U.S. Department of Justice
Office of the Inspector General
Evaluation and Inspections Division

Review of the Department of Justice's Reporting Procedures for Loss of Sensitive Electronic Information

June 2007

I-2007-005

INTRODUCTION

The federal government's loss of sensitive information, often stored on laptop computers (laptops), has generated significant concern.[1] For example, in May 2006 a laptop with 26.5 million records containing sensitive information on veterans and their spouses was stolen from a Department of Veterans Affairs employee. In June 2006, the Department of Agriculture disclosed that three of its systems were compromised, potentially making available the names, social security numbers, and photographs of 26,000 of its employees, contractors, and retirees in the Washington, D.C., area. In August 2006, a laptop containing personal information on 30,000 Navy applicants, recruiters, and prospects fell off a motorcycle belonging to a recruiter and was observed by a roadside worker being picked up by someone in a car.

According to a 2006 report on federal agency data breaches by the House Committee on Government Reform, 19 federal departments and agencies have reported hundreds of instances of loss of personally identifiable information (PII) since January 2003.[2] The number of individuals affected in each incident ranged from 1 to 26.5 million. The type of information lost and potentially compromised included personal information such as names, home addresses, photographs, dates of birth, social security numbers, fingerprints, medical information, tax information, earnings records, user passwords, law enforcement information requests, and personal information on law enforcement employees.

[1] The Department of Justice defines sensitive information in its *Security Program Operating Manual* as, "Any information, the loss, misuse, modification of, or unauthorized access to, could affect the national interest, law enforcement activities, the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but that has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy."

[2] See Committee on Government Reform, U.S. House of Representatives, 109th Congress, *Agency Data Breaches Since January 1, 2003*, October 13, 2006. According to Office of Management and Budget (OMB) Memorandum M-06-19, July 12, 2006, PII is defined as "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."

These incidents highlight the risk that PII and other sensitive data can be compromised when computers or storage media such as disks, CD-ROMs, and flash drives, are lost or stolen. The PII on lost or stolen computers or storage media can be used to commit fraud or identity theft. Further, other types of sensitive information, such as proprietary business information or sensitive law enforcement information, could be inappropriately disclosed or copied for purposes of industrial espionage, retaliation, or other crimes.

Because of the importance of these issues, the OIG conducted this review to identify the policies and procedures nine Department components are required to follow to (1) report and identify losses of sensitive information, including PII and classified information, and (2) notify affected parties of losses of their sensitive information.[3]

The report begins with a background section that provides information about the roles and responsibilities of the staff within the Department's Office of the Chief Information Officer and the development of the Department's reporting procedures by that office. The report then describes the Department's reporting and incident response procedures. The report also contains appendices that provide a detailed description of each of the nine components' reporting procedures and policies.

This review is intended to provide an overview of the policies and procedures the Department has established to respond to and report computer security incidents.[4] However, in this review, we did not verify that components followed Department reporting procedures or verify the accuracy of the data contained in the database used by the Department to track these incidents. Rather, the intent of this review was to identify

[3] The nine components reviewed were the Bureau of Alcohol, Tobacco, Firearms and Explosives; Federal Bureau of Prisons; Criminal Division; Drug Enforcement Administration; Executive Office for United States Attorneys; Federal Bureau of Investigation; Justice Management Division; Tax Division; and United States Marshals Service. These nine components were chosen because they accounted for a large percentage of the total number of all computer security incidents, including PII and other sensitive data loss incidents, reported to the Department between December 2005 and November 2006.

[4] According to DOJCERT, a computer security incident is any unexpected, unplanned event that could have a negative impact on IT resources. Computer security incidents can include the loss of both classified and unclassified systems, unauthorized removal of computer equipment, and exploited weaknesses in a computer system that allows unauthorized access to password files. DOJCERT considers losses of sensitive information to be a subset of computer security incidents.

what policies had been established, and what procedures were being followed in reporting computer security incidents.

RESULTS IN BRIEF

The Department has developed a computer security Incident Response Plan that provides standard reporting procedures that all Department components are required to follow. In December 2003, the Department developed a template to standardize procedures Department-wide for responding to and handling computer security incidents. The template includes detailed instructions for handling and reporting computer security incidents. The Department's Computer Emergency Readiness Team (DOJCERT) developed this Incident Response Plan template under the direction of the Department's Chief Information Officer and has updated it periodically to reflect new statutory and Office of Management and Budget (OMB) requirements and emerging computer security threats.[5]

In November 2006, the Department included in the template for the first time reporting requirements for PII and other data loss incidents. The new requirements include a 1-hour timeframe for reporting these incidents and define the information that components need to gather when a PII or other data loss occurs or when data has been potentially compromised. The 1-hour timeframe was first established by OMB in July 2006 in a memorandum issued to the Chief Information Officers of all federal agencies.

All of the Department's components are required to develop their own Incident Response Plans that conform to the template. The nine Department components the OIG reviewed have all developed their own component-specific Incident Response Plans that follow the template. However, as of April 2007, two of the nine components had not yet submitted their revised Incident Response Plans to DOJCERT for approval.

To supplement their Incident Response Plans, the components have developed internal policies, memorandums, or practices for their employees that provide more detailed reporting and incident response procedures within their own internal chains of command. While all nine

[5] DOJCERT is the organization to which all Department components are required to report computer security incidents, including PII and other data loss incidents. Established in 2000 within the Department's Office of the Chief Information Officer, it operates 24 hours a day, 7 days a week. A more detailed explanation of DOJCERT's role and responsibilities is provided in the Background section of this report.

components reviewed have multiple policies, two of the components have policies that provide contradictory or faulty chain-of-command reporting procedures. Specifically, ATF's staff has received contradictory instructions on which office is the primary point of contact for reporting computer security incidents. In addition, the USMS's policy instructs employees to report computer security incidents to staff titles and internal departments that either no longer exist or are inaccurate.

Four of the nine components have developed separate procedures for staff to follow if an incident is reported after normal business hours. One component's procedures were the same 24 hours a day. The remaining four components have no specific written procedures covering such incidents.[6] We found that at least 19 percent of the incidents reported between December 2005 and November 2006 occurred after hours (6:00 p.m. to 6:00 a.m.).

Reporting Procedures

Officials interviewed in the nine components told us that they believed that their employees were following the correct internal chain-of-command reporting procedures when reporting computer security incidents. Although this review did not examine or verify that employees actually were following Department or component procedures, we did note two issues, one specific to a component and one affecting multiple components. In reviewing the information that one component – the Federal Bureau of Investigation (FBI) – provided and information from DOJCERT's database, we noticed a discrepancy between the number of lost electronic devices that had been reported within the FBI and the number of lost electronic devices that the FBI had reported to DOJCERT.[7] We sought additional information to determine whether the FBI's employees were following reporting procedures. We also found indications that most of the components were not always reporting computer security incidents in a timely manner.

Compliance with Reporting Procedures

We found that the FBI did not always follow its or the Department's reporting procedures. Specifically, the FBI did not report

[6] Two of these components have developed draft procedures, but as of April 2007, those procedures had not yet been issued.

[7] DOJCERT maintains the Department's Incident Response and Vulnerability Patch Database. commonly called the Archer Database. See pages 18-19 of this report for a more detailed explanation of how we identified this discrepancy.

all incidents involving the loss of electronic devices to DOJCERT or all incidents involving classified information to the Department's Security and Emergency Planning Staff.[8] The FBI received internal reports of 35 lost or stolen laptops between December 2005 and November 2006. Although the FBI is required by the Department's Incident Response Plan template to report such losses to DOJCERT, the FBI did so for only 7 of those laptops. Additionally, the FBI received internal reports of 107 classified computer security incidents during that same time period, but did not report any of these incidents to the Security and Emergency Planning Staff as required in the Department's *Security Program Operating Manual*. This manual requires all Department components to report all classified incidents related to information technology (IT) to the Department's Security Officer and DOJCERT. We also did not examine whether the Department's other 31 components are reporting all classified computer security incidents to the Security and Emergency Planning Staff and DOJCERT as required.

Timeliness of Reporting All Computer Security Incidents

We examined 1,501 computer security incidents in the DOJCERT Archer Database that were reported by the 9 components between December 1, 2005, and November 30, 2006, and determined that the components were not always meeting the timeframes established in the Incident Response Plans. In particular, we found that the components were not meeting the 1-hour reporting timeframe established by the Department and OMB for reporting computer security incidents involving PII.[9] Only one of the nine components reviewed, the Tax Division, submitted timely reports for nearly all of its computer security incidents.

[8] The Security and Emergency Planning Staff (SEPS) is required to track all reports of losses of classified information for the Department. A more detailed explanation of SEPS's role and responsibilities is provided in the Background section of this report.

[9] DOJ, Reporting Incidents Involving Data Loss and Personally Identifiable Information, Vance Hitch, CIO, August 7, 2006; and OMB Memorandum M-06-19 for Chief Information Officers, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, Karen S. Evans, July 12, 2006. The former document establishes a 1-hour reporting timeframe after the discovery or detection of a security incident for components to report to DOJCERT and the latter document established a 1-hour timeframe for DOJCERT to report to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT). US-CERT is a partnership between the Department of Homeland Security and the public and private sectors established in 2003 to protect the nation's Internet infrastructure.

The DOJCERT Incident Response Plan template and the components' Incident Response Plans include reporting timeframes for each of seven categories of computer security incidents, such as Unauthorized Access and Improper Usage, that all Department components are required to report to DOJCERT.[10] We found that between December 2005 and November 2006, the Tax Division made timely reports for 95 percent of its reported computer security incidents. The other eight components made timely reports for between 37 percent and 84 percent of their security incidents.

For PII incidents in the nine components, we found that only 15 percent were reported to DOJCERT within 1 hour of occurrence, and none of these incidents were subsequently reported to US-CERT within the same 1-hour timeframe. Further, DOJCERT reported only 12 percent of PII incidents to US-CERT within 1 hour of the time it received notification from the components.[11] Officials from three components remarked that the 1-hour timeframe was impractical and unrealistic.

OMB's guidance and the Department's guidance differ as to when the 1-hour timeframe begins and ends. On July 12, 2006, OMB issued a memorandum requiring federal agencies to report computer security incidents involving PII to US-CERT within 1 hour of discovery.[12] The Department's November 2006 revision of the Incident Response Plan template requires that the components report PII incidents to DOJCERT within 1 hour of discovery. Our analyses found that the guidance in the DOJCERT Incident Response Plan template appears to conflict with the July 12, 2006, OMB memorandum. The timeliness standard in OMB's policy requires that incidents be reported to US-CERT within 1 hour of discovery or detection. By allowing 1 hour for reporting just to DOJCERT, the Department's incident response plan does not ensure compliance with OMB's 1-hour reporting requirement for US-CERT. Component staff, in fact, told us that employees interpret the OMB requirement to mean that they have 1 hour to report to DOJCERT.

[10] See Appendix XII for a description of the seven categories and the associated timeframes. An additional category is used for training exercises only.

[11] The period we used for measuring timeliness in reporting PII incidents was between July 12, 2006 (when OMB began requiring that PII incidents be reported within 1 hour), and November 30, 2006.

[12] OMB Memorandum M-06-19.

For our analysis, we assessed the amount of time that that elapsed between an incident's occurrence and when the component reported the incident to DOJCERT. For those incidents that were reported within 1 hour to DOJCERT, we determined if they were also reported to US-CERT within the same 1-hour period. We also assessed the amount of time that elapsed between when DOJCERT received notice of an incident and when DOJCERT reported that incident to US-CERT.

Ensuring that All Incidents Are Reported

Officials from the nine components reviewed all identified training as the primary method for ensuring employees are aware of the reporting requirements. The two training courses most often mentioned were the Department's annual Computer Security Awareness Training and the components' Information Technology Rules of Behavior.

Notification to Affected Parties

There is no Department requirement to notify the affected parties in the event of loss of PII, and none of the nine components we reviewed has a policy addressing the notification of affected parties. Further, according to a recent Government Accountability Office report, ". . . existing laws do not require agencies to notify the public when data breaches occur . . . ."[13] However, the Department's Privacy and Civil Liberties Office is currently finalizing a Department-wide notification policy.

Determining Type of Data Lost

To determine if sensitive information may have been lost or compromised during a reportable computer security incident, all nine components stated that they interview the employee who reported the incident. For most components, this consists of informal questioning in an attempt to assist the employee in reconstructing what occurred and to identify the information that a lost electronic device contained. Five components also supplement the employee's interview by using computer forensic techniques to determine what information or files were stored or accessed by the employee. For example, the Criminal Division and the Drug Enforcement Administration reported that for incidents involving a

[13] Testimony of David M. Walker, Comptroller General, Government Accountability Office, *Privacy: Preventing and Responding to Improper Disclosures of Personal Information* (GAO-06-833T), before the House Committee on Government Reform, June 8, 2006.

lost BlackBerry device, the BlackBerry Exchange Server allows them to identify the e-mails that were received and sent the last time the device was used.

Definitions of Sensitive Information, PII, and Reportable Data Loss

The Department has developed a standard definition for sensitive information but has not developed its own definitions for PII and a reportable data loss. Seven of the components we reviewed have also developed definitions of sensitive information while the remaining two components use the Department's definition. The components' definitions are similar to the one the Department issued in its *Security Program Operating Manual.*

To define PII, the Department relies on OMB's July 12, 2006, memorandum. However, two components stated that this definition may lead components to over-designate information as PII because the OMB definition is too broad and overly vague. Most of the components expressed the opinion that the Department needs to develop its own definition of PII.

We found no standard Department definition of a reportable data loss. The components provided a variety of answers when defining a reportable data loss. Their responses were generally in line with the causes of data loss that the DOJCERT Incident Response Plan template describes, such as hacker intrusion through network and system defenses or the loss or theft of a laptop, removable storage medium, or portable computing device containing PII or sensitive information.

Best Practices in Increasing Employee Awareness

Four of the nine components are taking additional steps to either minimize unauthorized access to sensitive information or educate employees on their reporting responsibilities. For example:

- The Tax Division reinforces employees' awareness of the 1-hour reporting requirement for loss of PII by posting this information prominently on its intranet.

- The Criminal Division displays a variety of security tips, including procedures for reporting computer security incidents, on the computer monitors when employees first log in.

- JMD Personnel staff receive verbal briefings on the procedures for reporting computer security incidents when they are given the equipment necessary to use the Justice Secure Remote Access system and also receive a wallet card summarizing those reporting procedures.

- BOP policy requires that to remove sensitive information from a BOP facility, an employee must obtain written approval from the Chief Executive Officer (CEO) of the facility. When requesting approval, the medium of the sensitive information (e.g., paper documents, electronic files), a description of the equipment being used and the contents, and the purpose for the removal must be documented along with the CEO's approval.[14]

Recent Developments and Future Plans

The Department frequently updates its guidance on data loss incidents and privacy issues and changes its policies to address newly identified needs. For example, the Department's Privacy and Civil Liberties Office and Office of the Chief Information Officer are developing a Department-wide policy on notifying affected parties in the event of loss of PII. Once this policy is finalized, DOJCERT plans to issue an addendum to its Incident Response Plan template explaining the notification procedures and the components' roles in them. Additionally, the Department stated that DOJCERT plans to release an *Incident Response Handbook* during fiscal year 2007. The handbook will provide guidance to the components on information-gathering techniques during and following an incident, techniques for determining the type of data included on lost equipment, and methods for identifying the level of residual risk associated with each incident.

Conclusion and Recommendations

The Department has developed an Incident Response Plan template to standardize the procedures that all Department components are required to follow to report computer security incidents. However, as of April 2007, two of the nine components have not updated their Incident Response Plans to conform to the Department's November 2006 revision, which requires all computer security incidents involving PII to be reported within 1 hour. The same two components have also issued internal policies that have contradictory instructions on the primary point of contact for reporting computer security incidents and that direct

[14] BOP, Information Security, P1237.13, March 31, 2006, Chapter 2, p. 14.

employees to contact officials with non-existent titles in departments that no longer exist. Another area where we found divergence among the components was in procedures for reporting incidents that occur after normal business hours. Four of the components have developed additional reporting procedures for incidents reported after hours, one component's procedures are the same 24 hours a day, and the remaining four components do not have specific written procedures covering after-hours incidents.

While all of the components stated that they believed their staff followed procedures established for reporting computer security incidents through their chains of command to component headquarters, we found that the FBI was not always following the reporting procedures outlined in its or the Department's Incident Response Plans.

We also found that components were not always reporting computer security incidents to DOJCERT within the timeframes established in the Department's Incident Response Plan template. In particular, the components were not consistently reporting PII incidents within 1 hour to DOJCERT, and none of the PII incidents in the Department were reported to US-CERT within 1 hour of discovery or detection. DOJCERT and component staff interpret the guidance from the Department and OMB differently as to whom the incident is to be reported to within 1 hour. Therefore, we believe clarification is needed on who must receive the report within 1 hour of discovery or detection – component IT staff, DOJCERT, or US-CERT.

Neither the Department nor any of the components we reviewed have developed procedures for notifying affected individuals in the event of a loss of PII, which could cause a delay in notifying affected individuals and increase their risk of falling victim to fraud or identity theft. The Department is developing a policy on this issue, and we believe it should be promptly finalized and distributed to Department components.

The Department has issued a standard definition of sensitive information in its *Security Program Operating Manual*, and seven components have developed component-specific definitions of sensitive information that are similar to the Department's definition. However, the Department has not developed its own definitions of PII and what constitutes a reportable data loss. At least seven of the nine components expressed the opinion that the Department should develop its own, more specific definition of PII.

Four components have developed what we consider to be Best Practices to increase employee awareness of the reporting requirements for computer security incidents. We believe the Department and its other components should examine these practices and determine if any should be adopted Department-wide.

To help the Department improve its computer security incident reporting procedures, including the procedures for reporting data loss and classified incidents, we recommend that the Department:

1. Require all components to ensure their procedures cover reporting of after-hours incidents.

2. Review the components' procedures for reporting classified incidents to ensure those procedures comply with the standards in the Department's *Security Program Operating Manual.*

3. Clarify the requirement that all losses of PII be reported within 1 hour and to whom so that all Department employees understand who to report to and when the 1-hour timeframe begins and ends.

4. Ensure all components meet the established reporting timeframes.

5. Promptly implement a Department-wide policy for notifying affected individuals in the event of a loss of PII.

6. Develop a Department-specific definition of PII.

7. Consider whether any of the procedures described as "Best Practices" should be implemented across the Department.

8. Ensure that components update their internal policies to reflect correct reporting procedures in conformance with the DOJCERT Incident Response Plan template and contain up-to-date titles of internal departments and staff.

TABLE OF CONTENTS

LIST OF ACRONYMS

ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
BOP	Federal Bureau of Prisons
CEO	Chief Executive Officer
CIO	Chief Information Officer
CRM	Criminal Division
DEA	Drug Enforcement Administration
DOJCERT	Department of Justice Computer Emergency Readiness Team
EOUSA	Executive Office for United States Attorneys
FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Management Act
ISSO	Information Systems Security Officer
IT	Information Technology
JMD	Justice Management Division
NCIC	National Crime Information Center
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
SEPS	Security and Emergency Planning Staff
SPOM	The Department of Justice's *Security Program Operating Manual*
USAO	United States Attorney's Office
US-CERT	United States Computer Emergency Readiness Team
USMS	United States Marshals Service

BACKGROUND

The background section provides information about the roles and responsibilities of the staff within the Department's Office of the Chief Information Officer and the development of the Department's computer security incident reporting procedures by that office. We also describe the Department's reporting requirements for classified computer security incidents.

The Chief Information Officer

Within the Department of Justice (Department), the management and protection of sensitive information, including personally identifiable information (PII), falls under the responsibility of the Office of the Chief Information Officer (CIO). The CIO, who is also the Deputy Assistant Attorney General for Information Resource Management, is responsible for overseeing the management, acquisition, and integration of the Department's information resources, including:

- Formulating Department-wide information technology (IT) policies and strategic plans;
- Ensuring that investments in IT processes are aligned with the Department's overall strategic goals, budget, and enterprise architecture;
- Making recommendations concerning the IT budget requests of the Department's components; and
- Overseeing the security of the Department's information systems.[15]

The creation of the role of CIOs in the government is attributed to the Clinger-Cohen Act of 1996, previously called the Information Technology Management Reform Act of 1996.[16] This Act mandates a CIO in each federal agency.

[15] Attorney General Order 2572-2002 designates the CIO to carry out the duties assigned under 40 U.S.C. § 1425. DOJ Order 2880.1B, Information Resources Management Program, September 27, 2005, further establishes the authority of the Office of the CIO in the Department and outlines the office's duties and responsibilities.

[16] Designation of Chief Information Officers, 44 U.S.C. § 3506, February 10, 1996.

Since the appointment of the current CIO in 2002, the following IT security policies have been issued:

July 2002	DOJ IT Strategic Plan
November 2003	DOJ Order 2640.2E, Information Technology Security
May 2004	DOJ Computer System User Rules of Behavior
May 2005	DOJ *Security Program Operating Manual*
September 2005	DOJ Order 2880.1B, Information Resources Management Program
November 2005	DOJ Order 2740.1, Use and Monitoring of DOJ Computers and Computer Systems
June 2006	DOJ IT Strategic Plan, Fiscal Years 2006-2011
August 2006	Information Technology Security Program Management Plan
November 2006	DOJ Incident Response Plan Template, (originally created in December 2003, updated annually)
December 2006[17]	IT Security Standards (17 policies)
December 2006	DOJ Configuration Management Plan

In these documents, the Department has established extensive security policies and incident response procedures for the Department's IT systems. Additionally, several memorandums have been issued by the CIO providing further requirements on reporting computer security incidents, particularly those involving loss of PII.

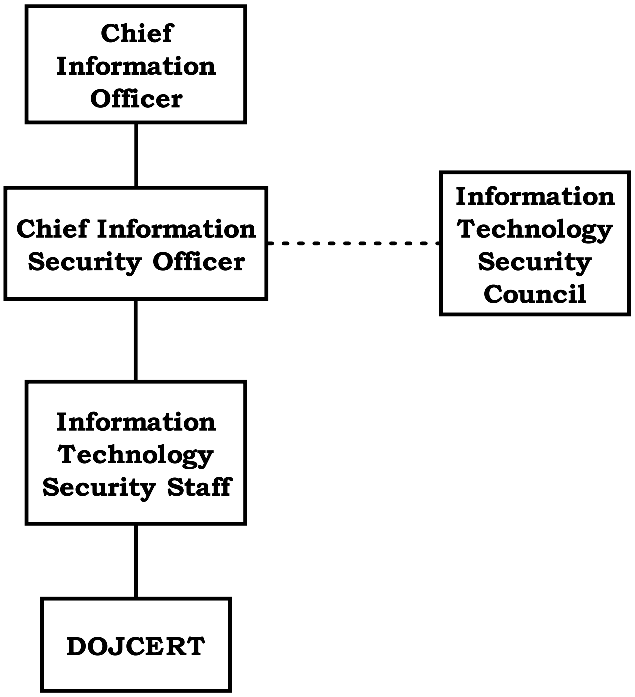
The Office of the CIO falls organizationally within the Department's Justice Management Division (JMD).[18] The CIO has supervisory responsibility for five offices. One of these five offices is the Information

[17] The Federal Information Security Management Act (FISMA) of 2002 mandates that all IT systems in the government must undergo certification and accreditation once every 3 years. The National Institute for Standards and Technology (NIST) issued government-wide technical guidance for the certification and accreditation process in Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (February 2005). The publication identifies 17 categories of information security, called "control families," and sets minimum security standards within each control family. The Office of the CIO has written 17 separate policies describing how the Department will meet the standards in each control family.

[18] JMD is the management arm of the Department and is led by the Assistant Attorney General for Administration. The four offices in JMD are the Controller; Human Resources; Information Resource Management; and Policy, Management, and Planning.

Technology Security Staff, whose mission is to ensure the protection of the Department's information systems that collect, process, transmit, store, or disseminate either classified or Sensitive But Unclassified information, including PII.[19] The Information Technology Security Staff is headed by the Chief Information Security Officer. See Chart 1 for the Office of the CIO organization chart.

