confirm with reasonable accuracy information about the volume, type, and sensitivity of data affected by this data loss incident and took steps to assess the impact the loss presented.

In addition, attorneys were able to provide prompt notice to the Court of Federal Claims and counsel for the affected defendants so they could assess the impact upon their clients. Further, the attorneys communicated with the consultant and another federal agency to determine whether its

⁷ Omega is the Civil Division's file litigation support portal used to share common litigation support documents between users working on the same cases.

information could have been compromised as a result of this data loss incident. The attorneys were able to confirm that no safeguarded information was affected or compromised by this data loss incident.

In our judgment, this loss was a serious security breach, and it should serve as an impetus for the Civil Division, as well as other DOJ components, to ensure that all laptops computers used in support of its work be properly encrypted.

Laptop Encryption Policy for DOJ Employees

DOJ Order 2640.2F establishes laptop encryption policy for DOJ employees. 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, Federal Information Processing Standards (FIPS) 140-2 validated or NSA approved encryption mechanisms.

Laptop Encryption Policy for Contractors

On March 20, 2008, the Department's Senior Procurement Executive issued the DOJ Procurement Guidance Document (PGD) 08-04, Security of Systems and Data, Including Personally Identifiable Information. PGD 08-04 sets forth 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 this 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 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.

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 need to be modified to include the applicable clause, within 60 days of the date of the issuance of the guidance, which was March 20, 2008. Thus, there is a 60-day grace period on all current contracts, after which, under the security clause, 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

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

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

In July 2008, the Civil Division issued a memorandum to the Senior Procurement Executive in response to the PGD 08-04 document in which the Civil Division requested an exemption from the requirement to incorporate the security clause into the Mega 3 and the OBD 47 contracts.⁸ A wide range of professionals are hired under the Mega 3 contracts, such as project managers, law clerks, paralegals, trial consultants, courtroom presentation specialists, technical writers, and programmers. The OBD 47 contracts hire experts and consultants.

The Civil Division described the following reasons for requesting the waiver on the Mega 3 contracts:

- The contracts are worth hundreds of millions of dollars, and changing the security requirements would require renegotiating the rates for each and every fixed line item affected by the security clause. The Government would be at a great disadvantage if it had to renegotiate these competitively-procured contract rates.
- The Civil Division was not in a position to certify all contractor, subcontractor, and vendor processing systems and shops. It estimated that certification of each shop would take 6 months, and cost about half a million dollars. The Civil Division stated that it did not have the resources or the funds for these certifications.
- The Civil Division believed that work performed under the Mega 3 contracts was stringently controlled through existing mechanisms and procedures. For example, the vendor facilities are controlled – locked at all times, sign-in sheets, escorted access for visitors. All contractor personnel working for Mega 3 complete the SF-85P and are cleared to work on Civil Division

⁸ As we explain later in this report, the Civil Division's request was to exempt them from the security clause requirement for their contracts, and not to exempt its contractors and subcontractors laptops from the encryption requirement.

contracts, sign non-disclosure agreements and are required to read and abide by standard rules of behavior.⁹

The Civil Division also described the following reasons for requesting the waiver for other contract vehicles including the OBD 47 contracts:

- The Civil Division's Assistant Attorney General would shortly issue guidance to clarify which data is "sensitive," and Civil Division attorneys and staff would be given additional training regarding the protection of sensitive data.¹⁰
- The Civil Division would implement the agreed-upon security clause on new contracts as they are issued. The Civil Division requested an exemption on the more than 1,500 current active contracts because attempting to retrofit these already existing contracts would require resources it does not have, and lead to its losing many current experts and consultants midway through litigation.

In August 2008, JMD responded that a blanket exemption would not be possible without further assurance that sensitive data was appropriately safeguarded. With respect to the Mega 3 contracts, JMD asked that the Civil Division provide the following additional documentation:

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

⁹ The Standard Form (SF) 85P is the Questionnaire for Public Trust Positions that is used by the government to conduct background investigations and reinvestigations to establish that applicants or incumbents either employed by the Government or working for the Government under contract, are suitable for the job and eligible for a public trust or sensitive position.

¹⁰ Civil Division officials stated that they were waiting on further guidance from JMD regarding possible approaches for protecting sensitive data.

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.

With respect to the other contract vehicles, the Senior Procurement Executive informed the Civil Division that he was willing to consider such an exemption for contracts that expire within a reasonably short period of time, assuming the Civil Division had a plan in place for implementing the security requirements on new contracts. He also stated that he was concerned about contracts that go on for longer periods. The Senior Procurement Executive asked the Civil Division for further information as to the duration of these current active contracts, and for the Civil Division to describe its plan for mitigating security risks for these contracts, particularly the ones that are not expiring within a reasonably short period of time.

In December 2008, as requested, the Civil Division provided JMD the following documentation to support the steps that the Civil Division had taken and planned to take to ensure that data security measures were implemented and enforced for the Mega 3 contracts:

1. Excerpts from the Mega 3 contract and the Mega 3 Contract Staff IT Security Guidance which included a revised Rules of Behavior dated October 1, 2008;¹¹
2. Written acknowledgement from the contractors that they received and accepted the data security guidance and instructions;
3. Written statements from the contractors that they will provide this guidance to their employees and subcontractors and develop adequate security training; and
4. More detailed descriptions of the steps the Civil Division has taken to strengthen the Mega 3 information technology security policies and procedures.¹²

¹¹ The October 1, 2008, Rules of Behavior required that contractors encrypt all Departmental data stored on transportable/mobile computers (including laptops) and on removable media (thumb drives, compact disks, floppy disks, etc.) being transported outside the Departments physical perimeter.

¹² The Civil Division's plan to strengthen security procedures for the Mega 3 contracts included updating the existing security requirements, ensuring contractors acknowledgment of the security requirements, conducting random audits of contractor equipment (laptops) and facilities, and developing a training plan.

The Civil Division did not provide JMD any response or documentation for the other contract vehicles, which would have included the OBD 47 contracts.

In January 2009, after reviewing the documentation provided by the Civil Division, the Senior Procurement Executive granted the waiver to exempt the security clause from being incorporated into the Mega 3 contracts. However, this waiver did not exempt contractor laptops from encryption requirements. This waiver was granted on the condition that the Civil Division implement clarifying revisions to the information technology security guidance for the Mega 3 contracts by the next quarterly update, which will be May 25, 2009.

The Senior Procurement Executive did not address any other contract vehicles in his January 2009 memo. The waiver only applied to the Mega 3 contracts and did not apply to the OBD 47 contracts. We determined during our audit that the Mega 3 primary contractors had numerous subcontractors, which totaled 166 subcontractors and the OBD 47 contract report provided by the Civil Division identified 1,483 vendors as providing contracted services to the Civil Division.¹³

Impact of the Waiver

Although the Civil Division was granted the waiver for the Mega 3 contracts, 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.

¹³ Although the OBD 47 report identified 1,483 vendors, upon consolidation of multiple awards to a single vendor by name, the total number of OBD 47 contracts was assessed to be approximately 374. See Appendix 1, Objectives, Scope, and Methodology for more details.

FINDING AND RECOMMENDATIONS

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

The Civil Division has complied with DOJ requirements by ensuring that its own laptop computers are encrypted to protect DOJ data. However, our audit identified areas where the Civil Division needs to improve its security procedures to include: (1) ensuring that its laptop inventory is maintained accurately in ARGIS; (2) ensuring that documentation is maintained to verify the successful installation of encryption software for all of its laptop computers; and (3) ensuring that warning banners are displayed on laptop computers to alert potential system users that they are about to access a federal computer system.

In addition, the Civil Division's efforts to ensure contractor safeguards over DOJ data need significant improvement. We found that: (1) an inventory of non-Civil Division laptop computers was not maintained; (2) a large percentage of contractor laptops used to process DOJ data were not encrypted; and (3) contractors had not received notification of DOJ laptop encryption requirements.

Laptop Computers Owned by the Civil Division

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

To perform our encryption testing, it was first necessary to establish an accurate universe of Civil Division-owned laptop computers. The majority of laptop computers owned by the Civil Division are part of its lending program.¹⁴ The lending program serves the laptop computer needs of Civil Division employees as well as contractors, subcontractors, and other vendors performing work on behalf of the Civil Division. Attorneys,

¹⁴ The Civil Division also had 12 laptop computers that were not used as part of its lending pool and 4 used solely for re-imaging purposes. All Civil Division laptops were considered in the universe sample group and subjected to selection as part of the OIG's encryption testing.

paralegals, contractors, and sub-contractors may reserve Civil Division laptops for use. The laptops are retrieved from a lending pool and are assigned to the requestor. Couriers pick up the laptops and deliver the laptops to the requestor. The laptops are usually reserved for short periods of time and returned by courier or in person.

The Civil Division was unable to produce an accurate inventory of the universe of laptop computers it owns from ARGIS, the official property management system. During our review, we were provided two sets of substantially different data for the number of laptops the Civil Division owned. The Civil Division's data in the ARGIS database identified 244 Civil Division-owned laptop computers, while a laptop tracking database used by the Civil Division's Office of Litigation Support (OLS) identified 136 laptop computers. Civil Division officials stated that ARGIS, which is a system developed by the Department's Justice Management Division, was not reliable and that they therefore developed their own database to track Civil Division laptop computers.

We performed limited testing of both data sources and found discrepancies between the two systems. Consistent with the statement made above by Civil Division officials, we found more discrepancies in ARGIS than in the OLS laptop tracking database. For example, two laptop computers listed on the OLS database printout were not contained in the ARGIS database. In addition, at least 57 of the laptop computers identified within ARGIS had been previously excedded. In our judgment, the Civil Division needs to reconcile the differences between the two data sources and ensure that the laptop inventory data in ARGIS is accurate and reliable.

We asked Civil Division officials about the discrepancy between the two sources of data and were told that the inaccuracies in ARGIS stem from the fact that the database is maintained by JMD and the Civil Division does not have privileges to update the data within ARGIS. We followed up with JMD and were told that JMD's Property Management Services decentralized in 2007 and granted Accountable Property Officers throughout the Offices, Boards, and Division's the ability to insert, update, and make final disposition changes (deletion status) to asset records. The term "deletion status" does not mean that assets are deleted from the database but are instead placed into a non-active status. We shared this information with Civil Division officials and they stated that they were unaware that they had the capabilities to perform these functions within ARGIS. As a result, the Civil Division stated that it will reconcile information in ARGIS with their separate laptop tracking database. In addition, in our follow-up discussions with JMD, we were told that JMD plans to retire the official property management system, ARGIS, in December 2009 and will deploy a new

inventory system in the future. If this occurs, we recommend that the Civil Division ensure that the laptop inventory data in the replacement system is accurate and reliable.