Chart 1: Organizational Chart for the Office of the Chief Information Officer


Chief Information Officer
Chief Information Security Officer
Information Technology Security Council
Information Technology Security Staff
DOJCERT

The Chief Information Security Officer

In June 2003, the CIO appointed a Chief Information Security Officer to help support the Department's IT security mission and goals, and to develop and maintain a Department-wide information security program. This program includes issuing procedures for detecting, reporting, and responding to security incidents, and conducting periodic risk assessments that seek to identify the magnitude of harm that could result from unauthorized access, use, disclosure, disruption,

[19] The other four offices under the CIO are E-Government Services, Policy and Planning, Operations Services, and Enterprise Solutions.

modification, or destruction of the information and information systems that support the operations and assets of the Department.[20]

The Chief Information Security Officer also is responsible for ensuring the Department's compliance with various federal laws, standards, and directives regarding electronic information security, such as the E-Government Act of 2002, the Federal Information Security Management Act (FISMA) of 2002, the Privacy Act of 1974, National Institute of Standards and Technology (NIST) standards, and Office of Management and Budget (OMB) and DOJ directives. (See Appendix X for a summary description of each of these laws, standards, and directives.)

The CIO's Information Technology Security Council

The CIO created an Information Technology Security Council (the Council), chaired by the Chief Information Security Officer, in August 2003 to address the security goals outlined in the Department's IT Security Program Management Plan, which is the guiding document for managing the Department's overall IT security program. The plan establishes goals and performance measures; identifies initiatives, resources, schedules, and controls; provides templates, guidelines, and tools for IT staff to ensure systems meet federal and Department certifications and accreditations; and describes IT security management strategies, roles and responsibilities, program implementation, and the goals and action plans for the security program.

The Council is composed of IT security staff from each of the Department's components. The Council created four project management teams devoted to different areas of IT security.[21] These teams develop templates and implementation guidance documents, and test cases for developing, implementing, and testing the security controls in the specific areas of security that are covered by each team.

Cyber Defense Operations Team. The Department's response to a computer security incident is handled by the Cyber Defense Operations Team, which is chaired by the Department of Justice Computer Emergency Readiness Team's (DOJCERT) Project Manager and also includes representation from all of the Department components. The

[20] Information Technology Security Program Management Plan, Version 5.41, August 2006.

[21] The four project management teams are the IT Security Employee Services Team, the Computing Environment and Enclave Defense Team, the Cyber Defense Operations Team, and the Certification and Accreditation Management Team.

team meets monthly to discuss changes in incident reporting standards and procedures. Any comments are incorporated into the Incident Response Plan template, which is updated at the beginning of each fiscal year. For example, in the November 2006 Incident Response Plan template, DOJCERT included for the first time reporting requirements for incidents of PII and data loss, and defined the information that components need to gather when a data loss occurs or when data has been potentially compromised.

DOJCERT

DOJCERT was established in 2000 within the Information Technology Security Staff to fulfill the Department's obligations under the Government Information Security Reform Act, which directed federal agencies to "establish procedures for detecting, reporting, and responding to security incidents."[22] In November 2003, the Department updated its Information Technology Security order to require all components to respond to and report all computer security incidents to DOJCERT in accordance with rules set forth by DOJCERT.[23] These requirements for incident response and reporting are also part of the Department's efforts to attain the goals in Homeland Security Presidential Directive 7, which established a national policy for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.[24]

DOJCERT is a centralized incident response team that provides Department-wide support for computer security incidents and can be contacted 24 hours a day, 7 days a week.[25] The CIO has assigned DOJCERT the responsibility to provide leadership and guidance to all Department components in incident response planning and plan evaluation. DOJCERT's stated objective is to work in coordination with all Department component incident response teams to provide a central

[22] Pub. L. No. 106-398, the Government Information Security Reform Act, October 30, 2000. This Act expired in November 2002 and was superseded by FISMA in December 2002.

[23] DOJ Order 2640.2E, Information Technology Security, November 28, 2003.

[24] Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003.

[25] DOJCERT is located in Rockville, Maryland.

point of information collection, information dissemination, and response planning.

DOJCERT Incident Response Plan. DOJCERT is the organization to which all Department components are required to report computer security incidents, including data loss incidents. DOJCERT developed an Incident Response Plan template in December 2003 that established a Department-wide standardized approach for handling and reporting computer security incidents and that provided detailed incident response procedures within each component. DOJCERT periodically updates the template to reflect new statutory or OMB requirements or emerging computer security threats.

As explained earlier, DOJCERT revised its Incident Response Plan template in November 2006 to require for the first time that the components add language that identifies the loss of PII as a distinct type of reportable incident, and that defines the category and timeframe (1 hour) that should be used to report these data loss incidents.

The Incident Response Plan identifies seven categories of computer security incidents, such as Unauthorized Access and Improper Usage, that all Department components are required to report to DOJCERT, and includes reporting timeframes for each category.[26] The DOJCERT Incident Response Plan also provides:

- Requirements for incident response handling,
- Agency objectives for incident response handling,
- Organizational structure for incident response handling,
- Roles and responsibilities for key elements and personnel,
- Preparation and training guidelines,
- Policy and procedures for handling incidents, and
- Incident reporting procedures for all Sensitive But Unclassified and classified incidents.

Each Department component is required to develop its own Incident Response Plan that is aligned with the requirements and goals of the DOJCERT Incident Response Plan. In addition, each component must conduct an exercise of that plan at least annually.[27] DOJCERT

[26] See Appendix XII for a description of the seven categories and the associated timeframes. An additional category is used for training exercises only.

[27] The IT Security Standard Incident Response Control Family, November 2006, written by DOJCERT, describes the Department's overall policy for incident response.

(Cont'd.)

reviews each component's plan annually for compliance with the DOJCERT Incident Response Plan template.

DOJCERT has also instituted regular monthly reporting requirements (in addition to the required reporting of security incidents as they occur) to collect additional details on incidents in two of the reporting categories and to promote component familiarity with the DOJCERT process and staff.[28] The DOJCERT template is a technical document for component IT staff and is not distributed to all employees.

DOJCERT's Archer Database. To manage and track the reporting process, DOJCERT maintains an Incident Response and Vulnerability Patch Database (commonly called the Archer Database, after the vendor that developed it) where incidents are recorded and monitored. Using the Archer Database, reports can be generated on all Sensitive But Unclassified incidents. All the components we reviewed have online access to this database.[29] Each component can choose whether to complete the online Incident Report Form, e-mail or fax the completed form to DOJCERT, or telephone DOJCERT with the specifics of the incident. Department components with access to the Archer Database are able to use it for their own internal tracking purposes as well.

DOJCERT's Educational and Technical Support. DOJCERT also provides information resources, technical support, coordination activities, and educational support to the Department on incident response. Furthermore, DOJCERT tracks the implementation of critical patches on IT systems and applications. As part of its educational

The policy requires that each component develop and implement a formal written incident response policy, provide annual training to incident response personnel, test its incident response plan at least annually, develop a capability for responding to and recovering from incidents that have occurred, track and document incidents, report incidents promptly, and provide assistance to users who need to report security incidents.

[28] The two categories are Spam and Scans/Probes/Attempted Access. Scans, probes, and attempted access include "any activity that seeks to access or identify a Department computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service." See Appendix XII.

[29] The United States Marshals Service (USMS) informed us that only one person had been trained to use the Archer Database and that this individual had been on extended sick leave. Due to work schedules and recent staff vacancies in the security office, the USMS has been unable to train any other staff to access the Archer Database. Therefore, the USMS reports new incidents to DOJCERT via telephone instead of through the Archer Database.

support responsibilities, DOJCERT provides annual training to all component IT security staff to meet the FISMA requirements for Incident Response and IT Contingency Plan training and testing.[30] Since 2002 DOJCERT has developed and distributed online, to component CIOs and their staff, a quarterly newsletter that provides the Department with security awareness information, security tips, training information, and updates to DOJCERT operations.

DOJCERT Reporting Responsibilities. DOJCERT reports all of the Department's computer security incidents, except spam, to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT). US-CERT is a partnership between the Department of Homeland Security and the public and private sectors that was established in 2003 to protect the nation's Internet infrastructure. US-CERT also coordinates defenses against and responses to cyber attacks across the nation.[31] It is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

Additionally, DOJCERT is responsible for reporting all actual or potential data loss incidents to appropriate components in the Department. If the incident involves PII, it is reported to the Department's Privacy and Civil Liberties Office in the Office of the Deputy Attorney General. If there is evidence that a crime has occurred – for example, computer crimes, child pornography, e-mail threats, successful malicious activity directed towards the Department, or financial fraud – then these incidents are reported to the Federal Bureau of Investigation (FBI), the U.S. Secret Service, the Criminal Division, the Office of the Inspector General (OIG), or other appropriate agencies. Additionally, DOJCERT reports any information that could be relevant to terrorism investigations to the FBI and the U.S. Secret Service.

Reporting Classified Incidents

Classified incident reporting in the Department is governed by the Department's *Security Program Operating Manual* (SPOM).[32] Classified

[30] FISMA established the responsibilities of agencies to assess their security risks.

[31] Department of Homeland Security website, www.us-cert.gov/aboutus.html, February 28, 2007.

[32] DOJ *Security Program Operating Manual,* May 2005.

computer security incidents are to be reported by the components' Security Programs Manager to the Department Security Officer, who is the Director of the Security and Emergency Planning Staff (SEPS).[33] SEPS maintains a separate database to track these reports. The SPOM defines nine categories of classified security incidents that are to be reported, including:

> Any incident involving a possible loss, compromise, or suspected compromise of classified information, foreign or domestic, and . . . Any event involving [IT] systems, equipment or media which may result in disclosure of classified information to unauthorized individuals, or that results in unauthorized modification or destruction of system data, loss of computer system processing capability, or loss or theft of computer system media.[34]

The SPOM also requires components to report all IT-related classified incidents to DOJCERT in addition to notifying the Department Security Officer. DOJCERT notifies SEPS of all data loss incidents, including classified data losses, via e-mail. DOJCERT, in its Incident Response Plan template, requests that components, if possible, sanitize and declassify the incident report and then report it through normal channels to DOJCERT.

[33] The Department Security Officer reports to the Deputy Assistant Attorney General for Human Resources, who reports to the Assistant Attorney General for Administration. The Assistant Attorney General for Administration is the head of the Justice Management Division.

[34] DOJ *Security Program Operating Manual,* § 1-302(a) and (e).

PURPOSE, SCOPE, AND METHODOLOGY OF THE OIG REVIEW

Purpose

The purpose of this review was to provide an overview of the policies and procedures that Department components are required to follow to respond to and report computer security incidents.

Scope

This review examined nine of the Department's components:

- Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF);
- Federal Bureau of Prisons (BOP);
- Criminal Division;
- Drug Enforcement Administration (DEA);
- Executive Office for United States Attorneys (EOUSA);
- Federal Bureau of Investigation (FBI);
- Justice Management Division (JMD);
- Tax Division; and
- United States Marshals Service (USMS).

These 9 components accounted for 69 percent of the total number of all computer security incidents reported to DOJCERT between December 2005 and November 2006. According to the 9 components, taken together they have 229 databases that contain PII. These databases contain personal information from or about the public and therefore present a potentially serious risk to the public if this sensitive data is lost.

We identified each component's reporting procedures for the following situations:

- Losses of electronic devices, including hardware such as laptops and BlackBerry devices that potentially could contain sensitive information; and
- Compromises of sensitive information, including PII and classified information, through unauthorized access to computer systems or data.

We also determined:

- Whether the components had procedures to identify the information that was lost,
- Whether the components had procedures to notify the affected parties, and
- Whether the components had procedures for reporting computer security incidents outside normal business hours.

However, the review did not:

- Examine Department or component procedures for tracking, protecting, or controlling sensitive information or PII prior to the reported occurrences;
- Examine Department or component procedures for tracking, protecting, or controlling removable electronic media, including disks, CD-ROMs, and flash drives;
- Verify components' compliance with reporting procedures by means of a case file review;
- Verify that all computer security incidents are reported; or
- Verify the accuracy of the data contained in the Archer Database.

Methodology

The methodology used in this review consisted of interviews with 40 staff, document review and analysis, and data analysis.

Interviews. To determine the computer security incident reporting procedures followed by each of the components, we interviewed officials from all nine components, including the headquarters-based individuals with primary responsibility for contacting DOJCERT on behalf of the component. For those components with field offices, we interviewed a field office official with computer security incident reporting responsibilities. We also interviewed officials from the Office of the CIO, the Security and Emergency Planning Staff (SEPS), and the Office of the Deputy Attorney General to discuss Department-wide standards for computer security incident reporting and Department-wide issues concerning privacy.

Department Component	Officials Interviewed
ATF	• Chief, Product Assurance Branch • Information Systems Security Officer • Project Manager, Information Systems Security Office • Special Agent in Charge, Investigations Division • Assistant Special Agent in Charge, Investigations Division • Assistant Special Agent in Charge, Miami Field Division
BOP	• Chief, IT Planning and Development • Chief, Information Security • Information Technology Security Administrator • Program Analyst, Information Security Programs Section • Supervisory Management Analyst, Internal Affairs Division • Computer Services Manager, Allenwood Federal Correctional Complex
Criminal Division	• Director, Information Technology Management • Information Systems Security Officer
DEA	• Chief, Information Security • Deputy Chief Information Officer • Deputy Chief Counsel • Security Programs Manager • Assistant Special Agent in Charge, Houston Field Division
EOUSA	• Information Systems Security Officer • Senior Security Programs Specialist • District Office Security Manager, Southern District of New York • Executive Assistant U.S. Attorney, Central District of California
FBI	• Unit Chief, Assurance Management Unit • Unit Chief, Security Compliance Unit • Unit Chief, Enterprise Security Operations Center • Unit Chief, Major Theft Unit • Assistant Special Agent in Charge, New York Field Division
JMD	• Chief Information Security Officer, Office of the CIO • Deputy Director for Information Technology Security, Office of the CIO • DOJCERT Project Manager, Office of the CIO • Assistant Director for Information Safeguards and Security Oversight, SEPS • Security Specialist, SEPS • Information Systems Security Officer, Personnel Staff
Tax Division	• Executive Officer • Associate Executive Officer • Information Technology Specialist
USMS	• Chief, Enterprise Management • Chief Deputy U.S. Marshal, District of Colorado
Office of the Deputy Attorney General	• Chief Privacy and Civil Liberties Officer

Document Review and Analysis. We reviewed federal, Department, and component procedures and policies regarding computer security incident reporting. These included various federal statutes, memorandums issued by OMB, US-CERT's Concept of Operations, Department Orders, memorandums issued by the Deputy Attorney General, memorandums issued by the Department's CIO, the DOJCERT Incident Response Plan Template, the Department's IT Security Standard on Incident Response, documents detailing the Department's compliance with FISMA, the components' Incident Response Plans, and the components' IT security policies. See Appendices X and XI for a complete list of the acts, directives, standards, and component policies we reviewed.

Data Analysis. DOJCERT maintains a database titled the DOJCERT Incident Response and Vulnerability Patch Database, also known as the Archer Database, for tracking all computer security incidents, including data loss incidents. We downloaded data from this database to identify all computer security incidents reported by the nine components that occurred in the 12-month period of December 1, 2005, through November 30, 2006. Within each incident category defined in the DOJCERT Incident Response Plan, we analyzed compliance with reporting timeframes.

We also conducted an analysis of this data to determine the number of incidents reported by each component that involved actual or potential loss of PII or classified information. We determined that an incident involved actual or potential loss of PII if the database showed that the components answered "Yes" or "Unknown," respectively, when asked if an incident involved personal data loss. We determined that an incident potentially involved classified information based on the incident description provided in the database. We did not verify this data with either DOJCERT or the components' internal records.

In addition, we analyzed the components' compliance with the July 12, 2006, OMB memorandum requiring all federal agencies to report actual or potential losses of PII within 1 hour.

RESULTS OF THE REVIEW

The Department has developed a computer security Incident Response Plan that provides standard reporting procedures that all Department components are required to follow. In December 2003, at the direction of the Chief Information Security Officer, DOJCERT developed an Incident Response Plan template to standardize procedures Department-wide for responding to and handling computer security incidents. Each of the nine Department components we reviewed has developed an Incident Response Plan that conforms to the DOJCERT template. The following is a summary discussion of:

- Reporting procedures that the nine components have established for reporting and responding to computer security incidents;
- Determining the type of data lost; and
- Defining sensitive information, PII, and reportable loss.

In addition, we identify best practices, recent developments, and future plans. Detailed discussions of the above areas for each component are included in Appendices I through IX.

Reporting and Responding to Computer Security Incidents

Written Procedures

All of the nine components the OIG reviewed have official written procedures for their employees to follow when reporting computer security incidents. All nine components have developed their own component-specific Incident Response Plans that follow the DOJCERT Incident Response Plan template. The Incident Response Plans are the primary written guidance for the components' IT staff response to and reporting of computer security incidents involving sensitive information, including PII, to DOJCERT.

DOJCERT updates the Incident Response Plan template as needed, but at least annually, to reflect new statutory or OMB requirements or emerging computer security threats. In November 2006, DOJCERT revised its Incident Response Plan template to require for the first time that the components add language that identifies loss of PII as a distinct type of reportable incident and that defines the category and timeframe (1 hour) for reporting these data loss incidents.

As of April 2007, seven of the nine components we reviewed had updated Incident Response Plans that conformed to the November 2006 DOJCERT template revision: the BOP, the Criminal Division, the DEA, EOUSA, the FBI, JMD, and the Tax Division. The remaining two components, ATF and the USMS, had not yet submitted their revised Incident Response Plans to DOJCERT for approval.

The DOJCERT template provides instructions for reporting computer security incidents to DOJCERT, but it does not dictate the internal reporting requirements within each component. Therefore, to supplement the DOJCERT template, each component has developed additional policies, memorandums, or practices for its employees that provide more detailed reporting and incident response procedures. These supplemental policies provide further tools to help components respond to computer security incidents or identify when data loss may have occurred. For example, components have policies that tell their employees how to identify reportable computer security incidents and how to contact internal IT staff to report such incidents. While all nine components reviewed have multiple policies, two of the components have policies that provide contradictory or faulty chain-of-command reporting procedures. ATF staff has received contradictory instructions on which office is the primary point of contact for reporting computer security incidents. The USMS policy instructs employees to report computer security incidents to staff titles and internal departments that either no longer exist or are inaccurate. Appendix XI identifies the policies that each component developed and relies on for guidance related to computer security incidents.

Four of the nine components have developed separate procedures for staff to follow if an incident is reported after normal business hours. One component's procedures were the same 24 hours a day. The remaining four components have no specific written procedures covering such incidents.[35] We found that at least 19 percent of the incidents reported between December 2005 and November 2006 occurred after hours (6:00 p.m. to 6:00 a.m.).

Between December 1, 2005, and November 30, 2006, the 9 components the OIG reviewed reported 1,501 computer security

[35] Two of these components have developed draft procedures but, as of April 2007, those procedures had not yet been issued.

incidents to DOJCERT. During this same period, all 40 Department components reported 2,162 incidents. (See Table 1 for the number of incidents reported by each of the nine components reviewed.)

Table 1: Total Computer Security Incidents, by Component

Component	**Incidents**
ATF	70
BOP	252
Criminal Division	24
DEA	43
EOUSA	463
FBI	206
JMD	402
Tax Division	22
USMS	15
DOJCERT	4
Total	**1,501**

Source: Archer Database

Of the 1,501 incidents reported by the 9 components in this review, 19 incidents involved the actual loss of PII and an additional 228 incidents involved the potential loss of PII. The number of PII incidents could be underreported because until July 2006 there was no requirement to identify and report whether incidents involved the loss of PII.[36] Prior to July 2006, the components' internal records may have indicated whether incidents involved the loss of PII, but the components were not required to report this detail to DOJCERT. According to the Archer Database, 5 actual losses of PII and 43 potential losses of PII were reported during the 8 months between the December 1, 2005, start of our review period and July 12, 2006, when the reporting requirement went into effect.

The 1,501 incidents also included 57 incidents involving classified information.[37] The remaining 1,215 incidents involved spam, computer viruses, or other types of incidents that did not involve either PII or

[36] OMB Memorandum M-06-19 for Chief Information Officers, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, Karen S. Evans, July 12, 2006.

[37] One of the incidents involving the actual loss of PII also involved classified information. Seventeen of the incidents involving the potential loss of PII also involved classified information.

classified information. Table 2 gives the breakdown of the types of incidents reported by the nine components.

Table 2: Types of Incidents Reported by Nine Components

Component	Total number of incidents	Incidents involving PII only	Incidents involving classified information only	Incidents involving both PII and classified information	All other types of incidents
ATF	70	7	0	1	62
BOP	252	24	0	0	228
Criminal Division	24	1	6	4	13
DEA	43	6	2	0	35
EOUSA	463	140	2	2	319
FBI	206	32	24	11	139
JMD	402	18	5	0	379
Tax Division	22	0	0	0	22
USMS	15	0	0	0	15
DOJCERT	4	1	0	0	3
Total	**1,501**	**229**	**39**	**18**	**1,215**

Source: Archer Database

Compliance with Reporting Procedures

IT security staff and other staff with related duties we interviewed in all nine components stated that their staff generally followed procedures established for reporting computer security incidents through their chain of command up to component headquarters. In this review, we did not test to verify those statements. However, in reviewing the information the FBI provided to us and the information we analyzed from the Archer Database, we noticed a discrepancy between the number of lost electronic devices that had been reported within the FBI and the number of lost electronic devices that the FBI had reported to DOJCERT. Therefore, we asked the FBI some additional questions to determine whether they were following their reporting procedures. We found that the FBI was not always following the procedures required in the DOJCERT Incident Response Plan template or its own required procedures.

Within the FBI, computer security incidents are reported to two separate offices, but only one of those offices is required to report incidents to DOJCERT. The FBI's *Security Policy Manual* requires staff to report computer security incidents to the FBI's Security Compliance Unit. The FBI's four Incident Response Plans require staff to report computer security incidents to the FBI's Enterprise Security Operations

Center.[38] Only the Enterprise Security Operations Center reports computer security incidents to DOJCERT.

We found that the FBI is not in full compliance with DOJCERT's requirement that all lost or stolen electronic devices be reported.[39] In reviewing the information the FBI provided, and in our analysis of information from the Archer Database, we noticed a discrepancy between the number of lost electronic devices that had been reported to the FBI's Security Compliance Unit and the number of lost electronic devices that had been reported to the Enterprise Security Operations Center and to DOJCERT. For the period from December 2005 through November 2006, FBI employees reported 35 lost or stolen laptops to the Security Compliance Unit, but only 7 lost or stolen laptops were reported to the Enterprise Security Operations Center.[40] The underreporting of incidents to the Enterprise Security Operations Center caused an underreporting of incidents to DOJCERT and US-CERT. Table 3 below shows the number of lost or stolen FBI laptops that were reported.

Table 3: Number of FBI Laptops Reported Lost or Stolen between December 1, 2005, and November 30, 2006

Reported to the Security Compliance Unit*	35
Reported to the Enterprise Security Operations Center*	6
Reported to DOJCERT via the Enterprise Security Operations Center**	7

* Based on FBI documents.

** Based on OIG analysis of Archer Database.

Sources: FBI documents and Archer Database

In addition to not reporting all incidents of lost electronic devices to DOJCERT, we found the FBI was underreporting classified computer security incidents to both SEPS and DOJCERT. The Department's *Security Program Operating Manual* (SPOM) requires that all

[38] All four of the Incident Response Plans conform to the DOJCERT template.

[39] The OIG recently conducted an audit that describes in greater detail the FBI's processes for identifying and reporting lost or stolen laptop computers. See OIG, *The Federal Bureau of Investigation's Control Over Weapons and Laptop Computers Follow-Up Audit,* Audit Report 07-18, February 2007.

[40] FBI officials told us that 35 lost or stolen laptops were reported to the Security Compliance Unit. We reviewed data from DOJCERT's Archer Database and determined that seven lost or stolen laptops had been reported to the Enterprise Security Operations Center and to DOJCERT. We did not verify those reports.

Department components report classified computer security incidents, including those involving losses of classified information, to SEPS. At least 72 classified computer security incidents that were reported to the Security Compliance Unit by FBI employees between December 2005 and November 2006 were not reported to either SEPS or DOJCERT as required. FBI policy does not require the Security Compliance Unit to report any computer security incident to any entity outside the FBI, including SEPS. FBI policy only requires the Enterprise Security Operations Center to report computer security incidents to DOJCERT. For additional details on FBI compliance with reporting procedures, see Appendix VI.

Timeliness of Reporting All Computer Security Incidents

We found that the components were not always timely in reporting all occurrences of computer security incidents, especially those involving PII, to DOJCERT. Further, DOJCERT was not always timely in reporting all occurrences of computer security incidents, especially those involving PII, to US-CERT.