Encryption Test Results

DOJ Order 2640.2F establishes the laptop encryption requirements for DOJ employees. Chapter 2, section 12 of this order states that information on mobile computers or devices (such as notebook computers, personal digital assistants) and removable media shall be encrypted using FIPS 140-2 validated or NSA approved encryption mechanisms.

To test whether laptop computers were properly encrypted, we selected 49 of 244 laptops contained in the ARGIS database. For each computer selected we verified that encryption software was installed and the date the installation was completed. We verified this by having a Civil Division staff member turn on each laptop and we visually inspected the Pointsec logon screen. Additionally, we accessed the Pointsec software and verified the installation date in the log management console. We found that all 46 Civil Division-owned operational laptop computers we tested were encrypted and complied with DOJ requirements. Our test sample also included three non-operational, unencrypted laptops that were used for operating system re-imaging purposes.

Other Areas of Concern

Although encryption was the primary focus of this audit, we identified other weaknesses in the areas of documentation and warning banners.

Documentation

DOJ Order 2640.2F, *Audit and Accountability*, requires that information system audit records be maintained to the extent needed to enable security monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information technology system activities.

We found that documentation was not maintained by the Civil Division to verify the successful installation of encryption software for its laptop computers. In the Civil Division, encryption software is installed on laptops by a technician in the Civil Division's Office of Litigation Support. Once the encryption installation is completed, the laptop computer is submitted to the technician's supervisor for review and approval to be deployed.

Although the Civil Division stated that it does not allow any non-encrypted laptop computers to be deployed, documentation was not maintained to evidence when or if the encryption software was installed. In the event that the laptop computer is lost, the Civil Division would not be able to provide sufficient evidence that the encryption software was appropriately installed.

We also have a concern about the four laptop computers used by Civil Division's OLS to re-image other laptop computer's encryption software. The Civil Division told us that encryption software could not be installed or it would impede the re-imaging process and that these laptop computers are never deployed for regular use. However, the only indicator the Civil Division used to distinguish its re-imaging laptop computers from the loaner laptop computers was the lack of a KIT number on the OLS laptop tracking database printout.¹⁵ No warning labels were attached to the re-imaging laptop computers to indicate their special use or differentiate it from other Civil Division laptops available for storing sensitive and PII data. In our judgment, these computers should be clearly labeled that they are not encrypted and should indicate that they not be used for purposes other than re-imaging. Without such clear notice, the Civil Division runs the risk of having the laptop computers inadvertently deployed for operational use.

Warning Banners

DOJ Information Technology Security Standard, Access Control (AC) Family Version 2.2 (control AC-08), requires that all DOJ systems display an approved notification message before a user accesses the computer system. The warning banner is required to remain on the laptop computer's screen until the user takes explicit actions to log on to the information system. Warning banners alert potential system users that they are about to access a federal computer system and that there are ramifications for illegal and unauthorized system use.

We found that 37 of the 49 (76 percent) Civil Division laptop computers we tested did not employ a DOJ system warning banner.¹⁶ Further examination of the Civil Division's laptop computers revealed that this security violation occurred because the laptop computers used to re-image other laptop computers did not contain the required warning banner.

¹⁵ A KIT number is the unique identifier used by the Civil Division to track laptop inventory in the OLS database.

¹⁶ This non-statistical sample design does not allow projection of the test results to all laptops. See Appendix 1 for more details.

We discussed this issue with Civil Division officials and were told that this was an oversight.

As a result of the issues we identified pertaining to Civil Division laptops, the Civil Division has updated its security procedures. Civil Division officials provided us with a laptop administrator guide and a screen printout from their laptop tracking database and stated that the Civil Division will verify that the encryption installation date and warning banners are employed on its laptops prior to deployment.

Laptop Computers Owned by Contractors and Subcontractors

Laptop Inventory

We asked the Civil Division for an inventory of non-Civil Division laptop computers used by its contractors, subcontractors, and other vendors performing litigation support on Civil Division contracts and we were told that the Civil Division does not maintain such an inventory. During this audit, a Civil Division official told us that it will begin to maintain an inventory for its contractor, subcontractor, and vendor laptops.

The DOJ Procurement Guidance Document (PGD) 08-04 security clause also requires that contracting firms must keep an accurate inventory of devices used by contractors, subcontractors, and other vendors on DOJ contracts. Furthermore, the contractor must certify, in writing with the contracting officer, that it has met this requirement.

Because the Civil Division did not maintain laptop inventory information on its contractors and subcontractors, we conducted a survey to estimate the number of contracted litigation support providers that used non-Civil Division-owned laptop computers on Civil Division tasks.

We surveyed 107 (20 percent) of the 540 Civil Division's contractors, subcontractors, and other vendors located throughout the United States and abroad. We received 83 responses to our survey. We found that 39 (47 percent) of the 83 vendor responses indicated they used non-Civil Division laptop computers to process Civil Division data. The remaining 44 responses from the contractors indicated that they did not use a laptop computer for their Civil Division work.

In our view, the lack of an inventory of contractor and subcontractor-owned laptops is a serious deficiency. Without an inventory, the Civil Division is at risk of not being able to account for non-Civil Division laptop

computers that are authorized to process DOJ data and cannot ensure that appropriate safeguards are in place.

Encryption Test Results for Contractors

PGD 08-04 requires that laptops owned by contractors and subcontractors must be encrypted. We found serious deficiencies with the level of encryption employed on laptop computers owned by contractor, subcontractor, and other vendor employees working on Civil Division business. Of the vendors responding that they used their own laptop computers for Civil Division work, 31 of the 39 (79 percent) stated that their laptops were not encrypted, while the remaining 8 (21 percent) responded that their laptops were installed with FIPS 140-2 approved encryption software.

The 31 vendors using non-encrypted laptops were on both the Mega 3 and OBD 47 contracts. Specifically, there were 4 Mega 3 and 27 OBD 47 contractors using their own laptops without encryption installed.¹⁷ Although the Civil Division was granted a waiver for the Mega 3 contracts, the Civil Division Rules of Behavior for Mega 3 requires that contractors process DOJ data on encrypted laptops. Moreover, the OBD 47 contractors did not receive a waiver from the requirement to incorporate the security clause into the OBD 47 contracts that requires laptop encryption. Therefore, these 31 vendors for both Mega 3 and OBD 47 contracts should have been using encryption software on their laptops.

Security Awareness

DOJ Order 2640.2F, Awareness and Training, requires that managers and users of DOJ information are aware of the security risks associated with their activities and of the applicable laws related to the security of DOJ data.

We found that the Civil Division had distributed notifications of laptop encryption requirements to some of its litigation support service providers. However, many contractors, subcontractors, and vendors had not received such notifications. In our survey, 40 of the 83 responses (48 percent) from vendors indicated that they had not received security instructions for protecting DOJ data. Of the 40 vendors that had not received security

¹⁷ During the audit, we provided the Civil Division with the names of the 4 Mega 3 subcontractors that had unencrypted laptops. The Civil Division followed up with these 4 subcontractors and provided us with additional information indicating that mitigating steps are being taken by the subcontractors to safeguard DOJ data. In addition, the Civil Division has drafted further IT security training guidance for all Mega 3 contractors and subcontractors.

instructions, 6 were from the Mega 3 and 34 were from the OBD 47 contracts.

The Civil Division's Director of Litigation Support stated that the Mega 3 contractors, subcontractors, and vendors are made aware of the importance of laptop encryption and security requirements, through weekly meetings that are held with the vendors that are required to manage and oversee their own staff in regards to encryption. Also, IT security guidelines are posted on the Civil Division's internal website, which contractors can access, after agreeing with the requirements of the Civil Division's Rules of Behavior.

However, according to a Civil Division Official for the OBD 47 contracts, these contractors are not specifically notified of the importance of laptop encryption and security. The official also stated that there is nothing in the contracts pertaining to encryption and security, but the Civil Division plan to implement such procedures in the future. In our judgment, the OBD 47 contracts should have a Rules of Behavior requirement similar to the Mega 3 contracts already in-place.

Civil Division officials stressed that the Mega 3 and the OBD 47 contracts are for two separate groups of contractors providing support. During our review, we noted that there were more security controls in place for the Mega 3 versus the OBD 47 contractors. Civil Division officials expressed how challenging it was to obtain valuable OBD 47 contractors and that the success of a case often depends on the testimony by experts and consultants obtained through this contract. While Civil Division officials recognize that enhanced security measures are needed for this group, they expressed concern with imposing more security requirements on the OBD 47 contracts. Civil Division officials stated that the OBD 47 contractors may be unwilling to testify if strict security requirements are forced upon them, and this could jeopardize Civil Division cases.

While we understand the necessity of obtaining experts and consultants for trials, we do not fully agree that requiring encryption would unduly burden all OBD 47 contractors, since several of these contractors stated during our survey that encryption was installed on their laptop computers. Failure to ensure that security awareness requirements are relayed to vendors places DOJ data at greater risk to unauthorized disclosure. In our judgment, it is critical that all litigation support providers be made aware of the security requirements for handling sensitive DOJ data and that Civil Division periodically check that such requirements are, in fact, implemented.

Conclusion

We found that all 46 Civil Division-owned operational laptop computers we tested were encrypted to protect sensitive DOJ data, in accordance with DOJ requirements. However, our review identified weaknesses in the areas of inventory, documentation, and warning banners that the Civil Division needs to address. Specifically, the Civil Division should ensure that it maintains an accurate laptop inventory in its property management system, ARGIS. In addition, unencrypted, non-operational laptops should be marked as such to prevent their use for operational purposes. Further, warning banners should be displayed on all of the Division's laptop computers to alert potential system users that they are about to access a federal computer system.

With respect to non-Civil Division-owned laptop computers, we identified significant weaknesses that need to be addressed. We found that an inventory of non-Civil Division laptop computers was not maintained. Also, according to surveyed participants, 79 percent of contractor laptops used to process DOJ data were not encrypted. Moreover, almost one-half of surveyed respondents had not received notification of DOJ laptop encryption requirements.

Given the sensitivity of the litigation work performed by the Civil Division in such areas as national security, banking, and insurance, we believe that Civil Division contractors, subcontractors, and vendors should encrypt their laptop computers or exclusively use the Civil Division's laptop computer lending pool. As a result of the issues identified in this report, we make seven recommendations to the Civil Division to enhance its safeguards over DOJ data on laptop computers. The officials concurred with all seven recommendations.

Recommendations

We recommend that the Civil Division:

1. Implement procedures for ensuring that the official inventory database, ARGIS, or any replacement system, maintains accurate and reliable information for all Civil Division laptop computers.
2. Ensure the laptop administrator's guide is used to document the successful installation of encryption software on Civil Division laptop computers.

3. Label re-imaging computers to indicate that they are not encrypted and not for operational use.
4. Ensure the laptop administrator's guide is used to verify that system warning banners are installed on all Civil Division laptop computers as required by DOJ policy.
5. Develop and maintain an inventory of authorized or approved non-Civil Division owned laptop computers for contractors, subcontractors, and other entities providing contract support services for the Civil Division.
6. Ensure that all non-Civil Division laptop computers used to process DOJ data are encrypted or require contractors to use encrypted Civil Division provided hardware.
7. Ensure that all contract support providers are aware of security information procedures for handling DOJ data in accordance with DOJ policy.

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 Civil Division's internal controls was *not* made for the purpose of providing assurance on its internal control structure as a whole. The Civil 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 Civil 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 Civil 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 Civil Division's internal control structure as a whole, this statement is intended solely for the information and use of the Civil 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 Civil 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 Civil 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 Civil Division and that were significant within the context of the audit objectives:

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

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

As noted in the Finding section of this report, we found that tested Civil Division-owned laptop computers were encrypted as required by DOJ policy. However, improvements are needed with the Civil Division's laptop computers program and practices in the areas of laptop inventory and warning banners. Significant improvements are required on the use of non-Civil 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 Civil Division's laptop computer encryption program and practices. Specifically, our audit objectives were to determine whether the Civil 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 Civil Division.

Our audit covered a 2-month period from November 12, 2008, through January 16, 2009. We performed field work on-site at the Civil Division's offices in Washington, D.C. During the audit period, key JMD, Civil Division, and contractor personnel with responsibilities related to encryption policy development and deployment practices were interviewed. We interviewed JMD's Contracting Officer responsible for finalizing contractual agreements between service vendors and the Civil Division and asked specific questions regarding security requirements for laptop computers. We also reviewed the Civil Division's contract documents for litigation support services.

Within the Civil Division, we interviewed the Contracting Officer's Technical Representative, and Counsel to the Chief Information Officer, as well as, key personnel responsible for tracking the loan process of laptop computers, laptop security, incident reporting, and laptop encryption installation.

Our testing of Civil Division laptop computers was conducted by judgmentally selecting a sample of 49 of 244 of the Civil Division's laptop computers identified within the official ARGIS database to be tested as part of the physical encryption verification process. This non-statistical sample design does not allow projection of the test results to all laptops.

Because the Civil Division did not maintain laptop inventory information on its contractors and subcontractors, we performed testing to estimate the number of contracted litigation support providers that used

non-Civil Division-owned laptop computers. To accomplish this we performed a survey of contractors, subcontractors, and other vendors from the two major contract methods used by the Civil Division to obtain litigation support services – Mega 3 and Office, Boards, and Division (OBD) contracts.

The Mega 3 contracts were awarded to three primary contractors: CACI International Inc., Labat-Anderson Incorporated, and Lockheed Martin. As of November 2008, each primary contractor had numerous subcontractors, which totaled 166 subcontractors. The Civil Division provided the OIG with documents to evidence that the three primary contractors for the Mega 3 contracts did not use non-Civil Division-owned laptop computers to process Civil Division data. Therefore, the primary contractors were not included in our survey.

As of November 2008, the OBD 47 contract report provided by the Civil Division identified 1,483 vendors as providing contracted services to the Civil Division. Upon consolidation of multiple awards to a single vendor by name, the total number of OBD contracts was assessed to be approximately 374.

Therefore, as of November 2008, our universe of the Civil Division's contractors, subcontractors, and other vendors totaled 540 (166 + 374). We surveyed 107 (20 percent) of the 540 vendors and received 83 responses. The responses are detailed in the Findings and Recommendations section of this report.

ACRONYMS

DOJ	Department of Justice
DOJCERT	Department of Justice Computer Emergency Readiness Team
JMD	Justice Management Division
OBD	Office, Boards, and Division
OIG	Office of the Inspector General
OLS	Office of Litigation Support
OMB	Office of Management and Budget
PII	Personally Identifiable Information




U. S. Department of Justice

MAR 20 2008

Washington, D.C. 20530

MEMORANDUM FOR BUREAU PROCUREMENT CHIEFS

FROM: Michael H. Allen 
Senior Procurement Executive

SUBJECT: DOJ Procurement Guidance Document 08-04, Security of Systems and Data, Including Personally Identifiable Information

My memorandum of January 18, 2008, notified you of recent instances of contractor loss of equipment containing sensitive data relating to Department programs or personnel. Section A of this guidance document sets forth a required security clause addressing Department systems and data, including provisions governing the use of laptops by contractors, to 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. Please note that in Section A, paragraphs a, b, and d apply to all data, even data that may not be personally identifiable information (PII)¹. Section B of this guidance document sets forth a required clause that must be used in contracts involving personally identifiable information obtained by the Department from a contractor, such as an information reseller or data broker. This guidance document supersedes Procurement Guidance Document 06-10.

A. Security of Systems and Data, Including Personally Identifiable Information.

The following clause must be used in any contract where the 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.

¹ The term "personally identifiable information," as defined by OMB, means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Security of Systems and Data, Including Personally Identifiable Data.

a. Systems Security

The work to be performed under this contract requires the handling of 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.

For all systems handling such data, the contractor shall comply with all security requirements applicable to Department of Justice systems, including but not limited to all Executive Branch system security requirements (*e.g.*, requirements imposed by OMB and NIST), DOJ IT Security Standards, and DOJ Order 2640.2E. The contractor shall provide DOJ access to and information regarding the contractor's systems when requested by the Department in connection with its efforts to ensure compliance with all such security requirements, and shall otherwise cooperate with the Department in such efforts. DOJ access shall include independent validation testing of controls, system penetration testing by DOJ, FISMA data reviews, and access by the DOJ Office of the Inspector General for its reviews.

The use of contractor-owned laptops or other media storage devices to process or store data covered by this clause is prohibited until the contractor provides a letter to the contracting officer (CO) certifying the following requirements:

1. Laptops must employ encryption using a NIST Federal Information Processing Standard (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 will utilize anti-viral software and a host-based firewall mechanism;
4. The contractor shall 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 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, shall not be removed from DOJ facilities unless encrypted using a NIST 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 shall address at a minimum: authorized and official use; prohibition against unauthorized users; and protection of sensitive data and personally identifiable information;

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;

b. Data Security

By acceptance of, or performance on, this contract, the contractor agrees that with respect to the data identified in paragraph a, in the event of any actual or suspected breach of such data (*i.e.*, 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 one hour of discovery) report the breach to the DOJ CO and the contracting officer's technical representative (COTR).

If the data breach occurs outside of regular business hours and/or neither the CO nor the COTR can be reached, the contractor shall call the DOJ Computer Emergency Readiness Team (DOJCERT) at 1-866-US4-CERT (1-866-874-2378) within one hour of discovery of the breach. The contractor shall also notify the CO as soon as possible during regular business hours.

c. Personally Identifiable Information Notification Requirement

The contractor further certifies that it has a security policy in place that contains procedures to promptly notify any individual whose personally identifiable information (as defined by OMB) was, or is reasonably believed to have been, breached. Any notification shall be coordinated with the Department, and shall not proceed until the Department has made a determination that notification would not impede a law enforcement investigation or jeopardize national security. The method and content of any notification by the contractor shall be coordinated with, and be subject to the approval of, the Department. The contractor assumes full responsibility for taking corrective action consistent with the Department's Data Breach Notification Procedures, which may include offering credit monitoring when appropriate.

d. Pass-through of Security Requirements to Subcontractors

The requirements set forth in Paragraphs a through c above, apply to all subcontractors who perform work in connection with this contract. For each subcontractor, the contractor must certify that it has required the subcontractor to adhere to all such requirements. Any breach by a subcontractor of any of the provisions set forth in this clause will be attributed to the contractor.

B. Information Resellers or Data Brokers

For contracts where the Department obtains PII from a contractor (such as an information reseller or data broker) but the contractor does not handle the data described in Section A of this guidance document, the following clause must be used:

Information Resellers or Data Brokers

Under this contract, the Department obtains personally identifiable information about individuals from the contractor. The contractor hereby certifies that it has a security policy in place which contains procedures to promptly notify any individual whose personally identifiable information (as defined by OMB) was, or is reasonably believed to have been, lost or acquired by an unauthorized person while the data is under the control of the contractor. In any case in which the data that was lost or improperly acquired reflects or consists of data that originated with the Department, or reflects sensitive law enforcement or national security interest in the data, the contractor shall notify the Department contracting officer so that the Department may determine whether notification would impede a law enforcement investigation or jeopardize national security. In such cases, the contractor shall not notify the individuals until it receives further instruction from the Department.

In my memorandum dated January 18, 2008, I encouraged you to identify all current and upcoming contracts that require the exchange of PII and other Departmental data between the contractor and the Department that need to include this security coverage. All current contracts to be covered will need to be modified to include the applicable clause, within 60 days of the date of this memorandum. Thus, there is a 60-day grace period on all current contracts, after which, under the security clause, laptops or devices not covered by certification letters may not be used on DOJ contracts. Contracting officers should alert contractors of this requirement as soon as possible in order to avoid disruption in the use of laptops. A request for a waiver from the requirement to include these clauses, or deviations from the language of these clauses (except those that are more stringent), must be made in writing to the Senior Procurement Executive. Permission for a deviation or waiver will only be granted in unusual circumstances.