Timeliness of Components' Reporting Computer Security Incidents Overall. Between December 2005 and November 2006, 66 percent of the computer security incidents were reported in a timely manner by the nine components overall. However, only one of the nine components reported nearly all of its computer security incidents within specified timeframes. We analyzed data from DOJCERT's Archer Database to determine the amount of time that elapsed between the occurrence of a potential or actual computer security incident and the time the incident was reported to DOJCERT. The timeframes are defined in the DOJCERT Incident Response Plan template and the components' Incident Response Plans and vary for the seven categories of computer security incidents the plans address.[41]

Between December 2005 and November 2006, the Tax Division made timely reports for 95 percent of its reported computer security incidents. The other eight components reported between 37 percent and 84 percent of their security incidents on a timely basis. Table 4 shows

[41] See Appendix XII for a detailed description of each category. An additional category is used for training exercises only.

the timeliness in reporting to DOJCERT by category of incident for all components.[42]

Table 4: Nine Components' Timeliness in Reporting Category 1-7 Incidents to DOJCERT

	Reporting timeframe*	**Incidents reported**	**Reported within timeframe**	**Reported after timeframe**	**Could not compute timeliness****
Category 0 (Exercise/Test)	None	29	N/A	N/A	29
Category 1 (Unauthorized Access)	1 hour	100	12	79	9
Category 2 (Denial of Service)	2 hours	4	1	3	0
Category 3 (Malicious Code)	1 day	402	143	166	93
Category 4 (Improper Usage)	1 week	264	144	84	36
Category 5 (Scans/Probes)	1 month	180	149	15	16
Category 6 (Investigation)	None	241	N/A	N/A	241
Category 7 (Spam)	1 month	281	233	11	37
Total		**1,501**	**682**	**358**	**461**

* For purposes of this table, "reporting timeframe" refers to the timeframes defined in the components' Incident Response Plans.

** We could not compute timeliness for some incidents because the Archer Database contained no information to indicate when DOJCERT received the reports. We also could not compute timeliness for incidents in Categories 0 and 6, which do not have timeframes.

Source: Archer Database

Timeliness of Components' Reporting of PII Incidents. The 9 components in this review reported 199 potential or actual losses of PII to DOJCERT between July 12, 2006, and November 30, 2006. Only 15 percent of those incidents were reported within 1 hour to DOJCERT, and none of the PII incidents were reported to US-CERT within 1 hour of discovery or detection. Table 5 provides data on the nine components' timeliness in reporting actual and potential PII incidents to DOJCERT.

[42] Our calculations are based on Categories 1 through 5 and Category 7. We did not include incidents found in Categories 0 and 6 because they had no associated time criteria, nor did we include incidents for which the Archer Database contained no information to indicate when DOJCERT received the report that an incident had occurred.

Table 5: Nine Components' Timeliness in Reporting Actual and Potential PII Incidents to DOJCERT

Category	Incidents occurring on or after 07/12/06	Reported within 1 hour (TIMELY)*	Reported after 1 hour	Could not compute timeliness**
ATF	6	4	2	0
BOP	7	1	6	0
CRM	4	0	4	0
DEA	6	1	5	0
EOUSA	134	19	101	14
FBI	26	0	25	1
JMD	16	2	12	2
TAX	0	N/A	N/A	N/A
USMS	0	N/A	N/A	N/A
Total	**199**	**27**	**155**	**17**

Note 1: Because the Archer Database does not require components to identify the date and time an incident was *discovered*, we relied on the components' reports of the date and time each incident *occurred* to conduct our analysis.

Note 2: PII incidents were reported in several incident categories.

* The 1-hour timeframe for PII incidents is defined in OMB Memorandum M-06-19.

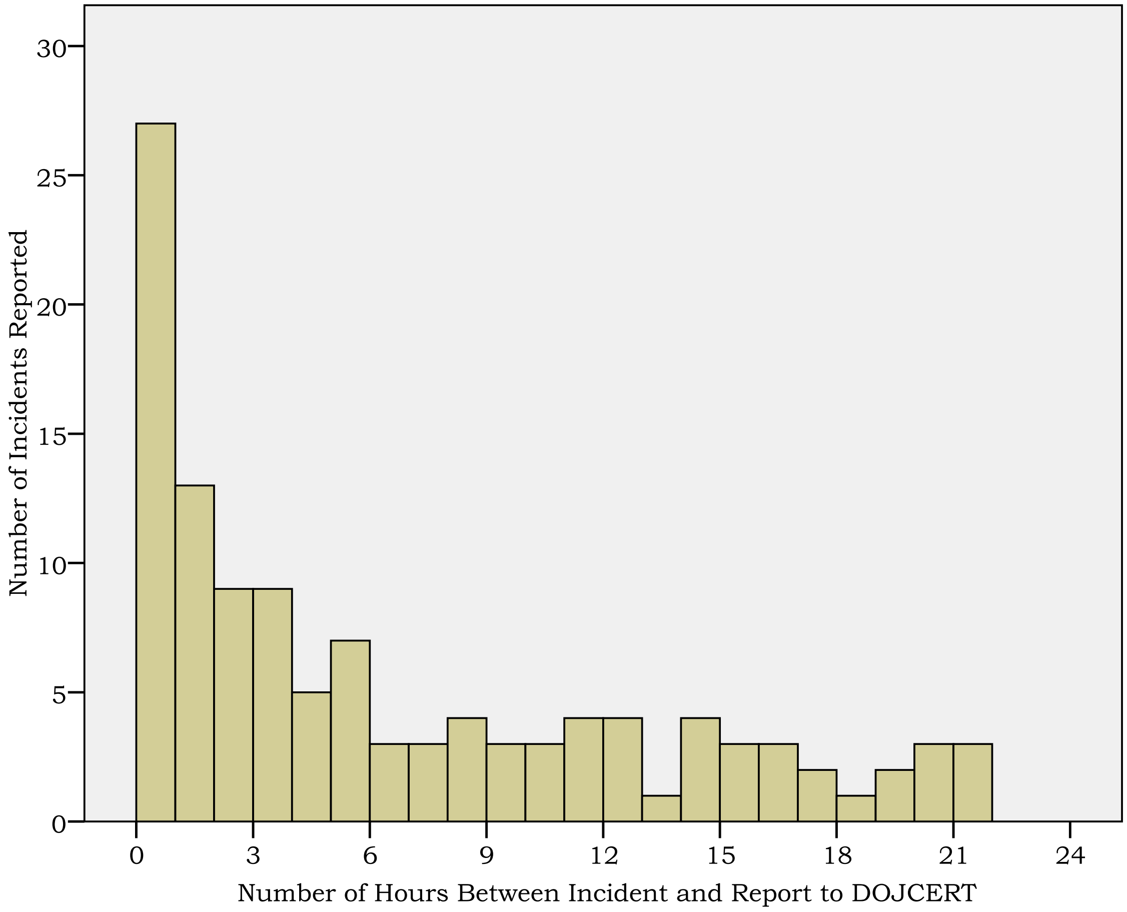
** We could not compute timeliness for some incidents because the Archer Database contained no information to indicate when DOJCERT received the reports.

Source: Archer Database

Although OMB requires that all potential or actual losses of PII be reported within 1 hour to US-CERT, the median time for the nine components to report such incidents to DOJCERT was slightly over 12 hours.[43] Chart 2 shows the components' timeliness in reporting PII incidents to DOJCERT within the first 24 hours after occurrence. The components reported 66 PII incidents (36 percent) to DOJCERT more than 24 hours after occurrence.

[43] The median refers to the middle number of a group of numbers; that is, half the numbers have values that are greater than the median, and half the numbers have values that are less than the median. For example, the median of 2, 3, 3, 4, 5, 7, and 10 is 4.

Chart 2: Components' Timeliness in Reporting PII Incidents to DOJCERT Within the First 24 Hours After Occurrence



Source: Archer Database

When discussing their timeliness in reporting PII incidents, the nine components' staff told us there was a lack of clarity as to when the 1-hour reporting timeframe begins and ends. OMB's July 12, 2006, memorandum requires federal agencies to report computer security incidents to US-CERT within 1 hour of discovery. However, the Department's November 2006 revision of its Incident Response Plan template requires that PII incidents be reported by the components within 1 hour of discovery or detection to DOJCERT. By allowing 1 hour for reporting to DOJCERT, the incident response plan appears to conflict with the OMB directive that incidents be reported to US-CERT within 1 hour of discovery or detection.

Component staff told us that component employees interpret the OMB requirement to mean that they have 1 hour to report incidents to their component's IT staffs. We found the components' IT staffs interpret the OMB requirement to mean that they have 1 hour to report incidents to DOJCERT. DOJCERT interprets the OMB requirement to mean that it has 1 hour from the time it is notified of an incident to report that incident to US-CERT. Therefore, the components may need further clarification from the Department on when the 1-hour window for reporting PII incidents begins and ends, and who must receive the report within 1 hour of discovery or detection – component IT staff, DOJCERT, or US-CERT. Officials from three components remarked that the 1-hour timeframe was impractical and unrealistic.

For our analysis, we assessed the amount of time that that elapsed between an incident's occurrence and when the component reported the incident to DOJCERT. For those incidents that were reported within 1 hour to DOJCERT, we determined if they were also reported to US-CERT within the same 1-hour period. We also assessed the amount of time that elapsed between when DOJCERT received notice of an incident and when DOJCERT reported that incident to US-CERT.

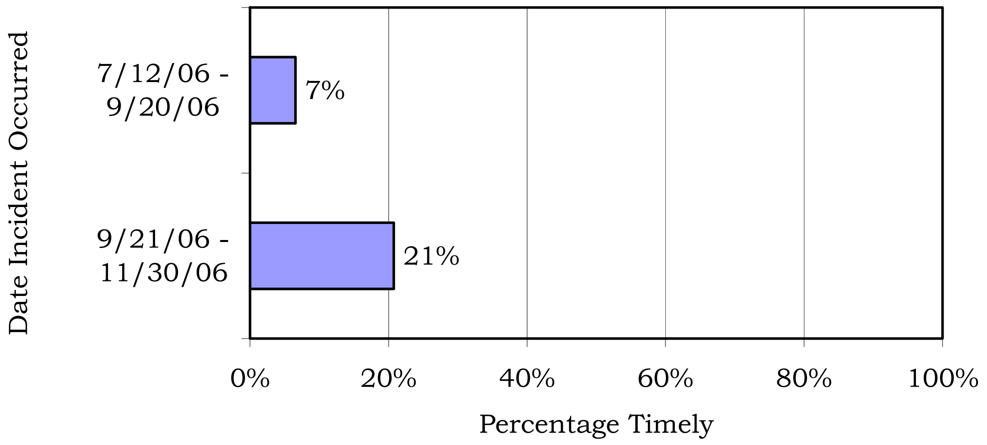
Because the 1-hour requirement is relatively recent, we also examined whether the components' timeliness in reporting PII incidents to DOJCERT was improving. To examine this, we compared incidents that occurred between July 12, 2006, and September 20, 2006, with incidents that occurred between September 21, 2006, and November 30, 2006.[44] We found that the components' reporting data suggests that their performance improved over time. Only 5 of the 76 potential or actual losses of PII that occurred between July 12, 2006, and September 20, 2006 (7 percent) were reported to DOJCERT within 1 hour of the incidents' occurrence.[45] However, between September 21, 2006, and November 30, 2006, 22 of the 106 potential or actual losses of PII (21 percent) were reported to DOJCERT within 1 hour of the incidents' occurrence.[46] (See Chart 3.)

[44] We chose September 20, 2006, as the cutoff date because it is halfway between July 12, 2006, and November 30, 2006.

[45] We could not analyze 10 incidents for timeliness because there was no information in the Archer Database to indicate when DOJCERT received the reports.

[46] We could not analyze seven incidents for timeliness because there was no information in the Archer Database to indicate when DOJCERT received the reports.

Chart 3: Timeliness of Reporting PII Incidents Improved Over Time



Source: Archer Database

Timeliness of DOJCERT's Reporting of PII Incidents. Between December 2005 and November 2006, DOJCERT reported 61 percent of computer security incidents to US-CERT in a timely manner. However, our analysis also showed that DOJCERT reported only 12 percent of the potential or actual losses of PII to US-CERT within 1 hour of being notified by the components of the incidents.[47] DOJCERT reported 88 percent of the potential or actual losses of PII to US-CERT more than an hour after being notified by the components.[48] See Table 6 for data on DOJCERT's timeliness in reporting PII incidents to US-CERT.

[47] For the 199 potential or actual losses of PII, we compared the date and time the incident was reported to DOJCERT with the date and time the incident was reported to US-CERT, to determine how well DOJCERT was meeting the 1-hour timeframe. We could not analyze 64 of the incidents for timeliness because there was no information in the Archer Database to indicate when the report was submitted to US-CERT.

[48] DOJCERT staff report incidents to US-CERT by completing a web-based form. DOJCERT staff also print a copy of each completed form and maintain the paper copies in their records. The date and time the form was printed appears automatically at the bottom of the page. DOJCERT staff type this information into the Archer Database for tracking purposes.

Table 6: DOJCERT's Timeliness in Reporting PII Incidents to US-CERT				
	Incidents occurring on or after 07/12/06 (reported by nine components)	Reported within 1 hour (TIMELY)*	Reported after 1 hour	Could not compute timeliness**
Total	**199**	**16**	**119**	**64**

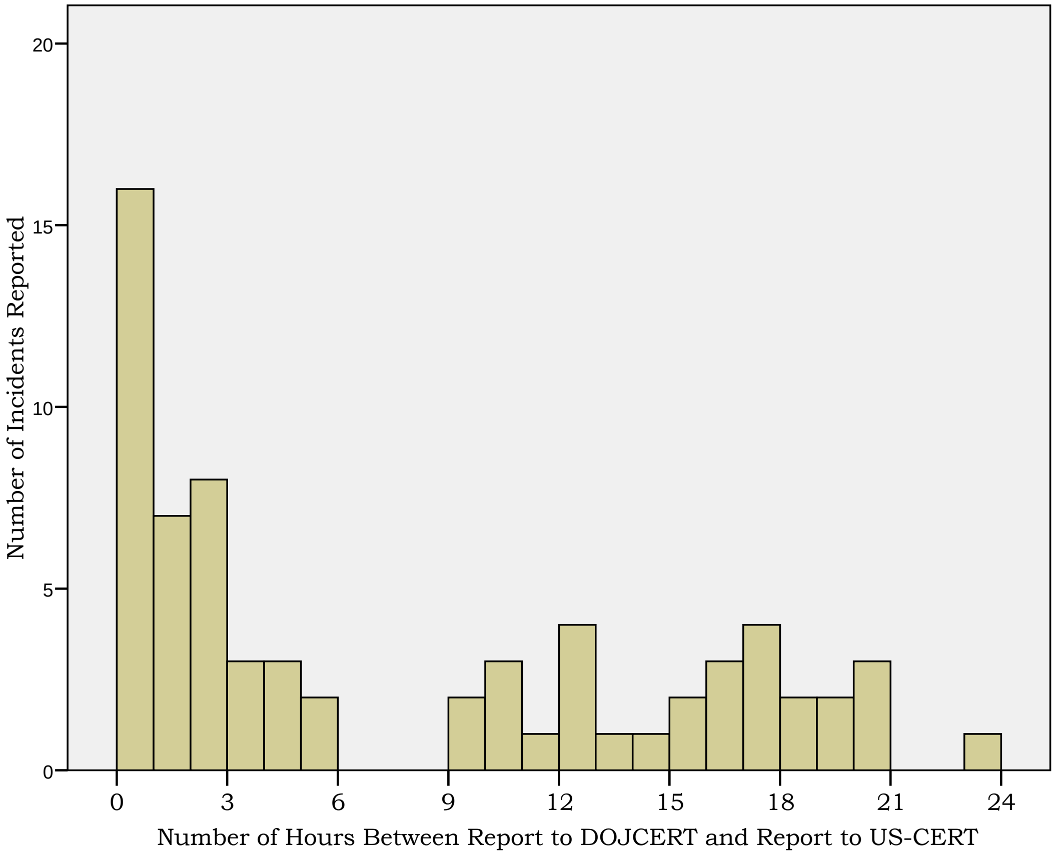
* The 1-hour timeframe for PII incidents is defined in OMB Memorandum M-06-19.

** We could not compute timeliness for the 64 incidents because the Archer Database contained no information to indicate when the report was submitted to US-CERT.

Source: Archer Database

The median time taken by DOJCERT to report potential or actual losses of PII to US-CERT was slightly under 24 hours, with 67 of the incidents being reported more than 24 hours after the components notified DOJCERT that they had occurred. Chart 4 shows DOJCERT's timeliness in reporting PII incidents to US-CERT within the first 24 hours after receiving notice that the incident had occurred.

Chart 4: DOJCERT's Timeliness in Reporting PII Incidents to US-CERT Within the First 24 Hours After Receiving Notice



Source: Archer Database

Ensuring that All Incidents Are Reported

The nine components stated that they cannot ensure that all incidents are reported, but they identified training as their primary method for ensuring that employees are aware of the requirement to report data loss incidents, including those involving PII. This training includes:

- *Computer Security Awareness Training* – Seven of nine components identified the Department's annual Computer Security Awareness Training as a way to ensure that all employees are aware of the reporting requirements.[49] This training consists of a 1-hour online PowerPoint presentation. The fiscal year 2007 Computer Security Awareness Training included, for the first time, a section on data loss reporting procedures, including PII. Additionally, the training defines computer security incidents, reviews the protection of systems information, and explains the consequences of lost or breached sensitive information.

- *Standards of Conduct and IT Rules of Behavior* – Two components use the Department's Standards of Conduct, and seven components use their own IT Rules of Behavior as other forms of training to inform all employees of their responsibilities related to computer use, including reporting all computer security incidents or vulnerabilities (as well as losses of sensitive information), accountability for and confidentiality of federally owned information, and reporting any loss or damage to laptops or BlackBerry devices.[50] All of those components' employees must read and sign the IT Rules of Behavior.

Two components use additional methods to make employees aware of the requirement to report data loss incidents:

- The Criminal Division displays security tips on computer monitors after employees have entered their passwords and are waiting for the computers to connect to the division's network.

[49] The seven components were ATF, the Criminal Division, the DEA, the FBI, JMD, the Tax Division, and the USMS.

[50] The two components that identified Standards of Conduct were ATF and the DEA. The seven components that identified IT Rules of Behavior were ATF, the Criminal Division, the DEA, the FBI, JMD, the Tax Division, and the USMS.

- The Tax Division posts the reporting requirements for data loss prominently on its intranet to make them readily accessible to employees.

Notification to Affected Parties

The Department does not have a policy to notify affected parties of a loss of PII. According to recent Government Accountability Office testimony, ". . . existing laws do not require agencies to notify the public when data breaches occur . . . ."[51] However, the Department's Privacy and Civil Liberties Office is circulating a draft Department-wide notification policy.

None of the nine components we reviewed had a written policy for notification. Four of the components reviewed offered suggestions for what the component might do if a loss of PII occurred, and three stated that the Department or OMB should develop a Department-wide notification policy so that responses would be standardized and consistent.

Determining the Type of Data Lost

All nine components informed us that when a computer security incident is discovered, the employee who reported the data loss is interviewed to determine what sensitive information the lost device or removable storage media may have contained. For most components, this consists of informal questioning in an attempt to assist the employee in reconstructing what occurred and to identify the information that the device contained. DOJCERT's Incident Response Plan template and the components' Incident Response Plans contain a section that provides general guidelines on how to respond to incidents. Three components – ATF, the FBI, and the USMS – have developed a questionnaire for use when interviewing the employee to identify the contents of the lost or compromised sensitive information.

ATF, the Criminal Division, the DEA, the FBI, and the USMS reported that they use computer forensic techniques in certain situations to supplement the employee's account of what information or files were

[51] Testimony of David M. Walker, Comptroller General, Government Accountability Office, *Privacy: Preventing and Responding to Improper Disclosures of Personal Information* (GAO-06-833T), before the House Committee on Government Reform, June 8, 2006.

stored or accessed by the employee. For example, the Criminal Division and the DEA reported that for incidents involving a lost BlackBerry device, the BlackBerry Exchange Server allows them to identify the e-mails that were received and sent the last time the device was used. All components can send a "kill signal" to a BlackBerry device once its loss is known, rendering it useless and the information on it inaccessible.

Defining Sensitive Information, PII, and Reportable Data Loss

The Department has developed a standard definition for sensitive information but has not developed its own definitions for PII and what constitutes a reportable data loss. The Department's definition for sensitive information in its *Security Program Operating Manual* (SPOM), which is distributed to the components' Security Programs Managers, is:

> Any information, the loss, misuse, modification of, or unauthorized access to, could affect the national interest, law enforcement activities, the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but that has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.[52]

However, officials in seven of the nine components we reviewed stated that basically all of their information is sensitive. One component official stated, "We've lowered it [the definition of sensitive information] to a point where nearly everything is sensitive and that's a problem."

The Department has not issued its own definition of PII but instead relies on the definition set forth in OMB Memorandum M-06-19:

> [A]ny 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.

Two components stated that this definition may lead components to over designate information as PII because the OMB definition is too broad and overly vague. One component official stated that even his government e-mail address was considered PII. Another component

[52] DOJ *Security Programs Operations Manual,* May 2005, p. A-7.

official voiced concern that the terms PII and sensitive are now interchangeable. Most of the components expressed the opinion that the Department needs to develop its own definition of PII.

In addition, we found no standard Department definition of a reportable data loss. However, the components provided a variety of answers when defining what they considered a reportable data loss. Their responses were generally in line with the causes of data loss described in the DOJCERT Incident Response Plan template, which notes that data loss can be caused by:

- Loss or theft of a laptop, removable storage medium, or portable computing device containing PII or sensitive information; . . .
- Successful phishing, pharming, or social engineering by a malicious attacker;
- Hacker intrusion through network and system defenses;
- Spyware, viruses, worms, Trojan horses, rootkits, backdoors, keyloggers, or other malicious code installed on a computing device;
- Eavesdropping of communications at public Internet access points, such as cyber cafes or hotels;
- Eavesdropping of wireless communications; . . .
- Failure to secure unattended documents containing sensitive information or PII; and
- Failure to clean sensitive information or PII from computers or storage devices before they are discarded.[53]

For more discussion on each component's definitions of sensitive information, PII, and a reportable data loss, see Appendices I through IX.

Best Practices in Increasing Employee Awareness

The OIG believes the following procedures or policies used by four of the nine components could be considered as a Best Practice. These components are taking additional steps to either minimize unauthorized access to sensitive information or to educate employees on their reporting responsibilities:

[53] DOJCERT Incident Response Plan template, version 1.3, § 9.4, November 2006. Social engineering is a collection of techniques, such as phishing and pharming, used to manipulate people into performing actions or divulging confidential information. Phishing is e-mail appearing to come from a legitimate business – a bank, or credit card company – requesting "verification" of information and warning of dire consequence if it is not done. Pharming is a hacker's attack aiming to redirect a website's traffic to another (bogus) website.

- The Tax Division reinforces employees' awareness of the 1-hour reporting requirement for loss of PII by posting this information prominently on its intranet.

- The Criminal Division displays a variety of security tips, including procedures for reporting computer security incidents, on computer monitors when employees first log in.

- JMD Personnel staff receives verbal briefings on the procedures for reporting computer security incidents when they are given the equipment necessary to use the Justice Secure Remote Access system and also receive a wallet card summarizing those reporting procedures.

- BOP policy requires that to remove sensitive information from a BOP facility, an employee must obtain written approval from the Chief Executive Officer (CEO) of the facility. When requesting approval, the medium of the sensitive information (e.g., paper documents, electronic files), a description of the equipment being used and the contents, and the purpose for the removal must be documented along with the CEO's approval.[54]

Recent Developments and Future Plans

The Department frequently updates its guidance on data loss incidents and privacy issues, or changes its policies to address a newly identified need. For example, the Department must comply with the Privacy Act, which regulates the collection, maintenance, use, and dissemination of certain types of personal information maintained by federal agencies.[55] The Act prohibits the disclosure of such information except with the prior written consent of the individual to whom the information pertains or if the disclosure falls within one of 12 statutory exceptions.[56] One of these exceptions permits disclosure for a "routine use," which is defined as "the use of such record for a purpose which is compatible with the purpose for which it was collected."[57] Consistent

[54] BOP, Information Security, P1237.13, March 31, 2006, Chapter 2, p. 14.

[55] 5 U.S.C. § 552a. For a comprehensive overview of the Act's requirements, see www.usdoj.gov/oip/04_7_1.html.

[56] 5 U.S.C. § 552a(b).