EXECUTIVE OFFICE OF THE PRESIDENT

OFFICE OF MANAGEMENT AND BUDGET

WASHINGTON, D.C. 20503

DEPUTY DIRECTOR
FOR MANAGEMENT

May 22, 2007

M-07-16

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Clay Johnson III
Deputy Director for Management

SUBJECT: Safeguarding Against and Responding to the Breach of Personally Identifiable Information

Safeguarding personally identifiable information¹ in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. This is a responsibility shared by officials accountable for administering operational and privacy and security programs, legal counsel, Agencies' Inspectors General and other law enforcement, and public and legislative affairs. It is also a function of applicable laws, such as the Federal Information Security Management Act of 2002 (FISMA)² and the Privacy Act of 1974.³

As part of the work of the Identity Theft Task Force,⁴ this memorandum requires agencies to develop and implement a breach⁵ notification policy⁶ **within 120 days**. The attachments to this memorandum outline the framework within which agencies must develop this breach notification policy⁷ while ensuring proper safeguards are in place to protect the information. Agencies should

¹ The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

² Title III of the E-Government Act of 2002, Pub. L. No. 107-347.

³ 5 U.S.C. § 552a.

⁴ Executive Order 13402 charged the Identity Theft Task Force with developing a comprehensive strategic plan for steps the federal government can take to combat identity theft, and recommending actions which can be taken by the public and private sectors. On April 23, 2007 the Task Force submitted its report to the President, titled "Combating Identity Theft: A Strategic Plan." This report is available at www.idtheft.gov.

⁵ For the purposes of this policy, the term "breach" is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

⁶ Agencies should use a best judgment standard to develop and implement a breach notification policy. Using a best judgment standard, the sensitivity of certain terms, such as personally identifiable information, can be determined in context. For example, an office rolodex contains personally identifiable information (name, phone number, etc.). In this context the information probably would not be considered sensitive; however, the same information in a database of patients at a clinic which treats contagious disease probably would be considered sensitive information. Similarly, using a best judgment standard, discarding a document with the author's name on the front (and no other personally identifiable information) into an office trashcan likely would not warrant notification to US-CERT.

⁷ Terms not specifically defined within this Memorandum (e.g., sensitive) should be considered to reflect the definition found in a commonly accepted dictionary.

note the privacy and security requirements addressed in this Memorandum apply to all Federal information and information systems.⁸ Breaches subject to notification requirements include both electronic systems as well as paper documents. In short, agencies are required to report on the security of information systems in any format (*e.g.*, paper, electronic, etc.).⁹

In formulating a breach notification policy, agencies must review their existing requirements with respect to Privacy and Security (see Attachment 1). The policy must include existing and new requirements for Incident Reporting and Handling (see Attachment 2) as well as External Breach Notification (see Attachment 3). Finally, this document requires agencies to develop policies concerning the responsibilities of individuals authorized to access personally identifiable information (see Attachment 4).

Within the framework set forth in the attachments, agencies may implement more stringent policies and procedures reflecting the mission of the agency. While this framework identifies a number of steps to greatly reduce the risks related to a data breach of personally identifiable information, it is important to emphasize that a few simple and cost-effective steps may well deliver the greatest benefit, such as:

- reducing the volume of collected and retained information to the minimum necessary;
- limiting access¹⁰ to only those individuals who must have such access; and
- using encryption, strong authentication procedures, and other security controls to make information unusable by unauthorized individuals.

This Memorandum should receive the widest possible distribution within your agency and each affected organization and individual should understand their specific responsibilities for implementing the procedures and requirements. Materials created in response to this Memorandum and attachments should be made available to the public through means determined by the agency, *e.g.*, posted on the agency web site, by request, etc.

Consistent with longstanding policy requiring agencies to incorporate the costs for securing their information systems, all costs of implementing this memorandum, including development,

⁸ FISMA security requirements apply to Federal information and information systems, including both paper and electronic format.

⁹ A plan to review the controls for information systems not previously included in other security reviews must be addressed in the agency's breach notification policy (*e.g.*, timeframe for completion of review, etc.); however, completion of the review for those systems is not required to be finished within the 120-day timeframe for development of the policy.

¹⁰ In this policy, "access" means the ability or opportunity to gain knowledge of personally identifiable information.

implementation, notification to affected individuals, and any remediation activities, will be addressed through existing agency resources of the agency experiencing the breach.

Because of the many alternate ways to implement a risk-based program within the framework provided, this Memorandum, or its attachments, should not be read to mean an agency's failure to implement one or more of the many security provisions discussed within¹¹ would constitute less than adequate protections required by the Privacy Act. These new requirements do not create any rights or benefits, substantive or procedural, which are enforceable at law against the government.

Questions about this Memorandum should be directed to Hillary Jaffe of my staff at hjaffe@omb.eop.gov.

Attachments

¹¹ For example, FISMA or associated standards, policies, or guidance issued by OMB or the National Institute of Standards and Technology (NIST).

Attachment 1: Safeguarding Against the Breach of Personally Identifiable Information

This Attachment reemphasizes the responsibilities under existing law, executive orders, regulations, and policy to appropriately safeguard personally identifiable information and train employees on responsibilities in this area (Section A).¹² It also establishes two new privacy requirements and discusses five security requirements as described below (Sections B and C).

A. Current Requirements

1. Privacy Act Requirements. In particular, the Privacy Act of 1974 (Privacy Act)¹³ requires each agency to:

a. Establish Rules of Conduct. Agencies are required to establish “rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of [the Privacy Act], including any other rules and procedures adopted pursuant to [the Privacy Act] and the penalties for noncompliance.” (5 U.S.C. § 552a(e)(9))

b. Establish Safeguards. Agencies are also required to “establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.”¹⁴

c. Maintain accurate, relevant, timely and complete information. The Privacy Act also requires personally identifiable information within a system of records to be maintained in a manner that is accurate, relevant, timely, and complete including through the use of notices to the public.¹⁵ It is important for agencies to fulfill their responsibilities with respect to identifying systems of records and developing and publishing notices as required by the Privacy Act and

¹² This Memorandum, or its attachments, should not be read to mean an agency’s failure to implement one or more of the many provisions of FISMA or associated standards, policies, or guidance issued by OMB or the National Institute of Standards and Technology (NIST) would constitute less than adequate protections required by the Privacy Act of 1974.

¹³ 5 U.S.C. § 552a.

¹⁴ 5 U.S.C. § 552a (e)(10).

¹⁵ The Privacy Act requires agencies to “maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination” in their systems of records. 5 U.S.C. § 552a(e)(5).

OMB's implementing policies.¹⁶ By collecting only the information necessary and managing it properly, agencies can often reduce the volume of information they possess, the risk to the information, and the burden of safeguarding it.

2. Security Requirements.

Below are four particularly important existing security requirements agencies already should be implementing:

a. Assign an impact level to all information and information systems. Agencies must follow the processes outlined in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, to categorize all information and information systems according to the standard's three levels of impact (*i.e.*, low, moderate, or high). Agencies should generally consider categorizing sensitive personally identifiable information (and information systems within which such information resides) as moderate or high impact.

b. Implement minimum security requirements and controls. For each of the impact levels identified above, agencies must implement the minimum security requirements and minimum (baseline) security controls set forth in FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, and NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, respectively.

c. Certify and accredit information systems. Agencies must certify and accredit (C&A) all information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.¹⁷ The specific procedures for conducting C&A are set out in NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, and include guidance for continuous monitoring of certain security controls. Agencies' continuous monitoring should assess a subset of the management, operational, and technical controls used to safeguard such information (*e.g.*, Privacy Impact Assessments).

d. Train employees. Agencies must initially train employees (including managers) on their privacy and security responsibilities before permitting access to agency information and information systems. Thereafter, agencies must provide at least annual refresher training to

¹⁴ The Privacy Act requires agencies to publish a notice of any new or intended use of information maintained in a system of records in the Federal Register to provide an opportunity for the public to submit comments. 5 U.S.C. § 552a(e)(4). Agencies are also required to publish notice of any subsequent substantive revisions to the use of information maintained in the system of records. 5 U.S.C. § 552a(e)(11). OMB Circular A-130 ("Management of Federal Information Resources") offers additional guidance on this issue. OMB Circular A-130, App. I, sec. 4.c.

¹⁷ 44 U.S.C. 3544(b).

ensure employees continue to understand their responsibilities.¹⁸ Additional or advanced training should also be provided commensurate with increased responsibilities or change in duties.

Both initial and refresher training must include acceptable rules of behavior and the consequences when the rules are not followed. For agencies implementing tele-work and other authorized remote access programs, training must also include the rules of such programs.¹⁹

B. Privacy Requirements

1. Review and Reduce the Volume of Personally Identifiable Information.

a. Review Current Holdings. Agencies must now also review their current holdings of all personally identifiable information and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete, and reduce them to the minimum necessary for the proper performance of a documented agency function.²⁰ Agency-specific implementation plans and progress updates regarding this review will be incorporated as requirements in agencies' annual report under FISMA.

Following this initial review, agencies must develop and make public a schedule by which they will periodically update the review of their holdings. This schedule may be part of an agency's annual review and any consolidated publication of minor changes of Privacy Act systems of records notices.

To help safeguard personally identifiable information, agencies are reminded they must meet the requirements of FISMA and associated policies and guidance from the OMB and NIST.²¹ FISMA requires each agency to implement a comprehensive security program to protect the agency's information and information systems; agency Inspectors General must independently evaluate the agency's program; and agencies must report annually to OMB and Congress on the effectiveness of their program.

¹⁸ Agencies may schedule training to coincide with existing activities, such as ethics training. Communications and training related to privacy and security must be job-specific and commensurate with the employee's responsibilities. The Department of Defense, the Office of Personnel Management, and the Department of State offer agencies a minimum baseline of security awareness training as part of the Information Systems Security Line of Business.

¹⁹ Agencies should also consider augmenting their training by using creative methods to promote daily awareness of employees' privacy and security responsibilities, such as weekly tips, mouse pads imprinted with key security reminders, privacy screens for public use of laptops, and incentives for reporting security risks.

²⁰ To the extent agencies are substantively performing these reviews, agencies should leverage these efforts to meet the new privacy requirements. This provision does not apply to apply to the accessioned holdings (archival records) held by the National Archives and Records Administration (NARA).

²¹ The Department of Defense and Intelligence Community establish their own policy and guidance for the security of their information systems. 44 U.S.C. 3543(c).

Within the above framework, agencies may implement more stringent procedures governed by specific laws, regulations, and agency procedures to protect certain information, for example, taxpayer data, census information, and other information.

2. Reduce the Use of Social Security Numbers.

a. Eliminate Unnecessary Use. Agencies must now also review their use of social security numbers in agency systems and programs to identify instances in which collection or use of the social security number is superfluous. Within 120 days from the date of this memo, agencies must establish a plan in which the agency will eliminate the unnecessary collection and use of social security numbers within eighteen months.²²

b. Explore Alternatives. Agencies must participate in government-wide efforts to explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs (*e.g.*, surveys, data calls, etc.).

C. Security Requirements

While agencies continue to be responsible for implementing all requirements of law and policy, below are five requirements²³ agencies must implement which derive from existing security policy and NIST guidance. These requirements are applicable to all Federal information, *e.g.*, law enforcement information, etc.

- Encryption. Encrypt, using only NIST certified cryptographic modules,²⁴ all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive, in writing, by your Deputy Secretary²⁵ or a senior-level individual he/she may designate in writing;
- Control Remote Access. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
- Time-Out Function. Use a “time-out” function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity;
- Log and Verify. Log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required; and

²² Agencies with questions addressing this assignment regarding the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) should contact their respective desk officer at the Office of Management and Budget.

²³ See OMB Memo 06-16 “Protection of Sensitive Agency Information” (www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf).

²⁴ See NIST’s website at <http://csrc.nist.gov/cryptval/> for a discussion of the certified encryption products.

²⁵ Non cabinet agencies should consult the equivalent of a Deputy Secretary.

- Ensure Understanding of Responsibilities. Ensure all individuals with authorized access to personally identifiable information and their supervisors sign at least annually a document clearly describing their responsibilities.

Agencies should also contemplate and incorporate best practices to prevent data breaches. Examples of such practices might include using privacy screens when working outside the office or requiring employees to include laptop computers in carry-on luggage rather than checked baggage.

Attachment 2: Incident Reporting and Handling Requirements

This Attachment applies to security incidents involving the breach of personally identifiable information whether in electronic or paper format. For the purposes of reporting, agencies must continue to follow existing requirements, as modified and described below.

A. Existing Requirements

1. FISMA Requirements. FISMA requires each agency to:

- implement procedures for detecting, reporting and responding to security incidents, including mitigating risks associated with such incidents before substantial damage is done
- notify and consult with:
 - the Federal information security incident center
 - law enforcement agencies and Inspectors General
 - an office designated by the President for any incident involving a national security system
 - any other agency or office in accordance with law or as directed by the President.²⁶
- implement NIST guidance and standards²⁷

Federal Information Processing Standards Publication 200 (FIPS 200) and NIST Special Publication 800-53 provide a framework for categorizing information and information systems, and provide minimum security requirements and minimum (baseline) security controls for incident handling and reporting. The procedures agencies must already use to implement the above FISMA requirements are found in two primary guidance documents: NIST Special Publication 800-61, *Computer Security Incident Handling Guide*²⁸; and the concept of operations for the Federal security incident handling center located within the Department of Homeland Security, *i.e.*, United States Computer Emergency Readiness Team (US-CERT).²⁹

²⁶ 44 U.S.C. § 3544(b)(7).

²⁷ For additional information on NIST guidance and standards, see www.nist.gov.

²⁸ See “Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology” (<http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>).

²⁹ The responsibilities of US-CERT are outlined in 44 U.S.C. § 3546. Its complete set of operating procedures may be found on the US-CERT website (www.us-cert.gov/federal/reportingRequirements.html). Separate procedures are in place for the Department of Defense as identified in Directive O-8530-1 and all components report incidents to the Joint Task Force Global Network Operations (JTF-GNO), which, in turn, coordinates directly with the US-CERT.

2. Incident Handling and Response Mechanisms. When faced with a security incident, an agency must be able to respond in a manner protecting both its own information and helping to protect the information of others who might be affected by the incident. To address this need, agencies must establish formal incident response mechanisms. To be fully effective, incident handling and response must also include sharing information concerning common vulnerabilities and threats with those operating other systems and in other agencies. In addition to training employees on how to prevent incidents, all employees must also be instructed in their roles and responsibilities regarding responding to incidents should they occur.

B. Modified Agency Reporting Requirements

1. US-CERT Modification. Agencies must report all incidents involving personally identifiable information to US-CERT. This reporting requirement does not distinguish between potential and confirmed breaches. The US-CERT concept of operations for reporting Category 1 incidents is modified as follows:

Category 1. Unauthorized Access or Any Incident Involving Personally Identifiable Information. In this category agencies must report when: 1) an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource; or 2) there is a suspected or confirmed breach of personally identifiable information regardless of the manner in which it might have occurred. Reporting to US-CERT is required within one hour of discovery/detection.

- For incidents involving personally identifiable information, agencies must:
 - Continue to follow internal agency procedures for notifying agency officials including your agency privacy official and Inspector General;
 - Notify the issuing bank if the breach involves government-authorized credit cards; and
 - Notify US-CERT within one hour. Although only limited information about the breach may be available, US-CERT must be advised so it can assist in coordinating communications with the other agencies. Updates should be provided as further information is obtained.
- Under specific procedures established for these purposes, after notification by an agency, US-CERT will notify the appropriate officials.
- Monthly, US-CERT will distribute to designated officials in the agencies and elsewhere, a report identifying the number of confirmed breaches of personally identifiable information and will also make available a public version of the report.

2. Develop and Publish a Routine Use.

a. Effective Response. A federal agency's ability to respond quickly and effectively in the event of a breach of federal data is critical to its efforts to prevent or minimize any consequent

harm.³⁰ An effective response necessitates disclosure of information regarding the breach to those individuals affected by it, as well as to persons and entities in a position to cooperate, either by assisting in notification to affected individuals or playing a role in preventing or minimizing harms from the breach.

b. Disclosure of Information. Often, the information to be disclosed to such persons and entities is maintained by federal agencies and is subject to the Privacy Act (5 U.S.C. § 552a). The Privacy Act prohibits the disclosure of any record in a system of records by any means of communication to any person or agency absent the written consent of the subject individual, unless the disclosure falls within one of twelve statutory exceptions.³¹ In order to ensure an agency is in the best position to respond in a timely and effective manner, in accordance with 5 U.S.C. § 552a(b)(3) of the Privacy Act, agencies should publish a routine use for appropriate systems specifically applying to the disclosure of information in connection with response and remedial efforts in the event of a data breach as follows:

To appropriate agencies, entities, and persons when (1) [the agency] suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.³²

As described in the President's Identity Theft Task Force's Strategic Plan, all agencies should publish a routine use for their systems of records allowing for the disclosure of information in the course of responding to a breach of federal data.³³ Such a routine use will serve to protect the interests of the individuals whose information is at issue by allowing agencies to take appropriate steps to facilitate a timely and effective response, thereby improving their ability to prevent, minimize, or remedy any harm resulting from a compromise of data maintained in their systems of records.

³⁰ Here, "harm" means damage, fiscal damage, or loss or misuse of information which adversely affects one or more individuals or undermines the integrity of a system or program.

³¹ 5 U.S.C. §§ 552a(b)(1)-(12).

³² See Appendix B of the Identity Theft Task Force report (www.identitytheft.gov/reports/StrategicPlan.pdf).

³³ *Id.*

Attachment 3: External Breach Notification

To ensure consistency across government, this Attachment identifies the questions and factors each agency should consider in determining when notification outside the agency should be given and the nature of the notification.³⁴ This Attachment does not attempt to set a specific threshold for external notification since breaches are specific and context dependant and notification is not always necessary or desired. The costs of any notifications must be borne by the agency experiencing the breach from within existing resources.

A. Background

1. Harm. Breaches can implicate a broad range of harms to individuals, including the potential for identity theft; however, this Section does not discuss actions to address possible identity theft or fraud. Agencies are referred to the ID Theft Task Force’s Strategic Plan for guidance.

2. Requirement. Agencies must implement the one specific new requirement discussed below; *i.e.*, develop a breach notification policy and plan (see Section B. below).

3. Threshold questions. Both the decision to provide external notification on the occasion of a breach and the nature of the notification will require agencies to resolve a number of threshold questions.³⁵ The likely risk of harm and the level of impact will determine when, what, how and to whom notification should be given.³⁶

Notification of those affected and/or the public allows those individuals the opportunity to take steps to help protect themselves from the consequences of the breach. Such notification is also consistent with the “openness principle” of the Privacy Act that calls for agencies to inform individuals about how their information is being accessed and used, and may help individuals mitigate the potential harms resulting from a breach.

4. Chilling Effects of Notices. A number of experts have raised concerns about unnecessary notification and the chilling effect this may have on the public.³⁷ In addition, agencies should

³⁴ These factors do not apply to an agency’s notification to US-CERT. Agencies must report all incidents – potential and confirmed – involving personally identifiable information to US-CERT.

³⁵ Notice may not be necessary if, for example, the information is properly encrypted because the information would be unusable.

³⁶ See OMB’s September 20, 2006 memorandum titled “Recommendations for Identity Theft Related Data Breach Notification” for information and recommendations for planning and responding to data breaches which could result in identity theft (www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf).

³⁷ Federal Trade Commission, *Prepared Statement of the Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, U.S. Senate, on Data Breaches and Identity Theft* (Washington, D.C.: June 16, 2005), p. 10. In this testimony, the Federal Trade Commission raised concerns about the threshold for which consumers should be notified of a breach, cautioning that too strict a standard could have several negative effects.

consider the costs to individuals and businesses of responding to notices where the risk of harm may be low. Agencies should exercise care to evaluate the benefit of notifying the public of low impact incidents.

B. New Requirement

Each agency should develop a breach notification policy and plan comprising the elements discussed in this Attachment. In implementing the policy and plan, the Agency Head will make final decisions regarding breach notification.

Six elements should be addressed in the policy and plan and when considering external notification:

- whether breach notification is required
- timeliness of the notification
- source of the notification
- contents of the notification
- means of providing the notification
- who receives notification: public outreach in response to a breach

To ensure adequate coverage and implementation of the plan, each agency should establish an agency response team including the Program Manager of the program experiencing the breach, Chief Information Officer, Chief Privacy Officer or Senior Official for Privacy, Communications Office, Legislative Affairs Office, General Counsel and the Management Office which includes Budget and Procurement functions.³⁸ A more detailed description of these elements is set forth below:

1. Whether Breach Notification is Required

To determine whether notification of a breach is required, the agency should first assess the likely risk of harm caused by the breach and then assess the level of risk. Agencies should consider a wide range of harms, such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved in the breach.³⁹ Agencies should bear in mind that notification when there is little or no risk of harm might create

³⁸ Non-Cabinet-level agencies should include their functional equivalent.