[57] 5 U.S.C. §§ 552a(b)(3) & (a)(7). An example of a published routine use for Department recordkeeping systems is disclosure to any criminal, civil, or regulatory law (Cont'd.)

with the Act, the Department and its components have published in the *Federal Register* its routine uses, "including the categories of users and the purpose of such use[s]."[58]

As part of its response to a data breach, the Department might be required to disclose information protected by the Privacy Act. For example, an official with the Privacy and Civil Liberties Office observed that the Department of Veterans Affairs, in responding to the May 2006 laptop theft, contacted other federal agencies to determine whether the contact information it had for the affected individuals was correct. In such a case, the Department would need to rely on a routine use to authorize the disclosure. Accordingly, the Privacy and Civil Liberties Office reviewed the Department's existing published routine uses and determined that a new routine use to cover this situation was required.

In October 2006, the Department published a notice in the *Federal Register* describing this new routine use. The routine use would "facilitate an effective response to a confirmed or suspected [data] breach by allowing for disclosure to those individuals affected by the breach, as well as to others who are in a position to assist in the Department's response efforts." The provision went into effect in December 2006.[59]

In February 2007, the Department's Privacy and Civil Liberties Office added a Privacy Resources page to the Department's intranet. This page provides Department employees with OMB's definition of PII, guidance and templates for preparing Privacy Impact Assessments, copies of DOJ Orders and Department guidance related to the general protection of privacy, and links to OMB privacy guidance.[60]

The Privacy and Civil Liberties Office and the Office of the CIO have also drafted a Department-wide policy on notification of affected parties

enforcement authority (whether federal, state, local, territorial, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

[58] 5 U.S.C. § 552a(e)(4)(D).

[59] The Department published a minor modification in the *Federal Register* in January 2007 to clarify that it is the Department that must confirm or suspect a data breach before disclosure would be permitted.

[60] The page defines PII as "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 a specific individual." This is the definition used in OMB Memorandum M-06-19, July 12, 2006.

in the event of a data loss incident that could result in identity theft. To ensure that the Department makes notification decisions in a consistent manner, the final determination about whether to notify affected parties in each situation will be made by high-ranking Department officials rather than by component officials. The draft policy calls for the establishment of an Identity Theft Core Management Team, which will convene in the event of a data breach and analyze the situation to determine the risk of identity theft.[61] If the management team determines that there is a risk of identity theft, and that affected individuals should be notified, the policy outlines factors that should be incorporated into the Department's response, including timing and the contents and methods of notification. Once this policy is finalized, DOJCERT plans to issue an addendum to the DOJCERT Incident Response Plan template explaining the procedures and the components' roles in relation to them.

DOJCERT told us that later in fiscal year 2007 it plans to release an *Incident Response Handbook* to provide the components with additional guidance on determining the type of data contained on lost equipment. The handbook will provide guidance to the components on:

- Information-gathering techniques during and following an incident,
- Techniques for determining the type of data included on lost equipment, and
- Methods for identifying the level of residual risk associated with each incident.

[61] The Identity Theft Core Management Team will consist of the Associate Attorney General; the Assistant Attorneys General for Administration, the Office of Legal Counsel, and the Office of Legislative Affairs; an Associate Deputy Attorney General; the CIO; the Chief Privacy Officer; the Inspector General; and the Director of the Office of Public Affairs.

CONCLUSION AND RECOMMENDATIONS

The Department has developed an Incident Response Plan template to standardize the procedures that its components are required to follow to report computer security incidents. The nine Department components reviewed by the OIG have all developed and implemented their own component-specific incident response plans that follow the Department's template. However, as of April 2007 two of the nine components had not updated their incident response plans to conform to the Department's November 2006 revision that requires all computer security incidents involving PII to be reported within 1 hour.

Although the Department's template does not require it, we also found that four of the nine components had developed additional written procedures to ensure prompt reporting of incidents that occur outside normal business hours and that one component's procedures are the same 24 hours a day. To ensure that all Department employees know who to call after hours to report a computer security incident, we believe the Department should require all of its components to develop after-hours reporting procedures.

While all of the components stated that they believed their staff followed procedures established for reporting computer security incidents through their chains of command up to component headquarters, we found indications that the FBI's IT staff was not always following the reporting procedures outlined in the Department's Incident Response Plan template or its own internal procedures. The FBI also was not reporting classified computer security incidents directly to the Security and Emergency Planning Staff, as required by the Department's *Security Program Operating Manual.*

Because this review covered only nine components, it is unknown whether other Department components are reporting all classified computer security incidents. Because of the potential risk involved in the loss of classified information, we believe the Department should review and ensure each component's compliance with the Department's requirements for the reporting of classified security incidents.

In addition, we found that the components were not always reporting all computer security incidents to DOJCERT within the timeframes established in the Department's Incident Response Plan template. In particular, the components were not consistently reporting PII incidents within a 1-hour timeframe to DOJCERT, nor was DOJCERT consistently reporting PII incidents within a 1-hour timeframe to US-CERT.

We believe the components need further clarification from the Department on when the 1-hour window for reporting PII begins and ends and who must receive the report within 1 hour of discovery or detection – component IT staff, DOJCERT, or US-CERT. Three components remarked that the 1-hour timeframe was impractical and unrealistic. We believe the Department should examine and clarify the 1-hour timeframe.

The components told us that training was the primary means of ensuring that employees report computer security incidents. The training most often used was the Department's annual Computer Security Awareness Training. Also, some components have developed additional methods of reminding their employees of the requirement to report computer security incidents that we consider Best Practices. For example, the Criminal Division displays security tips, including procedures for reporting computer security incidents, on employees' computer monitors each time they log in. We believe the Department and other components should examine these practices and determine if any should be adopted Department-wide.

Neither the Department nor any of the components we reviewed have developed procedures for notifying affected individuals in the event of a loss of PII. To address this issue, the Department's Privacy and Civil Liberties Office and the Office of the CIO are working together to develop a Department-wide policy. We believe this is a positive step and encourage the Department to finalize and issue this policy promptly.

To determine what data may have been lost as the result of a computer security incident, officials in all nine components interview the employee who reported the incident. Three components have developed questionnaires to conduct these interviews, while the other six components use more informal interviewing methods. Five components also use computer forensic techniques to supplement the information provided by the employee. DOJCERT told us that later in fiscal year 2007 it plans to release an *Incident Response Handbook* to provide the components with additional guidance on determining the type of data contained on lost equipment.

The Department has issued a standard definition of sensitive information in its *Security Program Operating Manual*, and seven components have developed component-specific definitions that are similar to the Department's definition. The other two components use the Department's definition. However, officials in seven of the nine components we reviewed stated that their components considered all information to be sensitive.

The Department currently relies on OMB's definition of PII. Most of the components reviewed expressed the opinion that the Department should develop its own, more specific definition of PII because they believed that OMB's definition was vague and overbroad. We agree and encourage the Department to clarify the definition of PII.

Recommendations

We make eight recommendations to help the Department improve its computer security incident reporting procedures, including the procedures for reporting data loss and classified incidents.

We recommend that the Department:

1. Require all components to ensure their procedures cover reporting of after-hours incidents.

2. Review each component's procedures for reporting classified incidents to ensure those procedures comply with the standards in the Department's *Security Program Operating Manual.*

3. Clarify the requirement that all losses of PII be reported within 1 hour and to whom so that all Department employees understand who to report to and when the 1-hour timeframe begins and ends.

4. Ensure all components meet the established reporting timeframes.

5. Promptly implement a Department-wide policy for notifying affected individuals in the event of a loss of PII.

6. Develop a Department-specific definition of PII.

7. Consider whether any of the procedures described as "Best Practices" should be implemented across the Department.

8. Ensure that components update their internal policies to reflect correct reporting procedures in conformance with the DOJCERT

Incident Response Plan template and contain up-to-date titles of internal departments and staff.

APPENDIX I: ATF REPORTING PROCEDURES

Introduction

Between December 2005 and November 2006, ATF reported 70 computer security incidents to DOJCERT, including 8 incidents involving potential PII loss and 1 incident potentially involving classified information.[62] According to ATF officials we interviewed, a reportable computer security incident is the loss of any data on an electronic device such as a laptop or BlackBerry device, receipt of an e-mail with a virus, or a server failure or hard drive crash in which all information was not backed up and could not be fully restored or reconstructed. ATF policy defines a computer security incident as "any event or condition that has the potential to affect the security or accreditation of an automated information system and that may result from either intentional or unintentional actions."[63] ATF considers "security incident" synonymous with "security violation," which is defined as "an event that may result in the disclosure of sensitive information to unauthorized individuals or that results in the unauthorized modification or destruction of system data, the loss of computer system processing capability, or the loss or theft of any computer system resources."[64]

ATF policy defines sensitive information as a category of unclassified information. Sensitive information is used synonymously with Sensitive But Unclassified and defined as "any information, the loss, misuse, or unauthorized access to, or modification of which could adversely affect the national interest or the conduct of federal programs."[65]

ATF has no written definition of PII but stated that in practice it defines PII as a collection of several pieces of information that can be used to identify a specific person or to construct an identity; for example, a social security number plus an address constitutes PII. What constitutes PII is a judgment call, according to ATF staff we interviewed,

[62] As of January 31, 2007, the loss of PII had been confirmed in two of these eight incidents. The remaining six incidents involve potential losses of PII.

[63] ATF H 7250.1, Automated Information System Security Program, July 26, 2006, p. B-13.

[64] ATF H 7250.1, p. B-14.

[65] ATF H 7250.1, p. B-14.

and they believed there should be more guidance from the Department regarding this definition. According to these officials, PII was not a term that was used prior to the May 2006 Department of Veterans Affairs' laptop theft.[66]

ATF uses the definition of classified information contained in Executive Order 12958, as Amended, Classified National Security Information, dated March 25, 2003.[67] This order requires all components in the Department and other executive branch agencies to use its uniform definitions.

Reporting Procedures

ATF has three written policies that define procedures for reporting computer security incidents:

- Automated Information System Security Program (ATF H 7250.1), dated July 26, 2006;
- Computer Security Incident Response Capability Incident Response Plan, dated July 24, 2006; and
- Computer Security Incident Response Capability, (ATF Order O 7500.4A), dated April 12, 2005.

The Automated Information System Security Program establishes the requirements for managing ATF's information systems to ensure the confidentiality, integrity, and accountability of those systems. It complements the DOJCERT and ATF Incident Response Plans by providing more detailed security roles and responsibilities for all employees and by expanding on the responsibilities and reporting

[66] Previous regulatory guidance from NIST on information systems did not specifically define PII and as a result, Department components were not required to identify which systems process or store PII. OMB Memorandums M-06-15 and M-06-19 issued in May and July 2006 respectively, required federal agencies to identify and ensure adequate safeguards to protect systems that contain PII, defined PII, and required, for the first time, that all incidents involving PII be reported to US-CERT within 1 hour.

[67] Executive Order 12958 provides for three classification levels. The "Top Secret" classification shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. The "Secret" classification shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security. The "Confidential" classification shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

instructions for specific staff in the event of a computer security incident. However, this policy also provides contradictory guidance to ATF employees. In two sections of the policy, it lists the Help Desk as the primary point of contact for all users to contact when reporting computer security incidents. In two other sections, it lists the Information Systems Security Office as the primary point of contact.

ATF's July 2006 Incident Response Plan conforms to the DOJCERT Incident Response Plan template, and lists the roles and responsibilities for ATF employees when reporting all suspicious computer events or incidents to ATF's Help Desk or Security Office. Section 9.3 of this plan, titled "Incident Reporting," includes ATF-specific procedures for reporting computer security incidents for the categories of technical/non-sensitive, sensitive, and classified information. DOJCERT added the data loss and PII requirements to its Incident Response Plan template in November 2006 with the requirement that all components incorporate this update by December 29, 2006. As of April 17, 2007, ATF has updated its Incident Response Plan to reflect requirements for reporting data loss incidents that include the loss of PII, but has not yet submitted it to DOJCERT for approval. ATF stated that this update will also include after-hours reporting procedures.

The Computer Security Incident Response Capability policy also describes expanded duties, responsibilities, and guidance to all ATF employees to respond to computer security incidents.

Reporting procedures are to be initiated as soon as an employee realizes that a potential computer security incident has occurred. Reporting procedures for non-sensitive, sensitive, and classified information are described below.

Non-Sensitive Information

For non-sensitive information, all ATF employees are required to report computer security incidents to the Help Desk by telephone, facsimile, e-mail, or in person, or via secure U.S. Postal Service mail. According to ATF officials, in practice the employee, although not required by written policy, will also notify his or her supervisor.[68]

[68] According to ATF officials, ATF employees in the field offices report security incidents to their field supervisors who in turn report the incidents through their chain of command to the Help Desk and the Information Systems Security Office at ATF Headquarters.

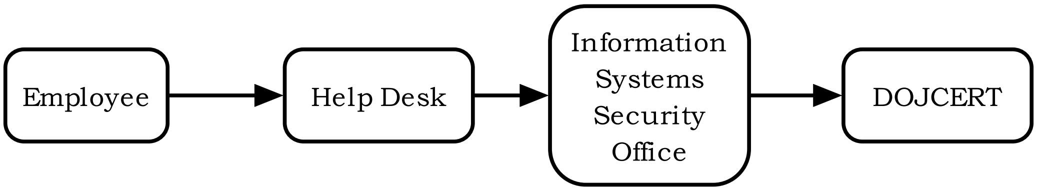
According to ATF officials, the Help Desk is used as the main point of contact for all incidents and is responsible for reporting all incident-related information to the Information Systems Security Office.[69] The person serving as the Information Systems Security Officer also serves as the Computer Security Incident Response Capability Coordinator. The Information Systems Security Office is required to report computer security incidents to DOJCERT within the timeframes required for the priority level of the incident as established in the DOJCERT Incident Response Plan. The Information Systems Security Office is required to notify DOJCERT by logging into the Archer Database and recording the incident. The Archer Database also serves as ATF's incident tracking system. When appropriate, the Information Systems Security Office may also notify managers such as the employee's Division Chief and the Office of Operations Security and even the Department's CIO.

When laptops or BlackBerry devices are lost or stolen, the ATF Investigations Division, Office of Professional Responsibility, and Security Operations must be notified. Also, in the event of a theft of a laptop or BlackBerry device, the employee involved is required to contact local law enforcement and may be required to provide a copy of the police report to his or her supervisor. For such thefts, the Information Systems Security Office also is required to notify the FBI, which should enter the stolen device's serial number into the National Crime Information Center (NCIC) system.[70] The ATF Investigations Division should be notified by the Information Systems Security Office of all incidents in which employee misconduct may be involved. Chart 5 shows ATF's reporting procedures for loss of non-sensitive information.

[69] Help Desk staff also are responsible for recording all incident reports from employees and making an initial assessment of the criticality (classified, mission-critical, and so forth) and the priority level of the incident and for assigning the incident to the Computer Security Incident Response Capability team for investigation.

[70] The NCIC is a computerized index of criminal justice information (i.e., information on criminal histories, fugitives, stolen property, missing persons, foreign fugitives, immigration violators, violent gangs, and terrorist organizations) maintained by the FBI.

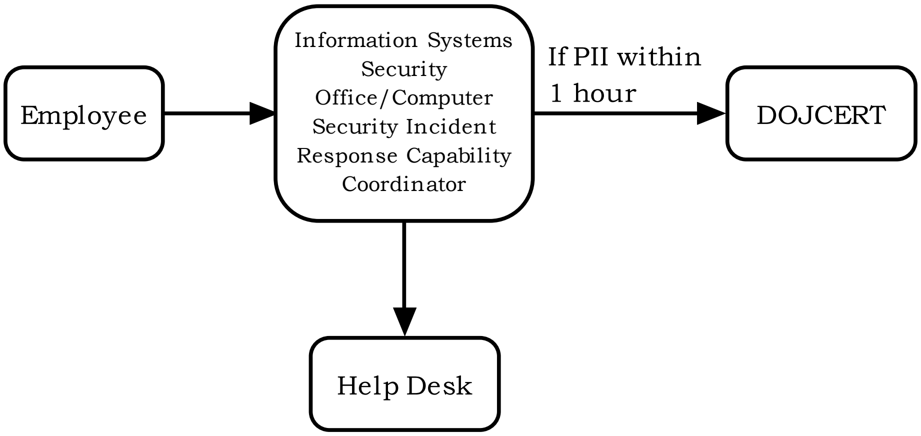
Chart 5: Flowchart of ATF's Reporting Procedures for Loss of Non-Sensitive Information



Sensitive Information

If sensitive information, including PII, is involved, ATF employees are required to contact the Information Systems Security Officer/Computer Security Incident Response Capability Coordinator directly. The Officer is then required to contact DOJCERT within the timeframes required for the category of incident. The Officer is also required to notify the Help Desk. Chart 6 shows ATF's reporting procedures for loss of sensitive information.

Chart 6: Flowchart of ATF's Reporting Procedures for Loss of Sensitive Information

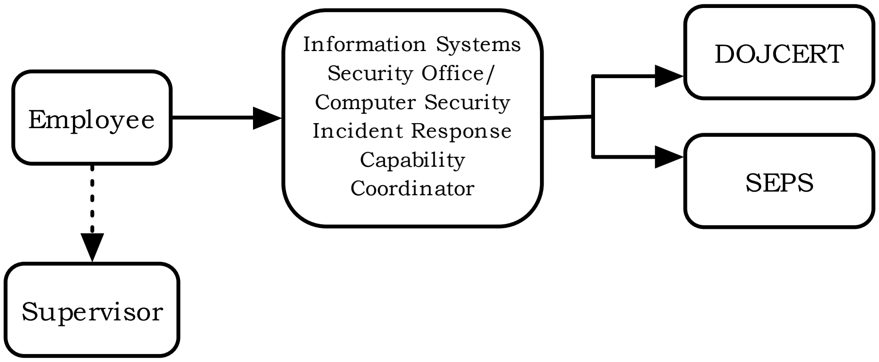

Employee
Information Systems Security Office/Computer Security Incident Response Capability Coordinator
If PII within 1 hour
DOJCERT
Help Desk

Classified Information

If classified information is involved, employees are required to contact the Information Systems Security Officer/Computer Security Incident Response Capability Coordinator in person or via secured facsimile or secure telephone. ATF officials told us that in practice the employee, although not required by written policy, will also notify his or her supervisor. The Computer Security Incident Response Capability Coordinator has a Top Secret clearance to respond to such incidents.

The Information Systems Security Office is then required to contact both DOJCERT and Security and Emergency Planning Staff (SEPS), which handles the Department's classified incidents. ATF does not provide DOJCERT or SEPS with details concerning the specific classified information that was lost or compromised. Chart 7 shows ATF's reporting procedures for loss of classified information.

Chart 7: Flowchart of ATF's Reporting Procedures for Loss of Classified Information


Employee
Supervisor
Information Systems Security Office/ Computer Security Incident Response Capability Coordinator
DOJCERT
SEPS

Indications of Compliance with Reporting Procedures

ATF officials told us that they believed their employees were following the correct reporting procedures. While we did not validate this statement, our analysis of the Archer Database showed that ATF was not always reporting computer security incidents, including PII, within the required timeframes specified in both the DOJCERT and ATF Incident Response Plans. Between December 2005 and November 2006, ATF reported 78 percent of its computer security incidents to DOJCERT within the required timeframes. Further, 66 percent of the PII incidents that occurred on or after July 12, 2006 were reported within the required 1-hour timeframe.[71] Table 7 shows ATF's reporting in each category.[72]

[71] We did not analyze incidents for timeliness that occurred before OMB established the 1-hour timeframe in July 2006.

[72] Our calculations are based on Categories 1 through 5 and Category 7. We did not include incidents found in Categories 0 and 6 because they had no associated time criteria, nor did we include incidents for which the Archer Database contained no information to indicate when DOJCERT received the report that an incident had occurred.

Table 7: ATF's Timeliness in Reporting Incidents to DOJCERT					
Category	**Reporting timeframe***	**Incidents reported**	**Reported within timeframe**	**Reported after timeframe**	**Could not compute timeliness****
Category 0 (Exercise/Test)	None	2	N/A	N/A	2
Category 1 (Unauthorized Access)	1 hour	13	2	10	1
Category 2 (Denial of Service)	2 hours	0	N/A	N/A	N/A
Category 3 (Malicious Code)	1 day	9	5	2	2
Category 4 (Improper Usage)	1 week	5	3	1	1
Category 5 (Scans/Probes)	1 month	18	17	0	1
Category 6 (Investigation)	None	5	N/A	N/A	5
Category 7 (Spam)	1 month	18	18	0	0
Total		**70**	**45**	**13**	**12**
PII incidents occurring on or after 7/12/06***	1 hour	6	4	2	0

* For purposes of this table, reporting timeframes for Categories 0-7 refer to the timeframes defined in the Incident Response Plan. Reporting timeframe for PII incidents refers to the timeframe defined in OMB Memorandum M-06-19.

** Some records did not include information to indicate when DOJCERT received the reports. Category 0 and 6 incidents, for which there are no reporting timeframes, are also included in this category.

*** PII incidents were reported in varying incident categories.

Source: Archer Database

Ensuring All Incidents Are Reported

Although ATF uses several methods to ensure employees know to report computer security incidents involving potential data loss, it relies primarily on training. ATF uses the Department's required annual Computer Security Awareness Training to educate and remind staff of their reporting responsibilities as well as of what is considered a reportable incident. All employees are also required to read and sign ATF's Conduct and Accountability and Rules of Behavior statements that address employees' responsibilities regarding the reporting of any incidents of improper use and the security and care of accountable property assigned to them. ATF also told us that it conducts property audits annually in which all staff are asked to bring in their accountable property to check against inventory. If property (such as a laptop or a BlackBerry device) is missing, the inventory uncovers the loss.

Notification to Affected Parties

ATF has not developed policies concerning notification to affected parties in the event of a loss of PII.

Determining the Type of Data Lost

To determine the type of data lost or compromised, ATF relies on interviewing the employee involved through an investigation conducted by the Computer Security Incident Response Capability team (which includes the Information Systems Security Officer as Computer Security Incident Response Capability Coordinator). The team determines, among other things, the type of incident, its level of impact, what action needs to be taken, and who should be involved in the investigation process. In interviewing the employee, the team attempts to determine what information may have been stored on the device. ATF staff told us that the Information Systems Security Office created a list of interview questions to help identify the lost or compromised data. ATF may also try to identify information on the employee's hard drive through the network system.

APPENDIX II: BOP REPORTING PROCEDURES

Introduction

Between December 2005 and November 2006, the BOP reported 252 security incidents to DOJCERT, including 24 incidents involving potential PII loss.[73] None of the incidents involved the loss of classified information.[74] According to BOP officials we interviewed, a reportable computer security incident or a reportable data loss includes the loss of PII, data lost due to a corrupted data system, violation of the Privacy Act, or an unauthorized release of information. A computer security incident or "violation" is defined by the BOP in its Information Security policy as an event such as password sharing, social engineering, computer hacking, software viruses, or other unauthorized information or system access, theft, or loss of automatic data processing equipment.[75]

The BOP defines sensitive information as information that, if released to the public, would pose an unacceptable risk to the BOP, its employees, or its inmate population. The BOP considers the term "sensitive" to be synonymous with Sensitive But Unclassified. All of the BOP's databases are considered Sensitive But Unclassified. The BOP does not have a policy that specifically defines PII as it is treated as synonymous with sensitive information.

Reporting Procedures

The BOP relies on two documents, in addition to the DOJCERT Incident Response Plan template, when reporting incidents of data loss:

1. BOP Information Security Policy, which provides primarily for the security and maintenance of information, computers, terminals, telecommunications, and data communications systems. This policy also provides incident response and reporting procedures,

[73] As of January 31, 2007, the loss of PII has been confirmed in 4 of these 24 incidents. The remaining 20 incidents involve potential losses of PII.

[74] The BOP processes classified information on a very limited basis as its networks are not authorized to process classified information. The BOP has only one stand-alone laptop computer that is authorized for classified processing, located at BOP Central Office. A second networked laptop, also physically located at BOP Central Office, is owned by the FBI who must approve all system access.

[75] BOP, Information Security, P1237.13, March 31, 2006, Chapter 2, pp. 24-25.

describes staff responsibilities related to information and computer security (including the BOP's Rules of Behavior), and sets annual training requirements to meet those responsibilities; and

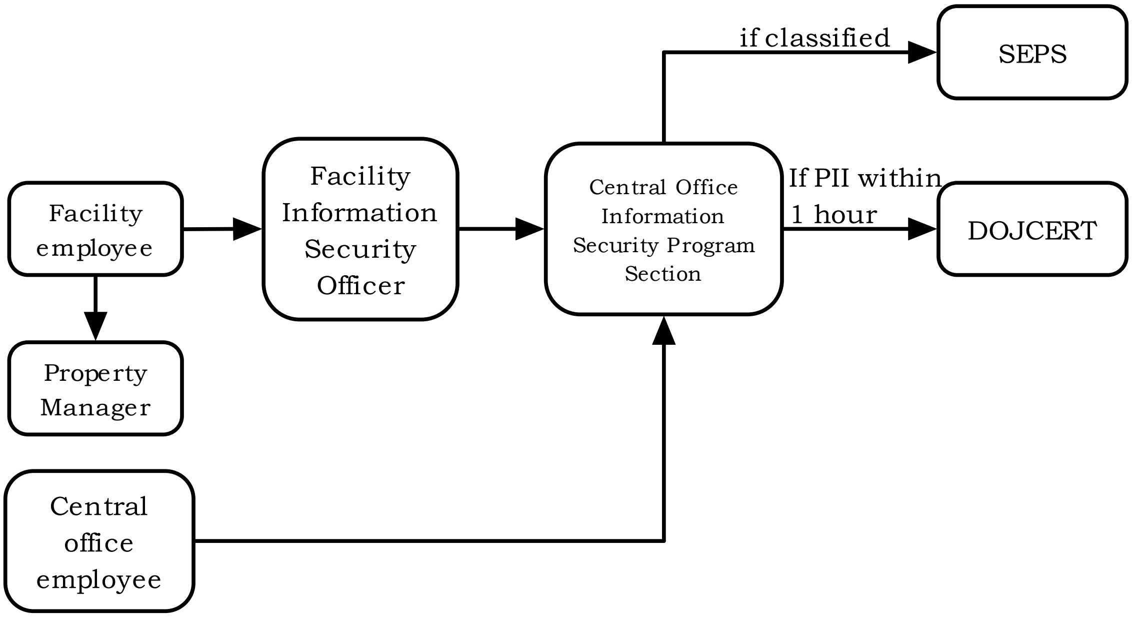
2. BOP Incident Response Plan, which is consistent with the DOJCERT Incident Response Plan template and was updated to reflect DOJCERT's most recent November 2006 changes that incorporate reporting procedures for loss of PII.

The BOP's Information Security Policy instructs employees in all institutions, Regional Offices, and Community Corrections Centers to report computer security violations to the facility Information Security Officer as soon as possible. Employees are also required to report loss or theft to the Property Officer. The Information Security Officer is required to then notify the BOP's Central Office Information Security Programs Section. Employees at the BOP's Central Office are to notify the Information Security Programs Section directly rather than reporting through an Information Security Officer. If PII is involved, notification is required to be made to the Information Security Programs Section within 1 hour. The Information Security Programs Section should then notify DOJCERT within the timeframes specified in the BOP Incident Response Plan. The BOP's Incident Response Plan, revised in December 2006, reflects timeframes in which to notify DOJCERT depending on the category and severity of the incident.

The Information Security policy further states that relevant supervisors, managers, executive staff, and Regional Administrators should also be notified. The Information Security Officer therefore notifies the appropriate chain of command (facility executive staff and regional personnel), including the Information Security Programs Section at the Central Office. The Information Security Officer, upon verification of the security threat, is encouraged to notify other facilities or localities that may be similarly susceptible to a particular security violation. Chart 8 shows the BOP's reporting procedures for loss of sensitive information.

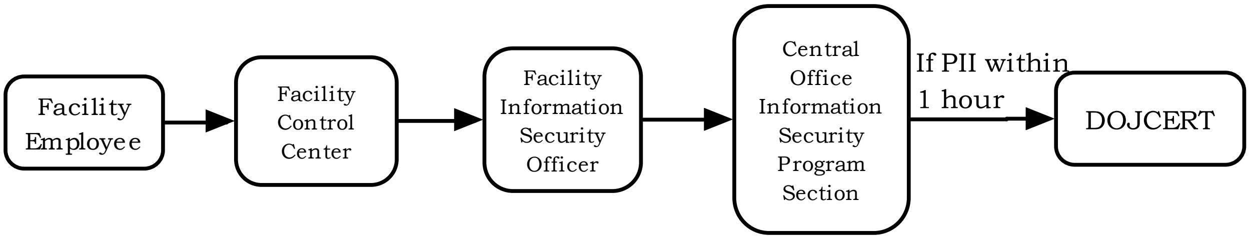
Although the BOP's processing of classified information is very limited, a BOP official told us that if a computer security incident occurred involving classified information, they would follow the Department's SPOM and report the incident to the Department's Security Officer.

Chart 8: Flowchart of the BOP's Reporting Procedures for Loss of Sensitive Information



If a computer security incident occurs after hours at one of the BOP facilities, the employee should call the facility's Control Center, which is manned 24 hours a day. The Control Center then calls the Information Security Officer at home. The Information Security Officer should then follow the procedures described above. Chart 9 shows the BOP's procedures for after-hours reporting of loss of sensitive information.

Chart 9: Flowchart of BOP Facility Staff After-Hours Reporting Procedures for Loss of Sensitive Information


Facility Employee
Facility Control Center
Facility Information Security Officer
Central Office Information Security Program Section
If PII within 1 hour
DOJCERT

In the event of a theft of a laptop or BlackBerry device at the Central Office, the BOP is required to report the theft to Federal

Protective Service.[76] If a theft or other computer security crime occurs at a facility, the FBI should be notified because it has jurisdiction to investigate crimes occurring in federal prisons. Employees should contact the local police department in the event of a laptop or BlackBerry device theft off-site. Any of these law enforcement officials should enter the theft into the NCIC database. Additionally, if employee negligence is suspected, the incident should be referred to the BOP Office of Internal Affairs and the OIG for possible investigation.

Indications of Compliance with Reporting Procedures

BOP officials told us that they believed their employees were following the correct reporting procedures. While we did not validate this statement, our analysis of the Archer Database showed that the BOP was not always reporting computer security incidents, including PII, within the required timeframes specified in both the DOJCERT and BOP Incident Response Plans. Between December 2005 and November 2006, BOP reported only 37 percent of its computer security incidents to DOJCERT within the required timeframes. Further, only 14 percent of the PII incidents that occurred on or after July 12, 2006 were reported to DOJCERT within the required 1-hour timeframe.[77] Table 8 shows the BOP's reporting in each category.[78]

[76] The Department of Homeland Security's Federal Protective Service provides law enforcement and security services to federal government agencies who occupy federally owned and leased facilities nationwide.

[77] We did not analyze incidents for timeliness that occurred before OMB established the 1-hour timeframe in July 2006.

[78] Our calculations are based on Categories 1 through 5 and Category 7. We did not include incidents found in Categories 0 and 6 because they had no associated time criteria, nor did we include incidents for which the Archer Database contained no information to indicate when DOJCERT received the report that an incident had occurred.

Table 8: The BOP's Timeliness in Reporting Incidents to DOJCERT

Category	Reporting timeframe*	Incidents reported	Reported within timeframe	Reported after timeframe	Could not compute timeliness**
Category 0 (Exercise/Test)	None	4	N/A	N/A	4
Category 1 (Unauthorized Access)	1 hour	19	2	17	0
Category 2 (Denial of Service)	2 hours	2	0	2	0
Category 3 (Malicious Code)	1 day	144	34	98	12
Category 4 (Improper Usage)	1 week	34	17	17	0
Category 5 (Scans/Probes)	1 month	19	15	2	2
Category 6 (Investigation)	None	14	N/A	N/A	14
Category 7 (Spam)	1 month	16	12	1	3
Total		**252**	**80**	**137**	**35**
PII incidents occurring on or after 7/12/06***	1 hour	7	1	6	0

* For purposes of this table, reporting timeframes for Categories 0-7 refer to the timeframes defined in the Incident Response Plan. Reporting timeframe for PII incidents refers to the timeframe defined in OMB Memorandum M-06-19.

** Some records did not include information to indicate when DOJCERT received the reports. Category 0 and 6 incidents, for which there are no reporting timeframes, are also included in this category.

*** PII incidents were reported in varying incident categories.

Source: Archer Database

Ensuring All Incidents Are Reported

The BOP relies on several methods to ensure that all computer security incidents are reported: training, program reviews, and policies. The BOP administers annual computer security training to all staff to educate them on their reporting responsibilities. The BOP also said that it conducts program reviews to ensure reporting procedures are being followed in the program area of information security. A BOP program or operational review is required annually for each facility's Information Security program.[79] Program reviews are a system of internal reviews conducted by BOP staff who are subject matter experts in the program

[79] BOP, Information Security, P1237.13, March 31, 2006.

under review. These reviews ensure that programs are in compliance with applicable laws, regulations, and policies.

The BOP *Property Management Manual* also establishes employee responsibilities for the management and control of government-owned personal property such as laptops and BlackBerry devices.[80] Designated Property Officers are responsible for maintaining up-to-date computer inventories of all accountable government-owned personal property and reconciling that property list against required quarterly and annual physical inventories conducted in all BOP facilities. According to policy, if a lost or stolen electronic device was not reported, both the Property Officer and the employee are held liable for the property. The *Property Management Manual* states that it is the employee's duty to report loss, theft, or damage to accountable property and requires that reports be made to the Property Officer upon discovery (but no later than the next working day).

This policy also establishes the Board of Survey, a BOP committee that investigates the circumstances surrounding lost, stolen, missing, damaged, or destroyed government-owned personal property. The board makes recommendations consistent with the findings disclosed by its review and, if applicable, may refer cases to the Office of Internal Affairs, which can refer cases to the OIG or the Criminal Division for prosecution.

The BOP also has Rules of Behavior concerning the use and security of computer systems.[81] The rules notify employees that sensitive information is to be protected from disclosure to unauthorized individuals and that they will be sanctioned for unauthorized use, disclosure, destruction, or misuse of information resources. The rules also state that security violations and system vulnerabilities are to be immediately reported to the appropriate authorities.

Notification to Affected Parties

The BOP has not developed policies concerning notification to affected parties in the event of a loss of PII.

[80] BOP, *Property Management Manual*, P4400.05, May 26, 2004.

[81] The BOP's Rules of Behavior are contained in a BOP policy entitled Information Resources Protection, P1237.12, February 20, 2001.

Determining the Type of Data Lost

The BOP said that it determines the type of data lost by having the Information Security Officer interview the employee involved in the computer security incident. The BOP Information Security policy states that the Information Security Officer may perform a preliminary review to confirm that a computer security violation has occurred.

In addition, the BOP also said that it has instituted controls to restrict employee access to sensitive data. The head of a facility is required to give written approval to employees before they remove laptops (or other devices) to process sensitive data off-site, such as while at home or traveling on official business. According to policy, a written request from the employee must include the type of device (such as a laptop), a description of the contents, and the purpose of the data removal.[82] However, in practice, according to interviews, it is up to the head of each facility whether the contents are actually described in the request.

[82] BOP, Information Security, P1237.13, March 31, 2006, p. 14.

APPENDIX III: CRIMINAL DIVISION REPORTING PROCEDURES

Introduction

Between December 2005 and November 2006, the Criminal Division reported 24 security incidents to DOJCERT, including 5 incidents involving potential PII loss and 10 incidents potentially involving classified information.[83] The Criminal Division considers a reportable data loss to be information on lost electronic media (CD-ROM, disk, or tape), and electronic devices (BlackBerry device or laptop), or information intentionally or inadvertently released from its network. Several Criminal Division policies refer to the term "Sensitive But Unclassified" without defining it. In general, the Criminal Division considers all of its information to be sensitive and relies on the Department's definition of the term "sensitive information."[84] The Criminal Division uses the definition of PII found in OMB Memorandum M-06-19 and therefore considers PII to be "any information about an individual" that is "maintained by an agency . . . which can be used to distinguish or trace an individual's identity." To define classified information, the Criminal Division relies on the National Security Information definition in Executive Order 12958, as Amended, Classified National Security Information, dated March 25, 2003.

Reporting Procedures

The Criminal Division uses a single Incident Response Plan for addressing the reporting of sensitive, PII, and classified computer security incidents. The division has updated its plan to conform to the DOJCERT template of November 2006 and identifies the seven categories of incidents that should be reported to DOJCERT within specified timeframes. Reporting procedures are as follows for sensitive, PII, and classified information.

[83] As of January 31, 2007, the loss of PII has been confirmed in one of these five incidents. The remaining four incidents involve potential losses of PII.

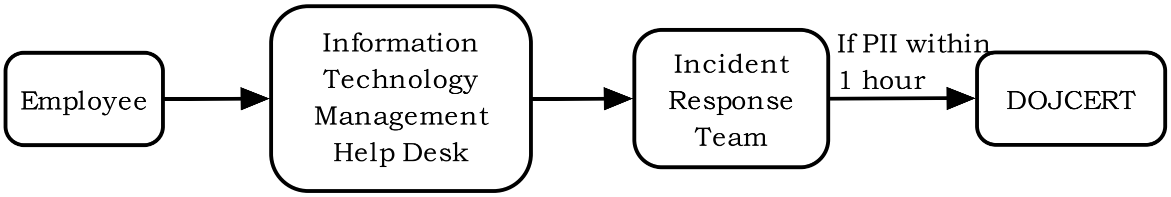
[84] The Department's *Security Program Operating Manual* defines sensitive information as "any information, the loss, misuse, modification of, or unauthorized access to, could affect the national interest, law enforcement activities, the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but that has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy."

Sensitive and PII Reporting Procedures

Criminal Division employees are required to report a potential sensitive computer security incident "immediately" to the division's Information Technology Management Help Desk when it is determined that an incident has occurred. The Help Desk should then log the incident information into its ticketing database and notify the Incident Response Team consisting of the Incident Response Team Coordinator, the Information Systems Security Manager, and the Network Security Officer. The Incident Response Team members should then determine the information that needs to be collected for the initial informal incident report and provide this report either verbally or in written form to DOJCERT. Once more information becomes known, the Network Security Officer should send a formal Preliminary Incident Report to DOJCERT, usually within 24 hours.

If a computer security incident involving a potential loss of PII occurs during normal work hours, Criminal Division employees should follow the same process as when reporting a sensitive data loss, except that the Incident Response Team makes an informal verbal or written report to DOJCERT within 1 hour. The Network Security Officer is directed to follow up with a formal Preliminary Incident Report within 24 hours. Chart 10 shows the Criminal Division's reporting procedures for loss of sensitive information, including PII.

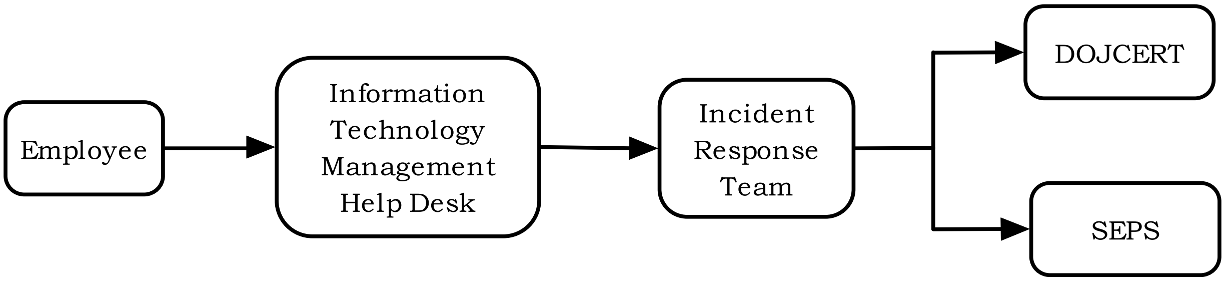
Chart 10: Flowchart of Criminal Division's Reporting Procedures for Loss of Sensitive Information, Including PII



Classified Information Incidents

The Criminal Division is required to follow the procedures contained in the Department's *Security Program Operating Manual* for reporting classified incidents. In addition to the notifications to the Help Desk and DOJCERT described above, the Incident Response Team also is required to notify the Department's Security and Emergency Planning Staff (SEPS). Chart 11 shows the Criminal Division's reporting procedures for loss of classified information.

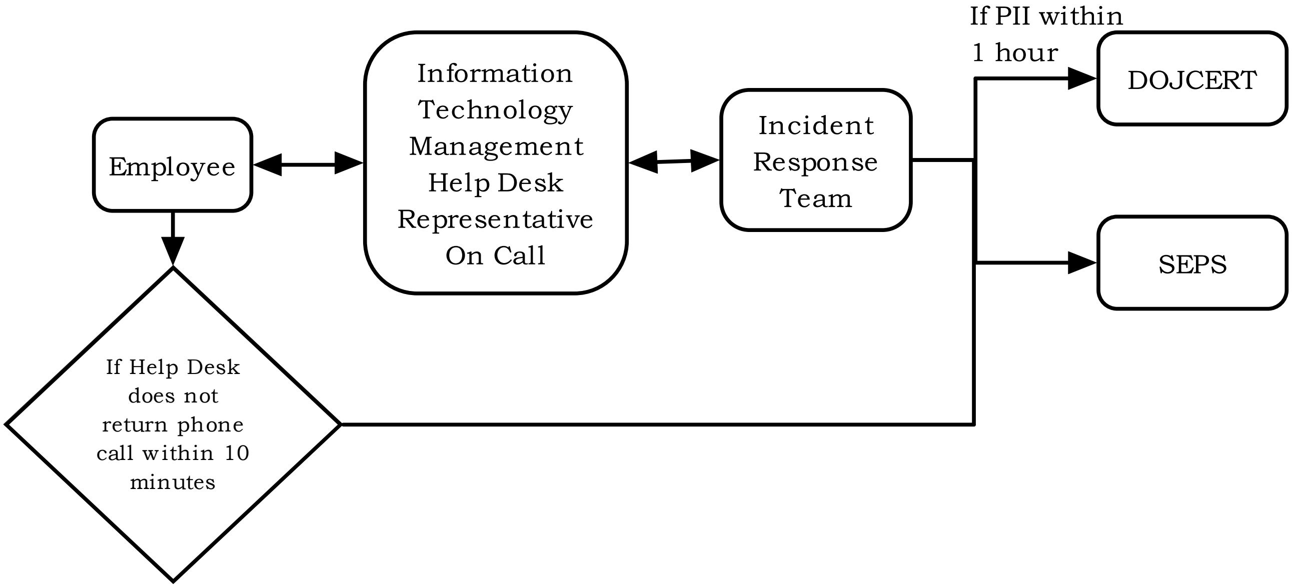
Chart 11: Flowchart of the Criminal Division's Reporting Procedures for Loss of Classified Information



After-Hours Reporting Procedures

If a sensitive, PII, or classified incident occurs after normal work hours, the employee involved should call the Help Desk representative who is on-call after hours. The Help Desk should notify the Incident Response Team who then notifies DOJCERT and SEPS (if the incident involves classified information). The Help Desk or a member of the Incident Response Team is required to follow up with the employee to ensure that all of the facts about the incident are collected and the incident has been properly reported to DOJCERT via a Preliminary Incident Report. According to the Criminal Division's Incident Response Plan, if the employee does not receive a return phone call from the Help Desk representative within 10 minutes, the employee then should report the computer security incident directly to DOJCERT. If the incident involves classified information the employee should also notify SEPS. Chart 12 shows the Criminal Division's procedures for after-hours reporting of sensitive, PII, or classified computer security incidents.

Chart 12: Flowchart of the Criminal Division's After-Hours Procedures for Reporting Loss of Sensitive, PII, or Classified Information


Employee
Information Technology Management Help Desk Representative On Call
Incident Response Team
If PII within 1 hour
DOJCERT
SEPS
If Help Desk does not return phone call within 10 minutes

Indications of Compliance with Reporting Procedures

Criminal Division officials told us that they believed their employees were following the correct reporting procedures. While we did not validate this statement, our analysis of the Archer Database showed that the Criminal Division was not always reporting computer security incidents, including PII, within the required timeframes specified in both the DOJCERT and Criminal Division Incident Response Plans. Between December 2005 and November 2006, the Criminal Division reported 60 percent of its computer security incidents to DOJCERT within the required timeframes. However, none of the PII incidents that occurred on or after July 12, 2006 were reported within the required 1-hour timeframe.[85] Table 9 shows the Criminal Division's reporting in each category.[86]

[85] We did not analyze incidents for timeliness that occurred before OMB established the 1-hour timeframe in July 2006.

[86] Our calculations are based on Categories 1 through 5 and Category 7. We did not include incidents found in Categories 0 and 6 because they had no associated time criteria, nor did we include incidents for which the Archer Database contained no information to indicate when DOJCERT received the report that an incident had occurred.

Table 9: The Criminal Division's Timeliness in Reporting Incidents to DOJCERT					
Category	**Reporting timeframe***	**Incidents reported**	**Reported within timeframe**	**Reported after timeframe**	**Could not compute timeliness****
Category 0 (Exercise/Test)	None	0	N/A	N/A	N/A
Category 1 (Unauthorized Access)	1 hour	1	0	1	0
Category 2 (Denial of Service)	2 hours	0	N/A	N/A	N/A
Category 3 (Malicious Code)	1 day	8	2	4	2
Category 4 (Improper Usage)	1 week	8	6	2	0
Category 5 (Scans/Probes)	1 month	3	3	0	0
Category 6 (Investigation)	None	2	N/A	N/A	2
Category 7 (Spam)	1 month	2	1	1	0
Total		**24**	**12**	**8**	**4**
PII incidents occurring on or after 7/12/06***	1 hour	4	0	4	0

* For purposes of this table, reporting timeframes for Categories 0-7 refer to the timeframes defined in the Incident Response Plan. Reporting timeframe for PII incidents refers to the timeframe defined in OMB Memorandum M-06-19.

** Some records did not include information to indicate when DOJCERT received the reports. Category 0 and 6 incidents, for which there are no reporting timeframes, are also included in this category.

*** PII incidents were reported in varying incident categories.

Source: Archer Database

Ensuring All Incidents Are Reported

While the Criminal Division uses several methods to ensure that employees report incidents of data loss, it primarily relies on training and the Rules of Behavior. The annual Computer Security Awareness Training that is required of all Department employees includes a segment on protecting, preventing, and reporting PII loss or compromise. The Rules of Behavior require users to immediately report any evidence of tampering with a computer. A member of the Information Technology Management staff also told us that employees must read and sign the Rules of Behavior when they are hired and must review them on a yearly basis.

Additionally, Criminal Division officials told us that when each computer in the Criminal Division starts up it displays a security statement screen and gives examples of security incidents, which serves as a daily reminder to all employees of their responsibility to report incidents. The Criminal Division also said it uses a physical property inventory to identify missing electronic devices.

Notification to Affected Parties

The Criminal Division has not developed policies concerning notification to affected parties in the event of a loss of PII.

Determining the Type of Data Lost

The Criminal Division said that it generally interviews its employees and obtains a statement of facts as the primary means for determining what information was on a disk, laptop, or other electronic device that was lost, stolen, or compromised. According to one Information Technology Management official, employees "know what was on the device."

In addition to interviewing the employee, the Criminal Division said that it has controls in place to monitor what is on electronic devices. For example, the Criminal Division said that a record is made of all e-mail that passes through a server to and from a BlackBerry device, so that if a BlackBerry device were lost, a method to identify the e-mail information on the device is available. Also, the Criminal Division said that a "kill signal" can be sent to a BlackBerry device once its loss is known, rendering it useless and the information on it inaccessible.

APPENDIX IV: DEA REPORTING PROCEDURES

Introduction

Between December 2005 and November 2006, the DEA reported 43 security incidents to DOJCERT, including 6 incidents involving potential PII loss and 2 incidents potentially involving classified information.[87] The DEA considers a reportable computer security incident to be any loss of electronic devices that might contain sensitive information such as laptops, flash drives, removable hard drives, tapes, or CD-ROMs.

The DEA considers all of its information to be sensitive, categorizing it as either Sensitive But Unclassified, Law Enforcement Sensitive, For Official Use Only, or DEA Sensitive. The DEA defines Sensitive But Unclassified information as information subject to controls outside the formal system for classifying National Security Information and considers Sensitive But Unclassified information as exempt from release to the public under the Freedom of Information Act. Law Enforcement Sensitive information is a subset of Sensitive But Unclassified. The term For Official Use Only is used to identify information or material that, although unclassified, may not be appropriate for public release. DEA Sensitive information is information, media, or material that must be afforded a higher level of protection than Sensitive But Unclassified information. According to the DEA, this includes information and materials:

- That are investigative in nature;
- To which access is restricted by law;
- That are critical to the operation and mission of the DEA;
- That, if disclosed, would violate a privileged relationship; and

[87] According to the DEA, its internal documents and DOJCERT and SEPS records showed that only one incident involving classified information occurred during the review period. Further, of the six incidents cited by the OIG as involving potential PII loss, only two were actual or suspected losses of PII. However, the numbers that DEA cites are not reflected in the DOJCERT's Archer Database data, which we used for each of the nine components reviewed in our analysis. See the Purpose, Scope, and Methodology section of this report for a more detailed discussion of our method for deriving our numbers.