³⁹ For reference, the express language of the Privacy Act requires agencies to consider a wide range of harms: agencies shall “establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.” 5 U.S.C. § 552a (e)(10).

unnecessary concern and confusion.⁴⁰ Additionally, under circumstances where notification could increase a risk of harm, the prudent course of action may be to delay notification while appropriate safeguards are put in place.

Five factors should be considered to assess the likely risk of harm:

a. Nature of the Data Elements Breached. The nature of the data elements compromised is a key factor to consider in determining when and how notification should be provided to affected individuals.⁴¹ It is difficult to characterize data elements as creating a low, moderate, or high risk simply based on the type of data because the sensitivity of the data element is contextual. A name in one context may be less sensitive than in another context.⁴² In assessing the levels of risk and harm, consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.

b. Number of Individuals Affected. The magnitude of the number of affected individuals may dictate the method(s) you choose for providing notification, but should not be the determining factor for whether an agency should provide notification.

c. Likelihood the Information is Accessible and Usable. Upon learning of a breach, agencies should assess the likelihood personally identifiable information will be or has been used by unauthorized individuals. An increased risk that the information will be used by unauthorized individuals should influence the agency's decision to provide notification.

The fact the information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals, however, depending upon a number of physical, technological, and procedural safeguards employed by the agency. (See Attachment 1 above.) If the information is properly protected by encryption, for example, the risk of compromise may be low to non-existent.⁴³

Agencies will first need to assess whether the personally identifiable information is at a low, moderate, or high risk of being compromised. The assessment should be guided by NIST

⁴⁰ Another consideration is a surfeit of notices, resulting from notification criteria which are too strict, could render all such notices less effective, because consumers could become numb to them and fail to act when risks are truly significant.

⁴¹ For example, theft of a database containing individuals' names in conjunction with Social Security numbers, and/or dates of birth may pose a high level of risk of harm, while a theft of a database containing only the names of individuals may pose a lower risk, depending on its context.

⁴² For example, breach of a database of names of individuals receiving treatment for contagious disease may pose a higher risk of harm, whereas a database of names of subscribers to agency media alerts may pose a lower risk of harm.

⁴³ In this context, proper protection means encryption has been validated by NIST.

2. Timeliness of the Notification

Agencies should provide notification without unreasonable delay following the discovery of a breach, consistent with the needs of law enforcement and national security and any measures necessary for your agency to determine the scope of the breach and, if applicable, to restore the reasonable integrity of the computerized data system compromised.

Decisions to delay notification should be made by the Agency Head or a senior-level individual he/she may designate in writing. In some circumstances, law enforcement or national security considerations may require a delay if it would seriously impede the investigation of the breach or the affected individual. However, any delay should not exacerbate risk or harm to any affected individual(s).

3. Source of the Notification

In general, notification to individuals affected by the breach should be issued by the Agency Head, or senior-level individual he/she may designate in writing, or, in those instances where the breach involves a publicly known component of an agency, such as the Food and Drug Administration or the Transportation Security Administration, the Component Head. This demonstrates it has the attention of the chief executive of the organization. Notification involving only a limited number of individuals (*e.g.*, under 50) may also be issued jointly under the auspices of the Chief Information Officer and the Chief Privacy Officer or Senior Agency Official for Privacy. This approach signals the agency recognizes both the security and privacy concerns raised by the breach.

When the breach involves a Federal contractor or a public-private partnership operating a system of records on behalf of the agency, the agency is responsible for ensuring any notification and corrective actions are taken. The roles, responsibilities, and relationships with contractors or partners should be reflected in your breach notification policy and plan, your system certification and accreditation documentation, and contracts and other documents.

4. Contents of the Notification

The notification should be provided in writing and should be concise, conspicuous, plain language. The notice should include the following elements:

- A brief description of what happened, including the date(s) of the breach and of its discovery;

security standards and guidance. Other considerations may include the likelihood any unauthorized individual will know the value of the information and either use the information or sell it to others.

d. Likelihood the Breach May Lead to Harm

1. *Broad Reach of Potential Harm.* The Privacy Act requires agencies to protect against any anticipated threats or hazards to the security or integrity of records which could result in “substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.”⁴⁴ Additionally, agencies should consider a number of possible harms associated with the loss or compromise of information. Such harms may include the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

2. *Likelihood Harm Will Occur.* The likelihood a breach may result in harm will depend on the manner of the actual or suspected breach and the type(s) of data involved in the incident. Social Security numbers and account information are useful to committing identity theft, as are date of birth, passwords, and mother’s maiden name. If the information involved, however, is a name and address or other personally identifying information, the loss may also pose a significant risk of harm if, for example, it appears on a list of recipients patients at a clinic for treatment of a contagious disease.

In considering whether the loss of information could result in identity theft or fraud, agencies should consult guidance from the Identity Theft Task Force.⁴⁵

e. Ability of the Agency to Mitigate the Risk of Harm. Within an information system, the risk of harm will depend on how the agency is able to mitigate further compromise of the system(s) affected by a breach. In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of the personal information and patterns of suspicious behavior, should be taken.⁴⁶ Such mitigation may not prevent the use of the personal information for identity theft, but it can limit the associated harm. Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and may be difficult to determine.

⁴⁴ 5 U.S.C. § 552a(e)(10).

⁴⁵ See “Recommendations for Identity Theft Related Data Breach Notification” (www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf).

⁴⁶ For example, if the information relates to disability beneficiaries, monitoring a beneficiary database for requests for change of address may signal fraudulent activity.

- To the extent possible, a description of the types of personal information involved in the breach (*e.g.*, full name, Social Security number, date of birth, home address, account number, disability code, etc.);
- A statement whether the information was encrypted or protected by other means, when determined such information would be beneficial and would not compromise the security of the system;
- What steps individuals should take to protect themselves from potential harm, if any;
- What the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and
- Who affected individuals should contact at the agency for more information, including a toll-free telephone number, e-mail address, and postal address.

Given the amount of information required above, you may want to consider layering the information as suggested in Section 5 below, providing the most important information up front, with the additional details in a Frequently Asked Questions (FAQ) format or on your web site. If you have knowledge the affected individuals are not English speaking, notice should also be provided in the appropriate language(s). You may seek additional guidance on how to draft the notice from the Federal Trade Commission, a leader in providing clear and understandable notices to consumers, as well as from communication experts who may assist you in designing model notices.⁴⁷ A standard notice should be part of your approved breach plan.

5. Means of Providing Notification

The best means for providing notification will depend on the number of individuals affected and what contact information is available about the affected individuals. Notice provided to individuals affected by a breach should be commensurate with the number of people affected and the urgency with which they need to receive notice. The following examples are types of notice which may be considered.

a. **Telephone.** Telephone notification may be appropriate in those cases where urgency may dictate immediate and personalized notification and/or when a limited number of individuals are affected. Telephone notification, however, should be contemporaneous with written notification by first-class mail.

⁴⁷ Additional guidance on how to draft a notice is available in the FTC publication titled “Dealing with a Data Breach” (www.ftc.gov/bcp/edu/microsites/idtheft/business/data-breach.html). Although the brochure is designed for private sector entities that have experienced a breach, it contains sample notice letters that could also serve as a model for federal agencies. You may also seek guidance from communications experts who may assist you in designing model notices.

b. First-Class Mail. First-class mail notification to the last known mailing address of the individual in your agency's records should be the primary means notification is provided. Where you have reason to believe the address is no longer current, you should take reasonable steps to update the address by consulting with other agencies such as the US Postal Service. The notice should be sent separately from any other mailing so that it is conspicuous to the recipient. If the agency which experienced the breach uses another agency to facilitate mailing (for example, if the agency which suffered the loss consults the Internal Revenue Service for current mailing addresses of affected individuals), care should be taken to ensure the agency which suffered the loss is identified as the sender, and not the facilitating agency. The front of the envelope should be labeled to alert the recipient to the importance of its contents, *e.g.*, "Data Breach Information Enclosed" and should be marked with the name of your agency as the sender to reduce the likelihood the recipient thinks it is advertising mail.

c. E-Mail. E-mail notification is problematic, because individuals change their e-mail addresses and often do not notify third parties of the change. Notification by postal mail is preferable. However, where an individual has provided an e-mail address to you and has expressly given consent to e-mail as the primary means of communication with your agency, and no known mailing address is available, notification by e-mail may be appropriate. E-mail notification may also be employed in conjunction with postal mail if the circumstances of the breach warrant this approach. E-mail notification may include links to the agency and www.U.S.A.gov⁴⁸ web sites, where the notice may be "layered" so the most important summary facts are up front with additional information provided under link headings.

d. Existing Government Wide Services. Agencies should use Government wide services already in place to provide support services needed, such as USA Services, including toll free number of 1-800-FedInfo and www.U.S.A.gov.

e. Newspapers or other Public Media Outlets. Additionally, you may supplement individual notification with placing notifications in newspapers or other public media outlets. You should also set up toll-free call centers staffed by trained personnel to handle inquiries from the affected individuals and the public.

f. Substitute Notice. Substitute notice in those instances where your agency does not have sufficient contact information to provide notification. Substitute notice should consist of a conspicuous posting of the notice on the home page of your agency's web site and notification to major print and broadcast media, including major media in areas where the affected individuals reside. The notice to media should include a toll-free phone number where an individual can learn whether or not his or her personal information is included in the breach.

⁴⁸ The current domain name for the Federal Internet portal required by section 204 of the E-Government Act of 2002 is www.usa.gov.

g. Accommodations. Special consideration to providing notice to individuals who are visually or hearing impaired consistent with Section 508 of the Rehabilitation Act of 1973 should be given. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large type notice on the agency web site.

6. Who Receives Notification: Public Outreach in Response to a Breach

a. Notification of Individuals. The final consideration in the notification process when providing notice is to whom you should provide notification: the affected individuals, the public media, and/or other third parties affected by the breach or the notification. Unless notification to individuals is delayed or barred for law enforcement or national security reasons, once it has been determined to provide notice regarding the breach, affected individuals should receive prompt notification.

b. Notification of Third Parties including the Media. If communicating with third parties regarding a breach, agencies should consider the following.