- That relate to any DEA employee's identification or location if revealing such information would negatively affect an operation or mission.[88]

The DEA has adopted the definition of PII that was published in OMB Memorandum M-06-19 on July 12, 2006. The DEA broadcast this definition to all DEA employees in an e-mail from the DEA's CIO and the DEA's Chief Inspector on October 12, 2006.[89] The broadcast e-mail defined PII as:

> any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, criminal or employment history, and any information which can be used to distinguish or can be traced to 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.

The DEA uses the definition of classified information contained in Executive Order 12958, as Amended, Classified National Security Information, dated March 25, 2003.

Reporting Procedures

The DEA outlined its reporting procedures for DEA Sensitive, Law Enforcement Sensitive, For Official Use Only, and PII in its October 12, 2006, e-mail to all DEA employees. These procedures apply to information on electronic devices such as flash drives, laptops, hard disks, tapes, and CD-ROMs as well as to printed information. These procedures are also contained in the DEA's eight Incident Response Plans, all of which have been updated to reflect the changes DOJCERT made to the November 2006 Incident Response Plan template.[90]

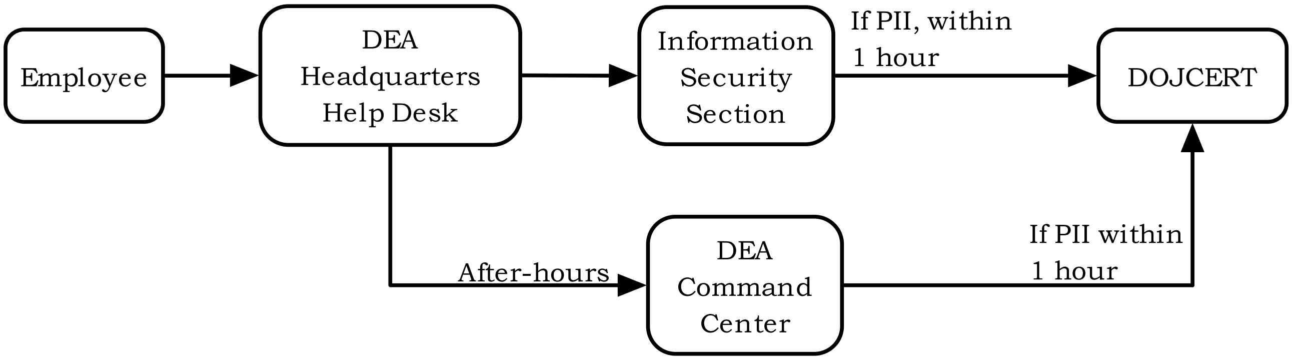
[88] DEA Policy, Control and Decontrol of DEA Sensitive Information, REF 99-001, June 2, 1999.

[89] DEA Headquarters broadcast e-mail to all DEA personnel, Personally Identifiable Information (PII) Media Loss Reporting Requirements and Procedures, October 12, 2006.

[90] One Incident Response Plan covers several IT systems that are part of the same IT network. The remaining seven Incident Response Plans cover seven stand-alone IT systems. The procedure defined in the Incident Response Plans is the same in each of the eight plans.

The DEA's written procedures for reporting computer security incidents involving Sensitive But Unclassified information, both electronic and paper, instruct all employees to report computer security incidents immediately to the DEA Headquarters Help Desk after determining that an incident has occurred.[91] The Help Desk is required to then notify the Information Security Section. The Information Security Section should then notify DOJCERT of incidents via the Archer Database. If the incident involves PII, the Information Security Section is required to report the incident to DOJCERT within 1 hour. The DEA Command Center is staffed 24 hours a day, 7 days a week. If an incident is reported outside normal business hours, the Help Desk should report it to the DEA Command Center instead of the Information Security Section, and the DEA Command Center should ensure that DOJCERT is notified within the required timeframe. Chart 13 shows the DEA's procedures for reporting sensitive information loss, including PII.

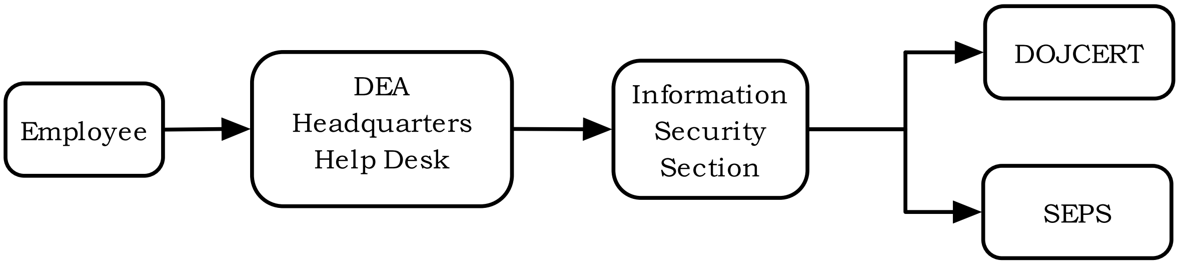
Chart 13: Flowchart of DEA's Reporting Procedures for Loss of Sensitive Information, Including PII



Incidents involving classified information must be reported following the same procedures as outlined in the Incident Response Plans. The DEA Incident Response Plans require the DEA to notify the Department's Security and Emergency Planning Staff (SEPS) of all incidents involving classified information and DOJCERT. Chart 14 shows the DEA's procedures for reporting of classified information loss.

[91] However, in interviews with DEA officials we were told that the employee reporting the loss is to notify his or her direct supervisor and the supervisor is responsible for ensuring that the Help Desk is notified. Further, if a device has been reported lost or stolen, the supervisor is required to initiate a search for that device while the incident is being reported.

Chart 14: Flowchart of the DEA's Reporting Procedures for Loss of Classified Information



In the event a device has been stolen, the employee reporting the theft is required to contact the local police and obtain a police report, after reporting the incident to the Help Desk. The DEA should then notify other law enforcement agencies about the loss of DEA information if there is a suspicion that such loss could have an impact on those agencies. The DEA should also notify the FBI about losses resulting from the theft of government equipment of significant value.

Indications of Compliance with Reporting Procedures

DEA officials told us that they believed their employees were following the correct reporting procedures. While we did not validate this statement, our analysis of the Archer Database showed that the DEA was not always reporting computer security incidents, including PII, within the required timeframes specified in both the DOJCERT and DEA Incident Response Plans. Between December 2005 and November 2006, the DEA reported 75 percent of its computer security incidents to DOJCERT within the required timeframes. However, only 17 percent of the PII incidents that occurred on or after July 12, 2006, were reported within the required 1-hour timeframe.[92] Table 10 shows the DEA's reporting in each category.[93]

[92] We did not analyze incidents for timeliness that occurred before OMB established the 1-hour timeframe in July 2006.

[93] Our calculations are based on Categories 1 through 5 and Category 7. We did not include incidents found in Categories 0 and 6 because they had no associated time criteria, nor did we include incidents for which the Archer Database contained no information to indicate when DOJCERT received the report that an incident had occurred.

Table 10: The DEA's Timeliness in Reporting Incidents to DOJCERT					
Category	**Reporting timeframe***	**Incidents reported**	**Reported within timeframe**	**Reported after timeframe**	**Could not compute timeliness****
Category 0 (Exercise/Test)	None	3	N/A	N/A	3
Category 1 (Unauthorized Access)	1 hour	7	2	5	0
Category 2 (Denial of Service)	2 hours	0	N/A	N/A	N/A
Category 3 (Malicious Code)	1 day	8	4	2	2
Category 4 (Improper Usage)	1 week	2	1	1	0
Category 5 (Scans/Probes)	1 month	3	3	0	0
Category 6 (Investigation)	None	6	N/A	N/A	6
Category 7 (Spam)	1 month	14	14	0	0
Total		**43**	**24**	**8**	**11**
PII incidents occurring on or after 7/12/06***	1 hour	6	1	5	0

* For purposes of this table, reporting timeframes for Categories 0-7 refer to the timeframes defined in the Incident Response Plan. Reporting timeframe for PII incidents refers to the timeframe defined in OMB Memorandum M-06-19.

** Some records did not include information to indicate when DOJCERT received the reports. Category 0 and 6 incidents, for which there are no reporting timeframes, are also included in this category.

*** PII incidents were reported in varying incident categories.

Source: Archer Database

Ensuring All Incidents Are Reported

The DEA told us that it has taken a number of steps to ensure employees are aware of procedures for reporting computer security incidents. The DEA said that most plans or manuals are available to all DEA employees on a common server called Webster. One of the documents required for employees to review is the DEA's Interim Information Technology Rules of Behavior that instructs employees to immediately report all security incidents or suspected incidents to the

DEA Help Desk.[94] Employees are required to review these Rules of Behavior when they are hired and annually thereafter.

To further reinforce these rules, the Deputy Chief Inspector in the Office of Security Programs sent a memorandum to the DEA Deputy Assistant Administrator in the Office of Information Systems advising of an amendment to the Rules of Behavior. The memorandum stated that "[a]ll personnel shall immediately report any loss of sensitive information or PII to the HELPDESK." This requirement was further reinforced in the most recent annual Computer Security Awareness Training, which explained the requirement to protect PII information and report any loss of PII information.

Notification to Affected Parties

The DEA has not developed policies concerning notification to affected parties in the event of a loss of PII.

Determining the Type of Data Lost

The DEA said that it primarily relies on employee interviews for identifying what was on lost equipment such as laptops and BlackBerry devices. However, under certain circumstances DEA officials told us they can use computer forensics to determine what file was last accessed by an employee on a server. Doing so could suggest what information might have been downloaded to a lost laptop.

[94] The Incident Response Plans are also on the Webster server and available to DEA employees should they need to find out how to report sensitive or PII computer security incidents.

APPENDIX V: EOUSA AND USAO REPORTING PROCEDURES

EOUSA provides the 93 United States Attorneys' Offices (USAO) with administrative management oversight, operational support, policy development, and coordination with other components of the Department and other federal agencies. As part of this support, EOUSA provides policy and procedural assistance for implementation of all security programs for the USAOs and ensures compliance with all applicable statutes and Executive and Department Orders.[95] The USAOs are required to report all computer security incidents to EOUSA, and EOUSA acts as the point of contact for notifying DOJCERT and the Security and Emergency Planning Staff (SEPS). For the purposes of this appendix, we use the acronym EOUSA to refer to EOUSA and the USAOs combined.

Introduction

Between December 2005 and November 2006, EOUSA reported 463 security incidents to DOJCERT, including 142 incidents involving potential PII loss and 4 incidents potentially involving classified information.[96] According to an EOUSA official, EOUSA considers a reportable computer security incident to be any physical loss of media, systems information, or a breach that results in the loss of data, a laptop, a cell phone, or a wireless device such as a BlackBerry device.

EOUSA considers its information to be either Limited Official Use or classified; however, most of its information is designated as Limited Official Use. EOUSA relies on the 1982 DOJ Order 2620.7, which defines Limited Official Use as "unclassified information of a sensitive, proprietary or personally private nature which must be protected against release to unauthorized individuals . . . ."[97] EOUSA uses the term Limited Official Use as synonymous with the terms "sensitive" and "Sensitive But Unclassified." Limited Official Use information includes but is not limited to "grand jury information, informant and witness information, investigative material, federal tax and tax return

[95] *United States Attorneys' Manual*, Security Programs Management, § 3-15.010, August 2004.

[96] As of January 31, 2007, the loss of PII has been confirmed in three incidents. The remaining 139 incidents involve potential losses of PII.

[97] DOJ Order 2620.7, Control and Protection of Limited Official Use Information, September 1, 1982, p. 1.

information, Privacy Act information, and information that can cause risk to individuals or could be sold for profit."[98]

In 2003, EOUSA further defined Limited Official Use information to include the term Law Enforcement Sensitive, which developed through "common usage and agency culture to identify a specific type of Limited Official Use or Sensitive information," for example, intelligence information unrelated to terrorism.[99]

EOUSA considers PII as a category of sensitive information. While EOUSA does not have its own specific definition of PII, it has adopted the definition of PII published in OMB Memorandum M-06-15 to Department and agency heads that defines PII to be "any information about an individual" that is "maintained by an agency . . . which can be used to distinguish or trace an individual's identity."[100]

To define classified information, EOUSA relies on the National Security Information definition in Executive Order 12958, as Amended, Classified National Security Information, dated March 25, 2003.[101]

Reporting Procedures

Limited Official Use and PII Reporting Procedures

EOUSA has several written policies that contain instructions for reporting computer security incidents. General reporting procedures for Sensitive But Unclassified (Limited Official Use) and PII are contained in EOUSA's Incident Response Plan, dated December 13, 2006. This plan is consistent with the DOJCERT Incident Response Plan and has been updated to reflect DOJCERT's November 2006 revision. Additionally, written policies and procedures for USAOs are contained in the *United*

[98] *United States Attorneys' Manual*, Security Programs Management, § 3-15.120, August 2004.

[99] EOUSA Memorandum sent via e-mail, Limited Official Use (Sensitive) Information Designation, January 14, 2003.

[100] OMB Memorandum M-06-15 for Heads of Departments and Agencies, Safeguarding Personally Identifiable Information, Clay Johnson III, Acting Director, May 22, 2006.

[101] Executive Order 12958, Classified National Security Information, April 17, 1995.

States Attorneys' Manual and the United States Attorneys' Procedures.[102] However, because no one policy defines the entire reporting chain of command from the field to EOUSA to DOJCERT, our description of reporting procedures is taken from a combination of policies, draft policies, and practice as stated by EOUSA officials during interviews.

According to interviews, the procedures for reporting computer security incidents involving Limited Official Use (Sensitive But Unclassified) information and PII are as follows: In the USAO districts, an employee is required to immediately notify the District Office Security Manager that a computer security incident had occurred.[103] If the District Office Security Manager is unreachable, then the employee should report the incident to a Regional Security Specialist for that District's region. The District Office Security Manager or Regional Security Specialist should then e-mail an incident report to the Assistant Director, Information Systems Security Staff, who should report the incident to DOJCERT. If a data loss incident occurs at EOUSA, the employee or the employee's immediate supervisor should notify the Assistant Director, Information Systems Security Staff. If PII is involved, the Assistant Director should notify DOJCERT within 1 hour.

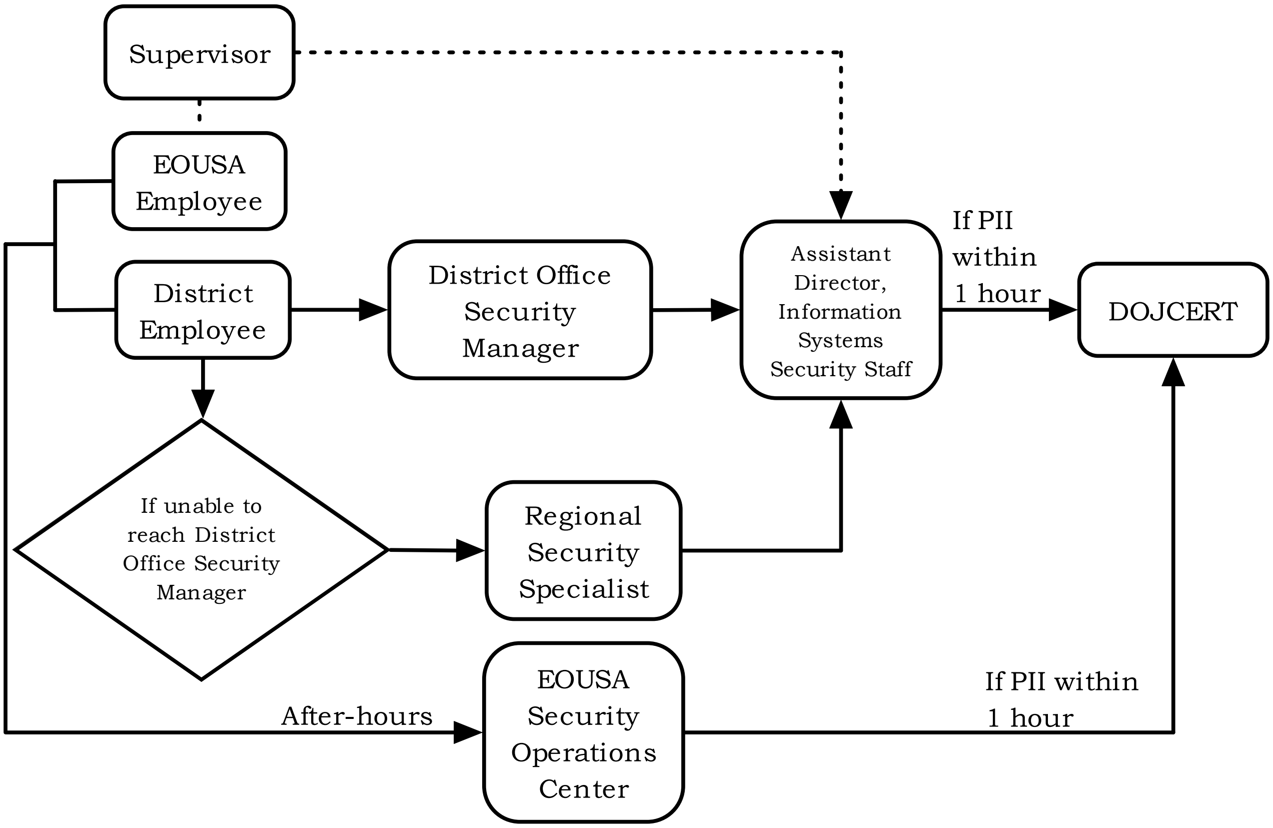
For incidents that do not involve PII, DOJCERT should be notified within the timeframes specified in the EOUSA Incident Response Plan. For both EOUSA and the USAOs, when an incident occurs after hours, the employee should contact the EOUSA Security Operations Center.[104] Depending on the severity of the incident, the Assistant Director may also report the incident immediately to the Department's CIO. An example of a severe incident could be a virus outbreak that hinders the operating capability of EOUSA or a particular USAO office. Chart 15 shows EOUSA's procedures for reporting the loss of sensitive information, including PII.

[102] The manual contains general policies and procedures relevant to the work of the USAOs and to their relations with the legal divisions, investigative agencies, and other components within the Department. *United States Attorneys' Manual,* § 1-1.100, September 1997.

[103] An employee may also notify his or her immediate supervisor, who then reports the incident to the District Office Security Manager. Each USAO has a District Office Security Manager.

[104] In April 2007, an EOUSA official stated that EOUSA had developed a draft policy on after-hours reporting procedures, but that this policy had not yet been issued.

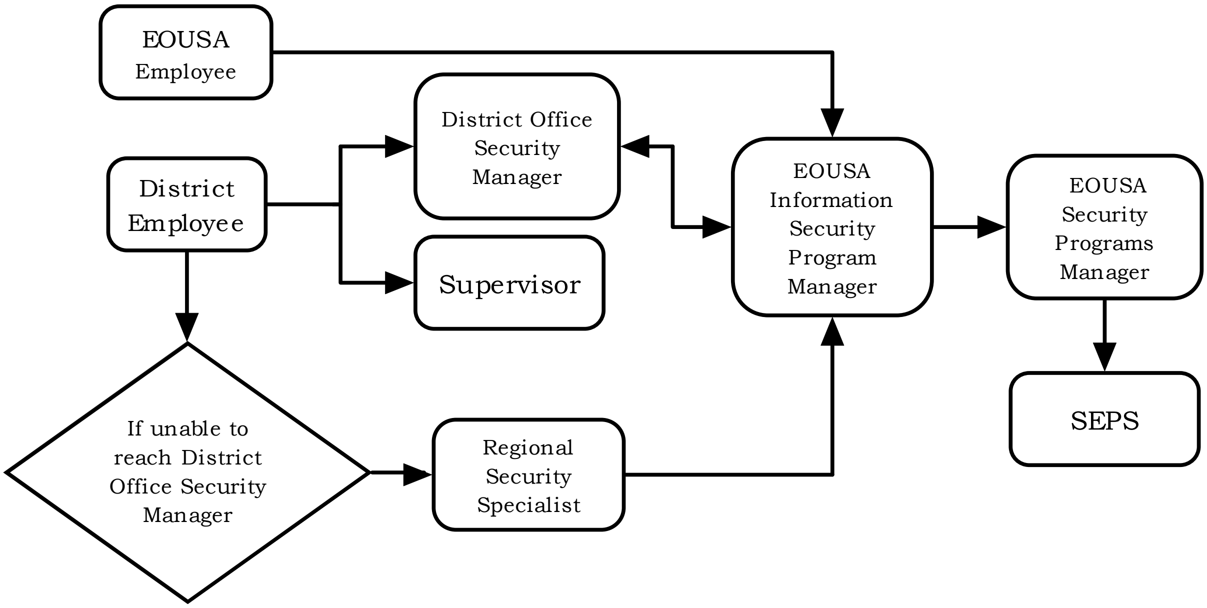
Chart 15: Flowchart of EOUSA's Reporting Procedures for Loss of Sensitive Information, Including PII


Supervisor
EOUSA Employee
District Employee
District Office Security Manager
Assistant Director, Information Systems Security Staff
If PII within 1 hour
DOJCERT
If unable to reach District Office Security Manager
Regional Security Specialist
After-hours
EOUSA Security Operations Center
If PII within 1 hour

Classified Reporting Procedures

For reporting classified information loss, the EOUSA's Incident Response Plan states that reporting procedures shall be done in accordance with the Department's *Security Program Operations Manual.* According to EOUSA officials we interviewed, when an USAO employee discovers a classified incident, the employee is required to report the incident to his or her supervisor and then to the District Office Security Manager. The District Office Security Manager in turn should report it to EOUSA's Information Security Program Manager. The Information Security Program Manager then should obtain the facts of the incident from the District Office Security Manager or EOUSA employee and forward the incident report to his supervisor, the Security Programs Manager, who then forwards the report to SEPS. If a data loss occurred at EOUSA Headquarters, the employee should report directly to EOUSA's Information Security Program Manager. Chart 16 shows EOUSA's procedures for reporting classified information loss.

Chart 16: Flowchart of EOUSA's Reporting Procedures for Loss of Classified Information


EOUSA Employee
District Employee
District Office Security Manager
Supervisor
If unable to reach District Office Security Manager
Regional Security Specialist
EOUSA Information Security Program Manager
EOUSA Security Programs Manager
SEPS

Indications of Compliance with Reporting Procedures

We were told in interviews by EOUSA officials that they believed their employees were following the reporting procedures. While we did not validate this statement, our analysis of the Archer Database showed that EOUSA was not always reporting computer security incidents, including PII, within the required timeframes specified in both the DOJCERT and EOUSA Incident Response Plan. Between December 2005 and November 2006, EOUSA reported 80 percent of its computer security incidents to DOJCERT within the required timeframes. However, only 16 percent of the PII incidents that occurred on or after July 12, 2006 were reported within the required 1-hour timeframe.[105] Table 11 shows EOUSA's reporting in each category.[106]

[105] We did not analyze incidents for timeliness that occurred before OMB established the 1-hour timeframe in July 2006.

[106] Our calculations are based on Categories 1 through 5 and Category 7. We did not include incidents found in Categories 0 and 6 because they had no associated time criteria, nor did we include incidents for which the Archer Database contained no information to indicate when DOJCERT received the report that an incident had occurred.

Table 11: EOUSA's Timeliness in Reporting Incidents to DOJCERT					
Category	**Reporting timeframe***	**Incidents reported**	**Reported within timeframe**	**Reported after timeframe**	**Could not compute timeliness****
Category 0 (Exercise/Test)	None	6	N/A	N/A	6
Category 1 (Unauthorized Access)	1 hour	25	0	18	7
Category 2 (Denial of Service)	2 hours	0	N/A	N/A	N/A
Category 3 (Malicious Code)	1 day	143	66	14	63
Category 4 (Improper Usage)	1 week	94	63	2	29
Category 5 (Scans/Probes)	1 month	15	7	0	8
Category 6 (Investigation)	None	179	N/A	N/A	179
Category 7 (Spam)	1 month	1	0	0	1
Total		**463**	**136**	**34**	**293**
PII incidents occurring on or after 7/12/06***	1 hour	134	19	101	14

* For purposes of this table, reporting timeframes for Categories 0-7 refer to the timeframes defined in the Incident Response Plan. Reporting timeframe for PII incidents refers to the timeframe defined in OMB Memorandum M-06-19.

** Some records did not include information to indicate when DOJCERT received the reports. Category 0 and 6 incidents, for which there are no reporting timeframes, are also included in this category.

*** PII incidents were reported in varying incident categories.

Source: Archer Database

An EOUSA official we interviewed stated that employees are expected to report computer security incidents immediately. This official also stated that while EOUSA tries to adhere as much as possible to the 1-hour requirement for reporting incidents to DOJCERT when PII is involved, the 1-hour requirement was impractical because of the number of steps that have to be taken prior to the notification to DOJCERT. The official stated that it takes time for an employee to recall when the incident occurred, what information was on the device, or where the device might have been lost. It also takes time for a District Office Security Manager to gather the necessary information and facts surrounding the loss of data or a device before reporting the incident to the EOUSA Information Systems Security Officer.

Ensuring All Incidents Are Reported

EOUSA said that it primarily relies on training and employee integrity for ensuring that employees report all computer security incidents. EOUSA relies on the Department's annual Computer Security Awareness Training and the USAOs' Justice Consolidated Office Network II Rules of Behavior to inform employees of their responsibility to report such incidents.[107] The Rules of Behavior, which employees are required to read and sign when they begin employment, state that loss of a Department laptop or personal digital assistant shall be reported immediately to the District Office Security Manager and EOUSA Assistant Director, Information Systems Security Staff. The rules also require any actual or suspected security violations, incidents, vandalism, or vulnerabilities be reported to the District Office Security Manager and Systems Manager. Any violation of these rules may be cause for disciplinary action. EOUSA also said that it relies on the employee to report any incidents in which electronic devices or sensitive data is lost or stolen.

Notification to Affected Parties

EOUSA has not developed policies concerning notification to affected parties in the event of a loss of PII.

Determining the Type of Data Lost

EOUSA said that it primarily relies on interviews with employees, supervisors, and systems managers for identifying the information contained on lost or stolen laptops and personal digital assistants.

[107] United States Attorneys' Offices Justice Consolidated Office Network II, Rules of Behavior, April 13, 2004.

APPENDIX VI: FBI REPORTING PROCEDURES

Introduction

Between December 2005 and November 2006, the FBI reported 206 computer security incidents to DOJCERT, including 43 incidents involving potential PII loss and 35 incidents potentially involving classified information.[108] The FBI considers all of its information to be sensitive – either Sensitive But Unclassified or classified – and requires its employees to report incidents that result in the loss of classified or Sensitive But Unclassified information as well as the loss or theft of all portable electronic devices or removable storage media, such as laptops, BlackBerry devices, hard drives, CDs, and flash drives. Sensitive But Unclassified is defined in the FBI's *Security Policy Manual* as "information that requires protection due to the risk or magnitude of loss or harm that could result from inadvertent or deliberate disclosure, modification and/or destruction of the information." The FBI *Security Policy Manual* states that records requiring protection under the Privacy Act are a subset of Sensitive But Unclassified information.[109] The FBI does not currently have a separate definition for PII. The FBI uses the definition of classified information contained in Executive Order 12958, as Amended, Classified National Security Information, dated March 25, 2003.

Reporting Procedures

Within the FBI, computer security incidents are reported to two separate offices, but only one of those offices is required to report incidents to DOJCERT. One office's procedure for reporting computer security is defined in an FBI policy issued by the Security Division called the *Security Policy Manual.*[110] The other office's procedure is defined in the FBI's four Incident Response Plans.[111] Both offices should be notified

[108] As of January 31, 2007, the loss of PII has been confirmed in 1 of the 43 incidents. The remaining 42 incidents involve potential losses of PII.

[109] 5 U.S.C. § 552a.

[110] FBI *Security Policy Manual*, POL05-0001-SecD, revised April 3, 2006.

[111] The procedure defined in the Incident Response Plans is the same in each of the four plans.

as soon as an employee informs both his or her supervisor and the Chief Security Officer that a computer security incident has occurred.[112]

Procedures Defined in FBI Security Policy

The *Security Policy Manual*, issued by the Security Division, requires FBI employees to report potential computer security incidents to the Security Compliance Unit via a web-based form.[113] The form is available to all employees on the FBI intranet and may be completed by either the employee who discovered the incident, the employee's supervisor, the Division's Chief Security Officer, or any other individual with direct knowledge of an incident. Employees must identify the type of security incident that occurred, choosing from five categories provided, and answer additional questions that are specific to that category of security.[114] For example, incidents identified as "Information Technology Security" require employees to describe the circumstances surrounding the loss of electronic information or the loss of a portable electronic device. Employees must also provide the serial number and classification level of a lost portable electronic device.

The Security Compliance Unit said that it tracks all reported security incidents in an Access database and provide monthly reports to the Section Chief of the Security Operations Section in FBI Headquarters. The Security Compliance Unit also said that it generates quarterly reports of security incidents, by type of incident, to keep the Career Services Management Unit (which develops FBI training) and the Policy Unit (which develops FBI policy) aware of areas of security that may need more attention.

[112] Each FBI field division and each division within FBI Headquarters has a Chief Security Officer.

[113] Subsequent to FBI Special Agent Robert Hanssen's arrest for espionage, the Commission for the Review of FBI Security Programs was formed. As a result of a recommendation from the Commission, the FBI established the Security Compliance Unit at FBI Headquarters in 2003 to coordinate and oversee all information and physical security compliance activity and violations. FBI employees, contractors, and task force members are required to report all types of security incidents, including data loss incidents and losses of PII, to the Security Compliance Unit.

[114] The five categories are Information Technology Security, Technical Security, Personnel Security, Physical Security, and Control/Loss of Documents.

Procedures Defined in Incident Response Plans

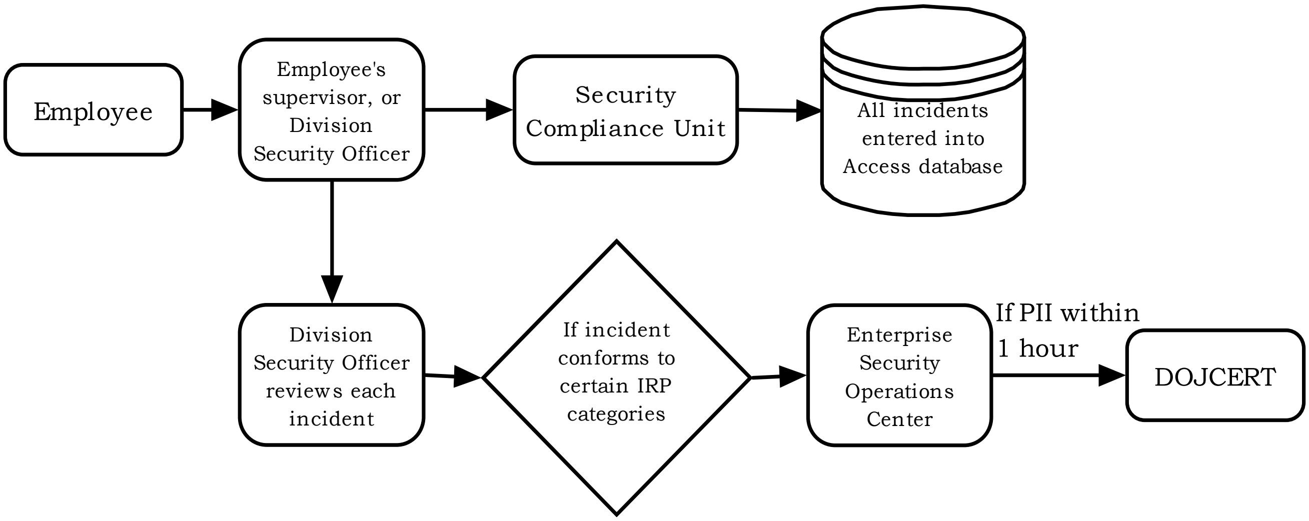
The FBI maintains four Incident Response Plans that conform to the DOJCERT template to cover the following four types of systems: the system that has been classified Top Secret, the systems that have been classified Secret, the unclassified systems, and the systems operated by the Criminal Justice Information Services Division. All four plans have been updated to reflect the changes DOJCERT made to the November 2006 template and identify the seven categories of incidents that should be reported to DOJCERT within specified timeframes.[115]

The Division's Chief Security Officer is required to review each reported incident and determine if the incident fits into one of the categories identified in the Incident Response Plans.[116] If it does, the division's Chief Security Officer is required to contact the FBI's Enterprise Security Operations Center. After-hours reporting procedures are the same as normal business hours procedures because the Enterprise Security Operations Center is staffed 24 hours a day, 7 days a week. The center should implement the procedures in the Incident Response Plans and notify DOJCERT via the Archer Database. Incidents reported to the center should also be tracked in the FBI's Security Information Management System. Quarterly reports generated from this system are provided to the FBI's CIO. Chart 17 shows the FBI's procedures for reporting all computer security incidents, including those involving sensitive, PII, and classified information.

[115] Incidents in these seven categories can be caused by either internal sources (threats that originate inside the FBI) or external sources (threats that originate outside the FBI). Threats caused by internal sources are reported to both the Security Compliance Unit and the Enterprise Security Operations Center. Threats caused by external sources are reported only to the Enterprise Security Operations Center.

[116] Some FBI divisions have an Information Systems Security Officer who makes this initial determination. If this is the case, the Information Systems Security Officer notifies both the division's Chief Security Officer and DOJCERT. However, for budgetary reasons, not all divisions have an Information Systems Security Officer.

Chart 17: Flowchart of the FBI's Procedures for Reporting All Computer Security Incidents, Including Sensitive, PII, and Classified (Includes After-Hours Reporting Procedures)


Employee
Employee's supervisor, or Division Security Officer
Security Compliance Unit
All incidents entered into Access database
Division Security Officer reviews each incident
If incident conforms to certain IRP categories
Enterprise Security Operations Center
If PII within 1 hour
DOJCERT

FBI officials told us that the Security Compliance Unit and the Enterprise Security Operations Center are supposed to routinely discuss information security incidents with each other and the actions each section will take to respond to those incidents. However, according one official, these discussions do not always occur within the timeframes established in the Incident Response Plans. The Security Compliance Unit is not involved in the communications between the center and DOJCERT.

Indications of Compliance with Reporting Procedures

Lost Electronic Device Reporting Procedures

The FBI was not in full compliance with DOJCERT's reporting requirements for lost electronic devices. The requirements in the *Security Policy Manual* (issued by the FBI Security Division) for reporting losses of electronic devices are not consistent with the requirements in the FBI's Incident Response Plans (issued by the Enterprise Security Operations Center). In reviewing the information the FBI provided to us and the information we analyzed from the Archer Database, we noticed a discrepancy between the number of lost electronic devices that had been reported to the Security Compliance Unit and the number of lost electronic devices that had been reported to the Enterprise Security Operations Center (who is required to report all computer security incidents to DOJCERT).

For the period from December 2005 through November 2006, FBI employees reported 35 lost or stolen laptops to the Security Compliance Unit, but reported only 7 lost or stolen laptops to the Enterprise Security Operations Center, and therefore to DOJCERT.[117] We asked the FBI to explain the discrepancy, and officials stated that, prior to the release of OMB Memorandum M-06-16 in June 2006, the FBI did not realize that all losses of electronic devices were considered reportable incidents as defined by DOJCERT's Incident Response Plan template. Previously, the FBI relied on Chapter 22 of its *Security Policy Manual*, dated April 2006, which addresses the reporting procedures for loss of portable electronic devices. This policy requires FBI employees to report security violations involving portable electronic devices to the Security Compliance Unit and does not mention the Enterprise Security Operations Center.

Additionally, we noted that although the FBI stated it did not realize that all losses of electronic devices were considered reportable incidents as defined by DOJCERT's Incident Response Plan template, the FBI's January 2006 Incident Response Plan for unclassified systems required FBI IT security staff to report thefts of computer assets to the Enterprise Security Operations Center.

The OIG recently released an audit that found deficiencies in the FBI's procedures for reporting the loss of laptops, including failure to report those incidents in a timely manner.[118] In response to a recommendation in that audit, the FBI agreed to revise its policies and to develop additional guidance for reporting incidents to DOJCERT.

Classified Reporting Procedures

The FBI was not following the chain-of-command reporting procedures for reporting of classified computer security incidents. Between December 2005 and November 2006, FBI employees reported

[117] One of the laptops that was reported to the Security Compliance Unit was a classified laptop.

FBI officials told us that 35 lost or stolen laptops were reported to the Security Compliance Unit. We reviewed data from DOJCERT's Archer Database and determined that seven lost or stolen laptops had been reported to the Enterprise Security Operations Center and to DOJCERT. We did not verify the information from either of these sources.

[118] OIG, *The Federal Bureau of Investigation's Control Over Weapons and Laptop Computers Follow-Up Audit,* Audit Report 07-18, February 2007.

107 classified computer security incidents to the Security Compliance Unit. Our analysis of data from the Archer Database showed that the Enterprise Security Operations Center reported 35 classified computer security incidents to DOJCERT.[119] However, the Department's Security and Emergency Planning Staff (SEPS) did not receive any reports of classified computer security incidents from the FBI during that same time period.

The Department's Definition of a Reportable Classified Incident. The Department's *Security Program Operating Manual* (SPOM) requires all components to report "any incident involving a possible loss, compromise, or suspected compromise of classified information" immediately to the Department Security Officer, who is the Director of SEPS.[120] The SPOM identifies nine categories of reportable classified incidents meeting this definition including:

- Any incident involving a possible loss, compromise, or suspected compromise of classified information;
- Efforts by any individual . . . to obtain illegal or unauthorized access to classified information or to compromise an employee's authorized access;
- Any emergency situation that renders a facility incapable of safeguarding classified material;
- A delay of more than 48 hours in the delivery of classified material by a commercial carrier;
- Any event involving . . . IT systems, equipment or media which may result in disclosure of classified information to unauthorized individuals, or that results in unauthorized modification or destruction of system data, loss of computer system processing capability, or loss or theft of computer system media;
- Any evidence of tampering with a shipment, delivery, or mailing containing classified information;
- Any shipment or transmission of classified information that is received by other than an approved method prescribed by this manual;
- Any incidents that indicate an employee knowingly or willfully violated security policies established for the protection of classified or sensitive information; and

[119] We did not conduct a case file review to determine whether the 35 classified computer security incidents reported to the Enterprise Security Operations Center were among the 107 classified computer security incidents reported to the Security Compliance Unit.

[120] *Security Program Operating Manual*, § 1-300. The *Security Program Operating Manual* is written by SEPS and applies to the entire Department.

- Any information that raises doubt as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security.[121]

Classified Incidents Reported to the Security Compliance Unit. The Security Compliance Unit utilizes the FBI's *Security Policy Manual* to define a classified incident as "a failure to safeguard FBI classified and sensitive material according to FBI policies, Executive Order 12958, and Director of National Intelligence Directives."[122] The FBI's *Security Policy Manual* identifies eight categories of reportable classified incidents meeting this definition including:

- Any loss, compromise, or suspected compromise of classified information;
- Efforts by a person to obtain unauthorized access to classified information, or to compromise an employee with access;
- Any emergency situation that renders a facility incapable of safeguarding classified materials;
- A delay of more than 48 hours in the delivery of classified materials by a commercial carrier;
- Any event involving computer or telecommunications equipment or media which may result in disclosure of classified information to unauthorized persons, or that results in unauthorized modification or destruction of system data, loss of computer system processing capability, or loss or theft of computer system media;
- Any evidence of tampering with a shipment, delivery or mailing containing classified information;
- Any shipment or transmission of classified information that is received by other than an approved method; and
- Any incidents that indicate an employee knowingly or willfully violated security policies.[123]

We noted that the *Security Policy Manual's* definition of reportable classified incidents was nearly identical to the SPOM's definition of reportable classified incidents. Even though the SPOM requires components to report classified incidents to SEPS, the FBI stated that it was unaware of any FBI policy requiring it to notify SEPS. However, the FBI also directed us to another passage from its *Security Policy Manual*, which requires the FBI to notify the Director of National Intelligence of:

[121] *Security Program Operating Manual*, § 1-302.

[122] FBI *Security Policy Manual*, § 17.3.

[123] FBI *Security Policy Manual*, § 17.4.

> a significant security violation or a compromise of intelligence information that is either extensive in scope, indicates pervasive breach of security procedures, or is otherwise likely to have a serious effect on national security interests. This notification is to be made through the AD [Assistant Director], Security Division, to the Department of Justice Security Officer.[124]

The OIG recognizes that not all classified incidents will meet the "significant" standard that requires reporting to the Director of National Intelligence, as outlined in § 17.10 of the *Security Policy Manual*. However, because the FBI's general definition of a classified security incident, found in §§ 17.3 and 17.4 of the *Security Policy Manual*, matches the Department's definition, the FBI should be reporting all of these incidents to SEPS as required by the SPOM. As noted above, the Security Compliance Unit's role is to track all reported security incidents in a database, and provide monthly reports to the Section Chief of the Security Operations Section in FBI Headquarters. FBI policy does not require the Security Compliance Unit to report any computer security incident to any entity outside the FBI, including SEPS.

Classified Incidents Reported to the Enterprise Security Operations Center. The Enterprise Security Operations Center defined a classified incident as "an event where an individual gains logical or physical access without permission or a 'need to know' to a network, system, application, data, or other resource that contains National Security Information," and stated that the loss of an electronic device or media (such as a laptop, CD, or flash drive) or the placement of information "on a lower level medium than it is intended for" also constituted a classified incident.[125] As noted above, the Enterprise Security Operations Center is required to report computer security incidents to DOJCERT.

The FBI stated that the Enterprise Security Operations Center had mistakenly believed that DOJCERT was a subcomponent of SEPS. As a result, the FBI believed that reporting classified computer security

[124] See FBI *Security Policy Manual*, § 17.10. The FBI also told us that computer security incidents meeting this standard are defined as "loss or compromise of information storage media or equipment containing intelligence information of such quantity or sensitivity as to potentially jeopardize intelligence activities, sources or methods."

[125] The placement of information "on a lower level medium than it is intended for" is commonly referred to as a classified spill.

incidents to DOJCERT constituted reporting them to SEPS.[126] Between December 2005 and November 2006, the Enterprise Security Operations Center reported 35 classified computer security incidents to DOJCERT.[127]

While this practice does not exactly match the requirements set out in the SPOM, DOJCERT provides SEPS the opportunity to review all data loss incidents, including classified incidents, via e-mail notification. We are more concerned that at least 72 classified computer security incidents which were reported to the Security Compliance Unit by FBI employees between December 2005 and November 2006 were not reported to either DOJCERT or SEPS.[128]

Timeliness of Reporting.

Our analysis of the Archer Database showed that the FBI was not always reporting computer security incidents, including PII, within the required timeframes specified in both the DOJCERT and FBI Incident Response Plans. Between December 2005 and November 2006, the FBI reported only 45 percent of its computer security incidents to DOJCERT within the required timeframes. Further, none of the PII incidents that occurred on or after July 12, 2006 for which we could determine timeliness were reported within the required 1-hour timeframe.[129] Table 12 shows the FBI's reporting in each category.[130]

[126] As noted earlier, both DOJCERT and SEPS are part of the Justice Management Division. However, the offices are in separate chains of command. DOJCERT reports to the Department's CIO, who reports to the Assistant Attorney General for Administration. SEPS reports to the Deputy Assistant Attorney General for Human Resources/Administration, who also reports to the Assistant Attorney General for Administration. See JMD's organizational chart at www.usdoj.gov/jmd/orginfo/chart.htm

[127] The FBI stated in a February 2007 e-mail sent to the OIG that it now understands that SEPS and DOJCERT have different, but complimentary, missions and that the FBI should make overlapping reports of classified computer security incidents.

[128] We did not conduct a case file review to determine whether or not the 35 classified, IT-related security incidents reported to the Enterprise Security Operations Center were among the 107 classified, IT-related security incidents reported to the Security Compliance Unit.

[129] We did not analyze incidents for timeliness that occurred before OMB established the 1-hour timeframe in July 2006. Additionally, we could not analyze one incident that occurred after OMB established the 1-hour timeframe because there was no information in the Archer Database to indicate when DOJCERT received the report.

[130] Our calculations are based on Categories 1 through 5 and Category 7. We did not include incidents found in Categories 0 and 6 because they had no associated

(Cont'd.)

Table 12: The FBI's Timeliness in Reporting Incidents to DOJCERT

Category	Reporting timeframe*	Incidents reported	Reported within timeframe	Reported after timeframe	Could not compute timeliness**
Category 0 (Exercise/Test)	None	0	N/A	N/A	N/A
Category 1 (Unauthorized Access)	1 hour	15	2	13	0
Category 2 (Denial of Service)	2 hours	1	0	1	0
Category 3 (Malicious Code)	1 day	42	14	28	0
Category 4 (Improper Usage)	1 week	113	50	57	6
Category 5 (Scans/Probes)	1 month	21	18	3	0
Category 6 (Investigation)	None	13	N/A	N/A	13
Category 7 (Spam)	1 month	1	1	0	0
Total		**206**	**85**	**102**	**19**
PII incidents occurring on or after 7/12/06***	1 hour	26	0	25	1

* For purposes of this table, reporting timeframes for Categories 0-7 refer to the timeframes defined in the Incident Response Plan. Reporting timeframe for PII incidents refers to the timeframe defined in OMB Memorandum M-06-19.

** Some records did not include information to indicate when DOJCERT received the reports. Category 0 and 6 incidents, for which there are no reporting timeframes, are also included in this category.

*** PII incidents were reported in varying incident categories.

Source: Archer Database

The FBI is aware of the Department requirement to report all incidents involving PII loss within 1 hour and has incorporated that requirement into its four Incident Response Plans. However, one FBI official stated that the Department's guidance concerning PII "is clear as mud." The FBI has raised concerns about this timeframe with the Department's CIO and asked for clarification. Specifically, the FBI told us they asked the Department to more clearly define the action that should trigger the 1-hour timeframe. An Assistant Special Agent in Charge assigned to a large field division told us that the 1-hour

time criteria, nor did we include incidents for which the Archer Database contained no information to indicate when DOJCERT received the report that an incident had occurred.

timeframe is “very difficult, if not impossible, to meet on a practical basis” and further noted that his particular office is so large that “I couldn’t find someone within 1 hour if my life depended on it.” The FBI would like the Department to work with the components to develop criteria and thresholds for reporting incidents involving PII loss so that the components can better determine which incidents may be serious enough to warrant reporting.

While the FBI is aware of the Department requirement to report all potential losses of PII within 1 hour, not all FBI employees had been notified of the requirement as of the end of 2006. For example, one Assistant Special Agent in Charge stated that, at the end of 2006, knowledge of the requirement was inconsistent in his field division, with employees in the sections that handle large amounts of PII, such as the White Collar Crime Section, aware of the requirement and employees in other sections, such as the Counterterrorism Section, not likely to be aware. The Assistant Special Agent in Charge also expressed concern that employees might not realize the urgency of the situation when an incident involving PII loss occurs.

Ensuring All Incidents Are Reported

The FBI said that it conducts training to ensure that employees are aware of the requirement to report computer security incidents, including those involving PII loss. The FBI said that it administers the Department’s annual Computer Security Awareness Training to remind employees of the requirement to report computer security incidents. The requirement is also included in the Information Technology Rules of Behavior, which employees are required to sign. The Computer Security Awareness Training has been updated to include the requirement that losses of PII be reported within 1 hour. FBI employees were scheduled to take this annual training between January 2007 and April 2007. An official in the FBI’s Security Division noted that the division always sees a spike in reporting incidents immediately after employees complete their annual training. All FBI staff with relevant responsibilities interviewed agreed that, beyond conducting training to ensure that all employees are aware of the requirement to report security incidents, there is no way to guarantee that every incident is properly reported. Employees are also reminded that failure to report a security incident is, in itself, a security incident. However, one Assistant Special Agent in Charge noted that employees may delay reporting a lost or stolen device because they fear the possibility of punishment. In addition to training, FBI staff identified the annual property inventory as a method of verifying whether all lost or stolen electronic devices were reported.

Notification to Affected Parties

The FBI has not developed policies concerning notification to affected parties in the event of a loss of PII.

Determining the Type of Data Lost

The FBI said that it determines the type of data lost through written questions and employee interviews. The Security Compliance Unit is supposed to review the initial report of the incident and send a series of questions to the Chief Security Officer. The Security Compliance Unit said that it began specifically asking about the loss of PII after that type of loss became an important issue for the government, although no written FBI policy requires the unit to obtain that information. Using the questions provided by the Security Compliance Unit, the Chief Security Officer is supposed to interview the employee reporting the loss to determine what type of information the device may have contained. Based on the employee's response, the Chief Security Officer should facilitate communication between the employee, the employee's supervisor, and the appropriate division in FBI Headquarters to conduct a damage assessment of the incident.[131] In addition, the Enterprise Security Operations Center can review server log-in records and e-mail servers to determine when an employee last logged in and which files the employee accessed during that time.