1. *Careful Planning*. An agency's decision to notify the public media will require careful planning and execution so that it does not unnecessarily alarm the public. When appropriate, public media should be notified as soon as possible after the discovery of a breach and the response plan, including the notification, has been developed. Notification should focus on providing information, including links to resources, to aid the public in its response to the breach. Notification may be delayed upon the request of law enforcement or national security agencies as described above in Section 2. To the extent possible, when necessary prompt public media disclosure is generally preferable because delayed notification may erode public trust.

2. *Web Posting*. Agencies should post information about the breach and notification in a clearly identifiable location on the home page of your agency web site as soon as possible after the discovery of a breach and the decision to provide notification to the affected individuals. The posting should include a link to Frequently Asked Questions (FAQ) and other talking points to assist the public's understanding of the breach and the notification process.⁴⁹ The information should also appear on the www.USA.gov web site. You may also consult with GSA's USA Services regarding using their call center.

3. *Notification of other Public and Private Sector Agencies*. Other public and private sector agencies may need to be notified on a need to know basis, particularly those that may be

⁴⁹ See the FAQ posted by the Department of Veterans Affairs in response to the May 2006 incident for examples of links to identity theft resources and a sample FAQ (www.usa.gov/veteransinfo.shtml).

affected by the breach or may play a role in mitigating the potential harms stemming from the breach.⁵⁰

4. *Congressional Inquiries.* Agencies should be prepared to respond to inquiries from other governmental agencies such as the Government Accountability Office and Congress.

c. Reassess the Level of Impact Assigned to the Information. After evaluating each of these factors, you should review and reassess the level of impact you have already assigned to the information using the impact levels defined by the NIST.⁵¹ The impact levels – low, moderate, and high, describe the (worst case) potential impact on an organization or individual if a breach of security occurs.⁵²

- **Low:** the loss of confidentiality, integrity, or availability is expected to have a **limited** adverse effect on organizational operations, organizational assets or individuals
- **Moderate:** the loss of confidentiality, integrity, or availability is expected to have a **serious** adverse effect on organizational operations, organizational assets or individuals.
- **High:** the loss of confidentiality, integrity, or availability is expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets or individuals.

The impact levels will help determine when and how notification should be provided. Where there is a range of risk levels attributed to the factors, the decision to provide notification should give greater weight to the likelihood the information is accessible and usable and whether the breach may lead to harm. If agencies appropriately apply the five risk factors discussed in section 1 of this attachment within the fact-specific context, it is likely notification will only be given in those instances where there is a reasonable risk of harm and will not lead to the overuse of notification.

⁵⁰ For example, a breach involving medical information may warrant notification of the breach to health care providers and insurers through the public or specialized health media, and a breach of financial information may warrant notification to financial institutions through the federal banking agencies.

⁵¹ See FIPS 199 and Attachment 1 of this memorandum. Reassessment is suggested as the context of any breach may alter your original designation.

⁵² The determination of the potential impact of loss of information is made by the agency during an information system's certification and accreditation process.

Attachment 4: Rules and Consequences

A. New Requirement: Rules and Consequences Policy.

Fairness requires that managers, supervisors and employees be informed and trained regarding their respective responsibilities relative to safeguarding personally identifiable information and the consequences and accountability for violation of these responsibilities. Therefore, it is the responsibility of each agency head to develop and implement an appropriate policy outlining the rules of behavior and identifying consequences and corrective actions available for failure to follow these rules. Consequences should be commensurate with level of responsibility and type of personally identifiable information involved. Supervisors also must be reminded of their responsibility to instruct, train and supervise employees on safeguarding personally identifiable information. Agencies should develop and implement these policies in accordance with the agency's respective existing authorities.

As with any disciplinary action, the particular facts and circumstances, including whether the breach was intentional, will be considered in taking appropriate action. Supervisors also should be reminded that any action taken must be consistent with law, regulation, applicable case law, and any relevant collective bargaining agreement. Supervisors should understand they may be subject to disciplinary action for failure to take appropriate action upon discovering the breach or failure to take required steps to prevent a breach from occurring.

Agencies having questions regarding development of a rules and consequences policy may contact OPM's Center for Workforce Relations and Accountability Policy at (202) 606-2930.

1. Affected Individuals. At a minimum, each agency should have a documented policy in place which applies to employees of the agency (including managers), and its contractors, licensees, certificate holders, and grantees.

2. Affected Actions. The agency's policy should describe the terms and conditions affected individuals shall be subject to and identify available corrective actions. Rules of behavior and corrective actions should address the following:

- Failure to implement and maintain security controls, for which an employee is responsible and aware, for personally identifiable information regardless of whether such action results in the loss of control⁵³ or unauthorized disclosure of personally identifiable information;

⁵³ Here, "control" means the authority of the government agency that originates information, or its successor in function, to regulate access to the information. Having control is a condition or state and not an event. Loss of control is also a condition or state which may or may not lead to an event, *i.e.*, a breach.

- Exceeding authorized access to, or disclosure to unauthorized persons of, personally identifiable information;
- Failure to report any known or suspected loss of control or unauthorized disclosure of personally identifiable information; and
- For managers, failure to adequately instruct, train, or supervise employees in their responsibilities.

3. Consequences. Applicable consequences may include reprimand, suspension, removal, or other actions in accordance with applicable law and agency policy. The minimum consequence agencies should consider is prompt removal of authority to access information or systems from individuals who demonstrates egregious disregard or a pattern of error in safeguarding personally identifiable information.



U.S. Department of Justice

DEC 26 2007

MEMORANDUM FOR ALL DEPARTMENT OF JUSTICE EMPLOYEES

FROM: Vance E. Hitch
Chief Information Officer *Vance E. Hitch*

SUBJECT: Protection of Department Sensitive Information on
Laptop and Mobile Computing Devices

The Department of Justice maintains a significant amount of sensitive information, including Personally Identifiable Information (PII), on its computer systems. The purpose of this memorandum is to remind Department personnel of their responsibility to protect Department information on laptops and other mobile computing devices and on removable media. This memorandum also reminds personnel of their responsibility to report the loss of sensitive data.

- All Department laptop computers and mobile computing devices processing sensitive information must employ Department approved encryption using Federal Information Processing Standard FIPS 140-2 (as amended) compliant software.
- All Department removable media which contains sensitive information and is being transported outside of the Department's secured, physical perimeter should employ Department approved encryption using Federal Information Processing Standard FIPS 140-2 (as amended) compliant software and remain in the personal custody of the individual when outside of Departmental facilities.
- All incidents involving known loss of PII must be reported within one hour of discovery or detection to the DOJCERT at (866) 874-2378. Any loss of any data storage devices, such as laptop computers, flash drives, disks, and tapes, must be reported within the same one hour time frame.

If you have any questions or require additional information, please contact Kevin Deeley, Deputy Director of the Information Technology Security Staff on (202) 353-2421 or <mailto:kevin.deeley@usdoj.gov>.

CIVIL DIVISION MANAGEMENT'S RESPONSE



U.S. Department of Justice

Civil Division

Washington, D.C. 20530

July 6, 2009

MEMORANDUM

To: Raymond J. Beaudet
Assistant Inspector General for Audit

From: Kenneth L. Zwick *KLZ*
Director, Office of Management Programs
Civil Division

Re: Draft Audit Report: The Civil Division's Laptop Computer Encryption Program and Practices

This memorandum is in response to the Draft Audit Report issued by the Office of the Inspector General (OIG) on May 19, 2009. The Civil Division appreciates the significant work performed by the OIG in auditing the Civil Division's encryption policies and practices, and agrees with the recommendations set forth in the report. The Division recognizes the need to adequately safeguard its data, and has reviewed the report's recommendations from this perspective.

The report discusses deficiencies in data encryption by contractors and subcontractors, and in the security instructions given them. As an initial matter, we note that the majority of such findings apply to experts, neutrals, and consultants hired by the Division under OBD-47 agreements. Unlike the Mega-3 contractors also discussed in the report, OBD-47 contractors are not often large litigation support firms, but individuals from teaching hospitals, academic institutions, or private practice. OBD experts generally do not provide expert services as a primary vocation, but regard their participation in Civil Division cases as a public service. As individual experts, they are not necessarily proficient with technology, nor do they have IT staffs on which to rely. The Civil Division is committed to safeguarding its data as recommended by the OIG. However, because of the varied and individual nature of such expert services, imposing security requirements without compromising our ability to produce

expert testimony in fast-paced litigation presents special challenges.¹

The Civil Division maintains a laptop computer tracking database. As noted in the report, this was necessary in part because of issues with the existing data in the ARGIS database provided by the Justice Management Division. The report notes discrepancies in both the ARGIS database and in the Division's internal laptop computer tracking database. Although the Division is not aware of any errors currently in the internal laptop computer tracking database, it will be further examined to ensure accuracy. We note, however, that both examples of inconsistencies in the two databases given in the report point to inaccuracies in ARGIS, rather than in the Civil Division laptop computer tracking database. Consistent with the report's recommendations, the Civil Division has recently completed a physical inventory of all laptop computers, and a wall-to-wall inventory of all accountable property. The Civil Division is in the process of reconciling the ARGIS database with these inventories to ensure accuracy. JMD has advised the Division that they will retire the aging ARGIS database system on November 1, 2009, and migrate data to the new Unicenter Asset Portfolio Management (UAPM) system.

Of note, the OIG report includes the result of testing a sample of computers in the Civil Division lending pool for the presence of a warning banner. The auditors found that 76% of the 47 laptop computers tested did not contain warning banners.² Further investigation by the Civil Division indicates that this issue was confined to a single model of laptop computer, which comprised only 46% of the laptop computer lending program inventory. Since this omission was discovered, laptop computer lending practices have been modified to document the presence of the banner on each loaner laptop computer before it is issued to the user.

In the course of the investigation, the auditors spoke with four subcontractors under the Mega-3 contract who reported having unencrypted laptop computers. Follow-up by the Civil Division indicates that three of those subcontractors did use laptop computers, but those computers did not contain DOJ data. However, the remaining subcontractor did not comply with Civil Division requirements regarding data security. Based on the OIG's investigation, mitigating steps are being taken with regard to the remaining Mega-3 subcontractor, and all Mega-3 contractors have received further security guidance and training.

¹ The OIG report states that the Civil Division initially provided a report listing 1,483 vendors hired under OBD-47 agreements. Actually, this represented the total number of OBD-47 agreements in force, rather than the number of unique vendors. Typically, one OBD-47 is executed for a contractor's work on each matter. Accordingly, a single expert, neutral, or consultant may be party to multiple OBD-47 agreements. The figure stated in the OIG report of approximately 374 unique vendors is correct.

² The OIG report notes that this is a non-statistical sample that does not allow projection of the results to all Civil Division laptop computers.

RESPONSE TO RECOMMENDATIONS

The Civil Division agrees with the recommendations set forth in the OIG report. Below are comments specific to each recommendation and expected times for implementation.

1. Implement procedures for ensuring that the official inventory database, ARGIS, or any replacement system, maintains accurate and reliable information for all Civil Division laptop computers.

This recommendation has already been implemented in part. Previously, the Accountable Property Officer for the Civil Division had annotated the ARGIS database to reflect older units that had been excessed. As noted in the report, authority to make changes to ARGIS database records to directly reflect these annotations was granted to the Civil Division in 2007; however, no training nor any information on these new features was provided. The annotations regarding excessed units were ultimately incorporated into the ARGIS database at the completion of the Civil Division's Physical Inventory of Capitalized Property and Portable Computers on March 26, 2009.

To help ensure the accuracy of the current ARGIS database, the Civil Division has in place procedures for conducting a physical inventory of laptop computers annually, and a wall-to-wall inventory of all accountable property every two years. Previously, the results of this audit were provided to JMD so ARGIS could be updated, but are now incorporated directly into the ARGIS database to reduce the possibility of error. The most recent laptop computer inventory was completed on March 26, 2009. The most recent wall-to-wall inventory was completed on May 21, 2009.

JMD has informed us that the conversion to the UAPM system (the successor to the ARGIS system), will take place on November 1, 2009. The Civil Division looks forward to working with JMD to obtain adequate training and documentation to help ensure that it is accurately maintained.

2. Ensure the laptop administrator's guide is used to document the successful installation of encryption software on Civil Division laptop computers.

This recommendation has been implemented. The Civil Division's laptop computer lending program tracking database has been updated to require the administrator to record whether a loaner laptop computer displays proper encryption information as a final step before it is released to the user. The relevant database screen now contains a link to the Laptop Administrator's Guide for reference. Screen shots of the relevant portion of the database are at Appendix A.

3. Label re-imaging computers to indicate that they are not encrypted and not for operational use.

This recommendation has been implemented. The phrase "Not encrypted - not for

operational use” has been permanently marked on the re-imaging laptop computers.

4. Ensure the laptop administrator’s guide is used to verify that system warning banners are installed on all Civil Division laptop computers as required by DOJ policy.

This recommendation has been implemented. The Civil Division’s laptop computer lending program tracking database has been updated to require the administrator to record whether a loaner laptop computer displays the warning banner as a final step before it is released to the user. The relevant database screen now contains a link to the Laptop Administrator’s Guide for reference. Screen shots of the relevant portion of the database are at Appendix A.

5. Develop and maintain an inventory of authorized or approved non-Civil Division owned laptop computers for contractors, subcontractors, and other entities providing contract support services for the Civil Division.

This recommendation has been implemented for contractors, subcontractors, and other entities under the Mega-3 contract.

The process for authorizing the use of laptop computers not owned by the Civil Division by contractors, subcontractors, and other entities under hired pursuant to an OBD-47 will be part of a comprehensive set of procedures. Please see the response to recommendation #6.

6. Ensure that all non-Civil Division laptop computers used to process DOJ data are encrypted or require contractors to use encrypted Civil Division provided hardware.

This recommendation has been implemented for contractors under the Mega-3 contract.

Implementing this recommendation for contractors hired under an OBD-47 will likely require a comprehensive set of new procedures, including changes in contract language, technical support resources, additional hardware acquisition, additional personnel, and training. It is likely that some OBD-47 contractors will have the resources to comply with this requirement. For others who may lack the technical sophistication to comply with the requirement, the Civil Division may have to provide some limited support or encrypted hardware. Any such hardware would have to be identified, tested, procured, and deployed. It is likely that the administrative overhead for this will require additional personnel. Finally, those acting as points of contact for OBD-47 contractors will require training in the additional contracting requirements and security procedures. We anticipate it will take 9-12 months to fully implement this recommendation.

7. Ensure that all contract support providers are aware of security information procedures for handling DOJ data in accordance with DOJ policy.

All Mega-3 contractors have been provided this information, and required to pass it through to sub-contractors. As to OBD-47 contractors, it will be part of the comprehensive

program outlined in response to recommendation #6. To ensure security awareness, the Civil Division will conduct periodic spot-checks of contract support providers.

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

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

The Civil Division was provided a draft of this audit report and their comments on the findings and recommendations were considered in preparing this Analysis and Summary of Actions Necessary to Close the Report. The Civil Division's response is incorporated as Appendix VI of this report. Since the Civil Division concurred with all of the recommendations, this report is being issued resolved. Our analysis of the Civil Division's responses and a summary of actions necessary to close the recommendations are provided below.

Analysis of Civil Division Response

In response to our audit report, the Civil Division concurred with our recommendations and discussed the actions it will implement in response to our findings. In addition, the Civil Division responded to information contained in our report unrelated to our recommendations. We respond to these statements before discussing the Civil Division's specific responses to each of our recommendations and the actions necessary to close those recommendations.

The Civil Division stated that the OBD 47 contractors regard their participation in Civil Division cases as a public service, and that these experts are not necessarily proficient with technology, nor do they have IT staffs on which to rely. In addition, the Civil Division stated that it is committed to safeguarding its data by imposing appropriate security requirements, but the Civil Division needs to do so without compromising its ability to produce expert testimony. We recognize this challenge with acquiring the OBD 47 contractors. However, in our judgment given the sensitive nature of the work performed, the Civil Division should ensure that the OBD experts use encrypted laptops. Therefore, we fully support the Civil Division's efforts outlined in its response to recommendation 6 and encourage the Civil Division to explore all options for protecting sensitive data on laptops, such as providing encrypted hardware, support, and training to the OBD 47 contractors.

The Civil Division stated that it is not aware of any errors in its internal laptop computer tracking database and that it will further examine the database to ensure its accuracy. In our report, we pointed out discrepancies between the ARGIS database and the OLS

laptop tracking database and provided an example where information contained in ARGIS did not reconcile with the OLS database. To help ensure the accuracy of the current ARGIS database or any replacement system, the Civil Division has recently completed a physical inventory of all laptop computers and a wall-to-wall inventory of all accountable property. We agree that these efforts should help to ensure the accuracy of the Civil Division's laptop inventory.

The Civil Division is correct in stating that our findings regarding the presence of a warning banner on computers in its lending pool does not allow projection of the test results to all laptops in its inventory. We reported that 37 of the 49 (76 percent) Civil Division laptop computers we tested did not employ a DOJ system warning banner. The Civil Division stated that it reviewed its laptop inventory and found that this issue was confined to a single laptop model that comprised 46 percent of its laptop computer inventory. We note that while this is less than the 76 percent of computers without the required security banner in our sample, this is still a substantial number of non-compliant laptops.

The Civil Division stated it followed-up with four subcontractors under the Mega 3 contract that we reported as having unencrypted laptop computers. The Civil Division indicated that three of those subcontractors used laptop computers that did not contain DOJ data, while the fourth subcontractor failed to comply with Civil Division requirements. Based on our survey and recommendations 5 - 7, the Civil Division has taken corrective steps with regards to all Mega 3 contractors and has developed a comprehensive plan for the OBD 47 contractors to develop an inventory of approved laptop computers for contractors and subcontractors, ensure that all DOJ data are stored on encrypted devices, and ensure that all contract support providers are aware of security information procedures.

Summary of Actions Necessary to Close the Recommendations

1. **Resolved.** The Civil Division concurred with the OIG's recommendation to implement procedures for ensuring that the official inventory database, ARGIS, or any replacement system maintains accurate and reliable information for all Civil Division laptop computers. To help ensure the accuracy of the current ARGIS database, the Civil Division conducted a physical inventory of laptop computers on March 26, 2009. JMD has informed the Civil Division that the conversion to the Unicenter Asset Portfolio

Management (UAPM), the successor to the ARGIS database, will occur on November 1, 2009. This recommendation can be closed when we receive documentation showing that the UAPM system is tracking the Civil Division's laptop inventory.

2. **Closed.** This recommendation is closed based on documentation provided by the Civil Division showing that the laptop computer lending program tracking database has been updated to require the administrator to record whether a loaner laptop computer displays proper encryption information.
3. **Resolved.** The Civil Division concurred with the OIG's recommendation to label re-imaging computers to indicate that they are not encrypted and not for operational use. The Civil Division stated that the phrase, "Not encrypted – not for operational use" has been permanently marked on the re-imaging laptop computers. This recommendation can be closed when we receive documentation showing that the re-imaging laptop computers are labeled to indicate that they are not encrypted and not for operational use.
4. **Closed.** This recommendation is closed based on documentation provided by the Civil Division showing that the laptop computer lending program tracking database has been updated to require the administrator to record whether a loaner laptop computer displays the warning banner.
5. **Resolved.** The Civil Division concurred with the OIG's recommendation to develop and maintain an inventory of authorized or approved non-Civil Division owned laptop computers for contractors, subcontractors, and other entities providing contract support services for the Civil Division. The Civil Division stated that this recommendation will take 9-12 months to fully implement. This recommendation can be closed when we receive documentation showing that an inventory of authorized non-Civil Division owned laptop computers for contractors, subcontractors, and other entities has been created.
6. **Resolved.** The Civil Division concurred with the OIG's recommendation to ensure that all non-Civil Division laptop computers used to process DOJ data are encrypted or that the Civil Division requires contractors to use encrypted hardware provided by the Civil Division. The Civil Division stated that this recommendation will take 9-12 months to fully implement. This

recommendation can be closed when we receive documentation showing that all non-Civil Division laptop computers used to process DOJ data are encrypted or that the Civil Division requires contractors to use encrypted Civil Division-provided hardware.

7. **Resolved.** The Civil Division concurred with the OIG's recommendation to ensure that all contract support providers are aware of security procedures for handling DOJ data in accordance with DOJ policy. The Civil Division stated that this recommendation will take 9-12 months to fully implement. This recommendation can be closed when we receive documentation showing that all contract support providers are aware of security procedures for handling DOJ data in accordance with DOJ policy.