[131] For example, if an employee states that a stolen laptop contained information related to a violent crime case still under investigation, the Chief Security Officer will help the employee and the supervisor arrange a meeting with someone from the Violent Crimes Unit at FBI Headquarters to determine if the theft of the laptop could have an impact on the ongoing investigation.

APPENDIX VII: JMD REPORTING PROCEDURES

DOJCERT is located within the Office of the CIO, which is a subcomponent of the Justice Management Division (JMD). For purposes of incident reporting, the subcomponents of JMD are treated as separate components. Each subcomponent reports its own incidents and maintains its own Incident Response Plan. The following section is based on interviews with and documents obtained from two subcomponents of JMD: Personnel and the Security and Emergency Planning Staff (SEPS).

Introduction

Between December 2005 and November 2006, JMD reported 402 computer security incidents to DOJCERT, including 18 incidents involving PII and 5 incidents potentially involving classified information.[132] Both Personnel and SEPS consider any loss of PII, including the loss of any electronic device or removable media containing PII, to be reportable computer security incidents.

JMD officials we interviewed stated that their subcomponents of JMD follow the Department's definition of sensitive information and consider all of their information to be sensitive. In the *Security Program Operating Manual*, the Department defines sensitive information as:

> any information, the loss, misuse, modification of, or unauthorized access to, could affect the national interest, law enforcement activities, the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but that has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.[133]

[132] Personnel reported 13 incidents to DOJCERT between December 2005 and November 2006, including 1 incident involving potential loss of PII, and no incidents involving classified information. SEPS reported four incidents to DOJCERT between December 2005 and November 2006, none of which involved either PII or classified information. All of the incidents reported by SEPS were instances of SEPS employees receiving spam e-mails.

[133] The *Security Program Operating Manual* is written by SEPS and applies to the entire Department.

The Personnel division considers PII to be synonymous with information that is protected by the Privacy Act.[134] However, SEPS uses OMB's definition of PII. Personnel does not handle classified information, while SEPS does. SEPS uses the definition of classified information contained in Executive Order 12958, as Amended, Classified National Security Information, dated March 25, 2003.

Reporting Procedures

JMD employees are required to contact the individual who handles security issues in their subcomponent to report any computer security incidents. In Personnel, the Avue User Rules of Behavior require all employees to report all computer security incidents to the Avue Administrator, who is required to notify the Personnel Information Systems Security Officer.[135] Personnel's Information Systems Security Officer should notify DOJCERT, via the Archer Database, and also should ensure that the Personnel staff follows the procedures outlined in Personnel's Incident Response Plan. Personnel staff may also notify their supervisors of computer security incidents, although no policy specifically requires them to do so. Personnel has not developed any written procedures for reporting computer security incidents after hours.

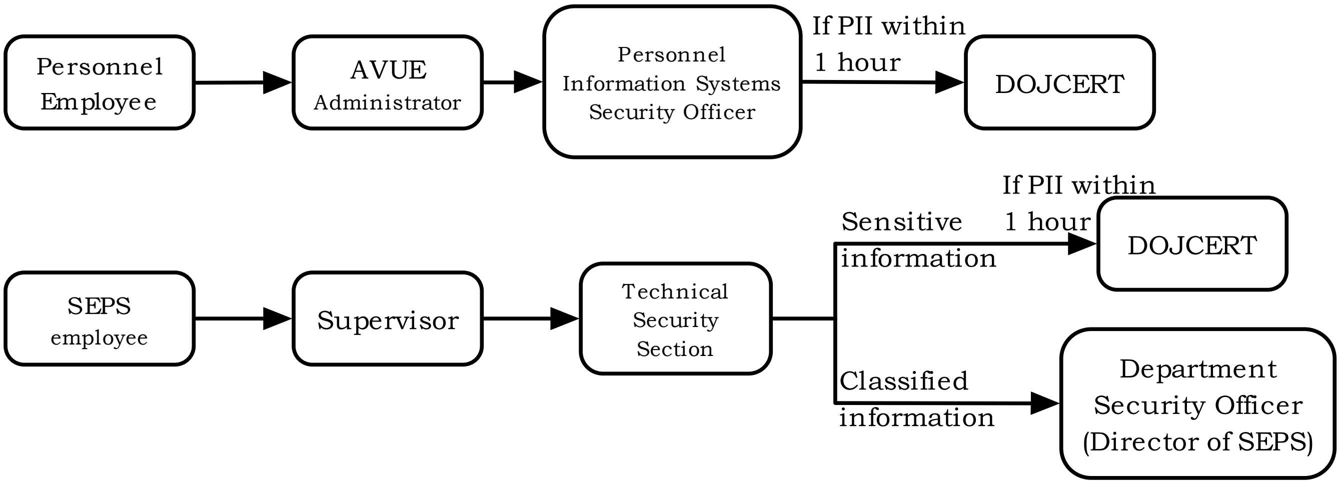
SEPS employees are not provided with written procedures instructing them on how to report computer security incidents through the SEPS reporting chain of command. We were told in interviews that, in practice, employees report computer security incidents to their supervisors, who forward the report to the staff of the Technical Security Section.[136] The Technical Security Section notifies DOJCERT, via the Archer Database, and also ensures that SEPS follows the procedures outlined in its Incident Response Plan. For classified incidents, SEPS's employees said that in practice they report a suspected loss to their supervisor. The supervisor then reports the incident to the Technical Security Section who forwards the report to the Department Security Officer (Director of SEPS). Chart 18 shows Personnel's and SEPS's procedures for reporting all computer security incidents, including those involving sensitive, PII, and classified information.

[134] 5 U.S.C. § 552a.

[135] Avue is the system the Department uses for online job applications.

[136] SEPS is divided into 10 different sections, each of which handles a different aspect of security. The Technical Security Section handles the security of technology used to store and transmit classified information.

Chart 18: Flowchart of Personnel's and SEPS's Procedures for Reporting All Computer Security Incidents, Including Sensitive, PII, and Classified Information



Personnel and SEPS have updated the Incident Response Plans they maintain to reflect the changes DOJCERT made to the November 2006 Incident Response Plan template. The Incident Response Plans identify the seven categories of incidents that should be reported to DOJCERT within specified timeframes.

Both Personnel and SEPS use the Archer Database to track incidents that have been reported to DOJCERT.

Indications of Compliance with Reporting Procedures

For the two JMD subcomponents we reviewed, subcomponent officials told us that they believed employees were following the correct reporting procedures. While we did not validate this statement, we did analyze data from the Archer Database to determine if all of the subcomponents of JMD were reporting incidents to DOJCERT in a timely manner.[137] Our analysis showed that JMD was not always reporting computer security incidents, including PII, within the required timeframes specified in both the DOJCERT and JMD Incident Response Plans. Between December 2005 and November 2006, JMD reported 84 percent of its computer security incidents to DOJCERT within the required timeframes. However, only 14 percent of PII incidents that occurred on or after July 12, 2006 were reported within the required

[137] The Archer Database included incidents that were reported by 25 different subcomponents of JMD.

1-hour timeframe.[138] Personnel reported one PII incident after July 12, 2006, but did not report it in the required 1-hour timeframe. SEPS did not report any PII incidents. Table 13 shows JMD's overall reporting in each category.[139]

Table 13: JMD's Timeliness in Reporting Incidents to DOJCERT

Category	**Reporting timeframe***	**Incidents reported**	**Reported within timeframe**	**Reported after timeframe**	**Could not compute timeliness****
Category 0 (Exercise/Test)	None	11	N/A	N/A	11
Category 1 (Unauthorized Access)	1 hour	17	3	13	1
Category 2 (Denial of Service)	2 hours	1	1	0	0
Category 3 (Malicious Code)	1 day	42	16	15	11
Category 4 (Improper Usage)	1 week	6	2	4	0
Category 5 (Scans/Probes)	1 month	99	84	10	5
Category 6 (Investigation)	None	21	N/A	N/A	21
Category 7 (Spam)	1 month	205	165	8	32
Total		**402**	**271**	**50**	**81**
PII incidents occurring on or after 7/12/06***	1 hour	16	2	12	2

* For purposes of this table, reporting timeframes for Categories 0-7 refer to the timeframes defined in the Incident Response Plan. Reporting timeframe for PII incidents refers to the timeframe defined in OMB Memorandum M-06-19.

** Some records did not include information to indicate when DOJCERT received the reports. Category 0 and 6 incidents, for which there are no reporting timeframes, are also included in this category.

*** PII incidents were reported in varying incident categories.

Source: Archer Database

[138] We did not analyze incidents for timeliness that occurred before OMB established the 1-hour timeframe in July 2006. We could not analyze two incidents that occurred after OMB established the 1-hour timeframe because there was no information in the Archer Database to indicate when DOJCERT received the reports.

[139] Our calculations are based on Categories 1 through 5 and Category 7. We did not include incidents found in Categories 0 and 6 because they had no associated time criteria, nor did we include incidents for which the Archer Database contained no information to indicate when DOJCERT received the report that an incident had occurred.

Ensuring All Incidents Are Reported

JMD said that it relies primarily on training as its method for ensuring employees are aware of the requirement to report computer security incidents, including those involving PII loss. An official on the Personnel staff described the Department's annual Computer Security Awareness Training as "the number one vehicle" for emphasizing the importance of security to Personnel staff and for reinforcing the reporting requirements that are outlined in the Avue User Rules of Behavior. JMD said that personnel staff members receive verbal briefings on the procedures for reporting computer security incidents when they are given the equipment necessary to use Justice Secure Remote Access and also receive a wallet card summarizing those reporting procedures. Lost laptops or BlackBerry devices can be identified through Personnel's annual inventory process. Personnel's Property Officer told us that the annual property inventory has not uncovered any problems with lost or stolen electronic devices.

A Security Specialist in the SEPS Technical Security Section noted that there is no failsafe method for ensuring that all incidents are reported but stated that explaining the reporting procedures and encouraging employees to make reports was an important method for ensuring that incidents are properly reported. SEPS's Executive Officer told us that the annual property inventory has not uncovered any lost or stolen electronic devices.

Notification to Affected Parties

JMD has not developed policies concerning notification to affected parties in the event of a loss of PII.

Determining the Type of Data Lost

JMD said that it generally determines the type of data loss through employee interviews. In Personnel, the Information Systems Security Officer is required to interview both the employee reporting the loss and the employee's supervisor to determine how the employee used the device and what data it may have contained. In addition, in August 2006 Personnel modified its Avue User Rules of Behavior to require employees to obtain written permission from their supervisors before downloading PII to the hard drive of a laptop.

SEPS does not have any written procedures for determining what data a lost or stolen electronic device may have contained, and SEPS officials stated that only one laptop has been stolen in the past 15 years. A member of SEPS's Technical Security Section stated that if a lost or stolen laptop were to be reported, the Technical Security Section would speak with the employee reporting the loss and his or her supervisor to determine what information the laptop may have contained. SEPS did not report any lost or stolen electronic devices between December 2005 and November 2006.

APPENDIX VIII: TAX DIVISION PROCEDURES

Introduction

Between December 2005 and November 2006, the Tax Division reported 22 computer security incidents to DOJCERT, none of which involved the loss of PII. The Tax Division defines reportable computer security incidents as the loss of sensitive data; PII; or any portable electronic device or removable storage media that contains Tax Division information, including the loss of any laptop, BlackBerry device, flash drive, or CD. The Tax Division considers all of its information to be sensitive, including PII, Privacy Act information, federal taxpayer information, and grand jury information. The Tax Division defines PII as information that uniquely identifies an individual, which may include social security numbers, Taxpayer ID numbers, driver's license numbers, license plate numbers, credit card numbers, current or previous addresses, current or previous telephone numbers, birthdates, maiden names, previous married names, aliases, and family or medical history. Tax return information, which is defined in Internal Revenue Service Publication 1075 and DOJ Order 2620.5A as including a taxpayer's identity and information about his or her finances, is considered to be synonymous to PII, as is Privacy Act information. The Tax Division does not generally handle classified information.

Reporting Procedures

Tax Division employees are required to notify their supervisors and the Division's Security Program Manager within 1 hour of discovering that sensitive data or PII may have been lost.[140] If Tax Division employees mistakenly contact the Help Desk to report sensitive data loss incidents, the Help Desk staff should direct them to contact the Security Program Manager. The Tax Division told us that employees have been instructed to report data loss incidents directly to the Help Desk if they are unable to reach the Security Program Manager immediately. The Help Desk should then notify the Information Systems Security Officer.

[140] On September 5, 2006, the Assistant Attorney General of the Tax Division sent a memorandum to all division employees instructing them to contact their supervisors and the division's Security Program Manager within 1 hour of discovering that sensitive data or PII may have been lost. This 1-hour timeframe is also reflected in the Tax Division's Incident Response Plan. All other types of computer security violations, incidents, and vulnerabilities are reported to the Tax Division Help Desk. The Help Desk is not required to report incidents that do not involve sensitive data or PII beyond this point.

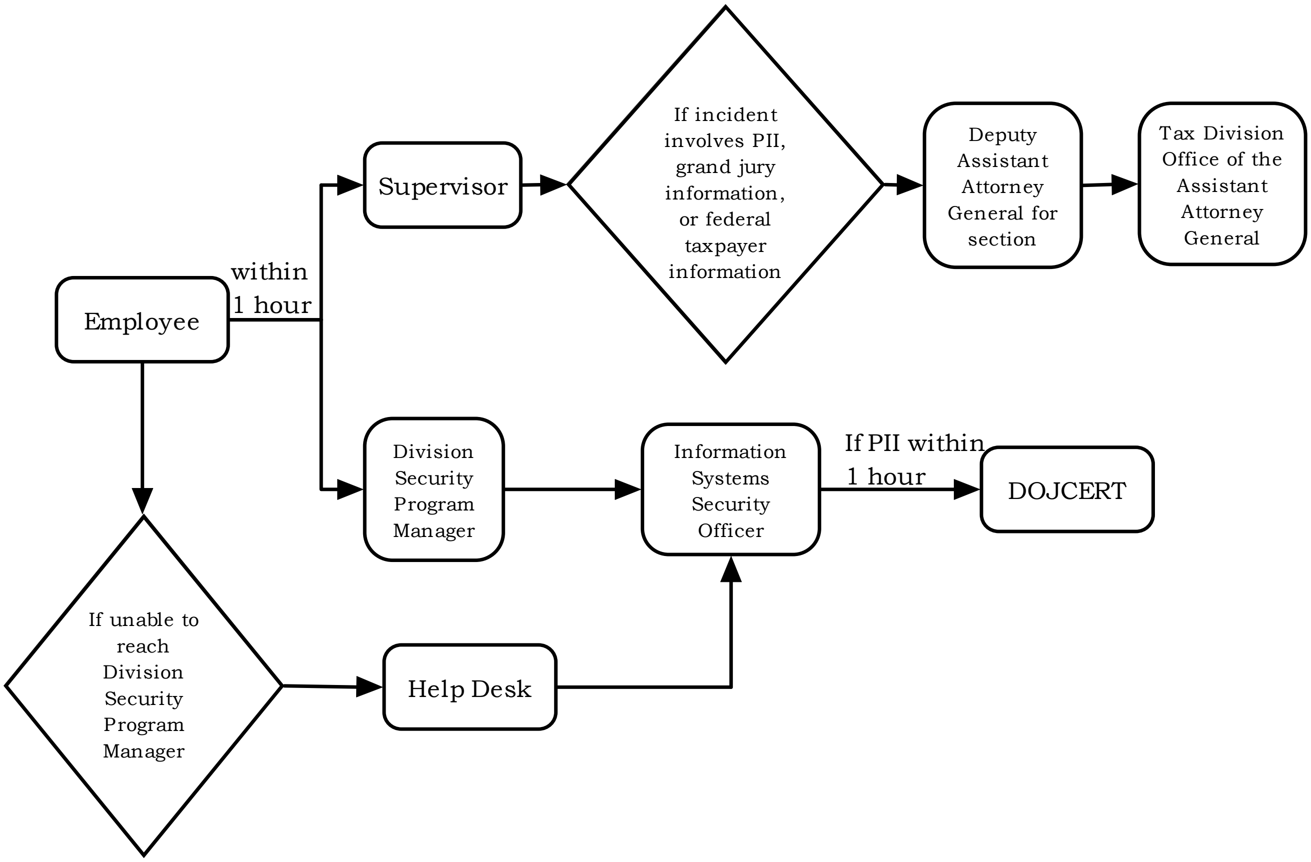
Tax Division officials also told us that if an incident occurs after hours, employees should notify their supervisors. The supervisors have an after-hours contact number for the Security Program Manager.

The Security Program Manager should notify the Tax Division's Information Systems Security Officer of all computer security incidents. The Information Systems Security Officer should notify DOJCERT, via the Archer Database, and ensure that the Tax Division follows the procedures outlined in its Incident Response Plan.[141] The Tax Division's plan identifies the seven categories of incidents that should be reported to DOJCERT within specified timeframes. The plan has been updated to reflect the required changes DOJCERT made in November 2006 to the DOJCERT Incident Response Plan template.

The Tax Division also has procedures in place for notifying senior Tax Division management of incidents. If a computer security incident includes PII, grand jury information, or federal taxpayer information, the supervisor of the employee involved should notify the Deputy Assistant Attorney General who oversees the section where the incident occurred. The Deputy Assistant Attorney General should then notify the Tax Division's Office of the Assistant Attorney General. Chart 19 shows the Tax Division's procedures for reporting loss of sensitive information, including PII.

[141] The Tax Division's Information Systems Security Officer supervises the Help Desk and thus should be aware of all reports of data loss incidents made to the Help Desk instead of to the Security Program Manager. The Information Systems Security Officer should inform the Security Program Manager of all sensitive data loss incident reports the Help Desk receives.

Chart 19: Flowchart of the Tax Division's Procedures for Reporting Sensitive Information Loss, Including PII


Employee
within 1 hour
Supervisor
If incident involves PII, grand jury information, or federal taxpayer information
Deputy Assistant Attorney General for section
Tax Division Office of the Assistant Attorney General
Division Security Program Manager
Information Systems Security Officer
If PII within 1 hour
DOJCERT
If unable to reach Division Security Program Manager
Help Desk

For internal tracking purposes, computer security incidents and equipment losses are supposed to be recorded in the Tax Division Help Desk's ticket database, known as Remedy. Equipment losses have been tracked in this way for several years, and the Tax Division began tracking data losses specifically in August 2006. The Information Systems Security Officer stated that all information tracked in Remedy is also entered into the Archer Database. Tax Division officials said they routinely query Remedy to generate reports on equipment losses.

Indications of Compliance with Reporting Procedures

Tax Division officials told us that they believed employees were following the correct reporting procedures. While we did not validate this statement, our analysis of the Archer Database showed that between December 2005 and November 2006, the Tax Division reported 95 percent of its computer security incidents within the required timeframes specified in both the DOJCERT and Tax Division Incident Response Plans. We did not analyze any Tax Division incidents for timeliness because the Tax Division did not report any incidents involving PII. Table 14 shows the Tax Division's reporting in each category.[142]

Table 14: The Tax Division's Timeliness in Reporting Incidents to DOJCERT

Category	**Reporting timeframe***	**Incidents reported**	**Reported within timeframe**	**Reported after timeframe**	**Could not compute timeliness****
Category 0 (Exercise/Test)	None	1	N/A	N/A	1
Category 1 (Unauthorized Access)	1 hour	1	1	0	0
Category 2 (Denial of Service)	2 hours	0	N/A	N/A	N/A
Category 3 (Malicious Code)	1 day	1	0	1	0
Category 4 (Improper Usage)	1 week	0	N/A	N/A	N/A
Category 5 (Scans/Probes)	1 month	1	1	0	0
Category 6 (Investigation)	None	1	N/A	N/A	1
Category 7 (Spam)	1 month	17	17	0	0
Total		**22**	**19**	**1**	**2**
PII incidents occurring on or after 7/12/06***	1 hour	0	N/A	N/A	N/A

* For purposes of this table, reporting timeframes for Categories 0-7 refer to the timeframes defined in the Incident Response Plan. Reporting timeframe for PII incidents refers to the timeframe defined in OMB Memorandum M-06-19.

** Some records did not include information to indicate when DOJCERT received the reports. Category 0 and 6 incidents, for which there are no reporting timeframes, are also included in this category.

*** PII incidents were reported in varying incident categories.

Source: Archer Database

[142] Our calculations are based on Categories 1 through 5 and Category 7. We did not include incidents found in Categories 0 and 6 because they had no associated time criteria, nor did we include incidents for which the Archer Database contained no information to indicate when DOJCERT received the report that an incident had occurred.

Ensuring All Incidents Are Reported

While the Tax Division uses several methods to ensure division employees are reporting computer security incidents, it relies primarily on training to ensure employees are aware of the requirement to report computer security incidents, including those involving loss of sensitive data or PII. The Tax Division said that it conducts annual Computer Security Awareness Training to remind users of the responsibility to report computer security incidents and has updated this training to instruct employees to report losses of PII within 1 hour. To remind employees of the importance of reporting sensitive data loss incidents, the Tax Division has also posted a copy of the Assistant Attorney General's September 5, 2006, memorandum in a prominent position on the Tax Division's intranet page. The Tax Division's Rules of Behavior also instructs employees to report known or suspected incidents to the Information Systems Security Officer. Tax Division employees are required to read and acknowledge the Rules of Behavior annually.

Tax Division officials said that lost equipment is tracked through the annual inventory process. One Tax Division official we interviewed noted that it is easier for management to determine if hardware, such as a laptop or BlackBerry device, is missing because the user will need a replacement device. For other types of computer security incidents, this same official stated that there is no failsafe method for ensuring that all incidents are reported.

Notification to Affected Parties

The Tax Division has not developed policies concerning notification to affected parties in the event of a loss of PII. Tax Division officials expressed a general desire for the Department to take a greater leadership role in computer security issues, including developing a policy on notification.

Determining the Type of Data Lost

In the Tax Division, determining the type of data loss is usually accomplished through employee interviews. In general, the Tax Division's Information Systems Security Officer is tasked with interviewing the employee reporting the loss and asks the employee to identify the information that the device may have contained. The Information Systems Security Officer may also speak with the employee's supervisor to determine which cases the employee was most likely to have been working on, but the Tax Division is ultimately dependent on the employee's memory of the device's contents.

When an employee is working off-site and a computer security incident occurs, in addition to interviewing the employee reporting the loss, the supervisor may be able to determine the type of data lost through the Tax Division's Document Management System. The Tax Division maintains a Document Management System that organizes case-related files, and employees' access is restricted to the cases to which they have been assigned. To work on Tax Division information from a remote location without having to dial in to the Tax Division's network, the employees can check out files from the Document Management System and have those files uploaded onto the hard drives of their laptops. If an employee chooses this access option and then reports the laptop lost or stolen, the Tax Division supervisor may be able to recreate the files that were on the device by reviewing the Document Management System's checked out records. Data saved on flash drives must also be saved on the Document Management System or another part of the Tax Division's network to provide a backup in the event that the flash drive is lost or stolen.[143]

Alternatively, employees can access the Tax Division's network remotely, either through a hard network connection in a United States Attorney's Office or by dialing in using Justice Secure Remote Access. When employees choose to access the network remotely, the laptop serves as a dumb terminal, with all files saved to the Tax Division's network instead of to the laptop's hard drive.

[143] Only Tax Division-purchased flash drives are permitted; these flash drives are encrypted, use biometric security (a thumbprint is required to access the data on the flash drive), and are tracked in the Tax Division's annual property inventory.

APPENDIX IX: USMS REPORTING PROCEDURES

Introduction

Between December 2005 and November 2006, the USMS reported 15 security incidents to DOJCERT, none of which involved the loss of PII or involved classified information. The USMS stated that reportable losses include the loss of electronic devices such as desktop computers, laptops, or BlackBerry devices that possibly contain classified or investigative case-sensitive information or printed documents that include PII. However, the USMS stated it did not begin tracking or reporting sensitive data loss incidents, including PII, to DOJCERT until the August 2006 Department memorandum that instructed all components to report these incidents to DOJCERT.[144]

The USMS defines sensitive information as synonymous with Law Enforcement Sensitive. In the USMS Security Programs Manager policy, Law Enforcement Sensitive information is defined as unclassified information of a sensitive and proprietary nature that if disclosed could cause harm to law enforcement activities by jeopardizing investigations, compromising operations, or causing life-threatening situations for confidential informants, witnesses, or law enforcement personnel.[145] These categories are designated as law enforcement sensitive:

- Informant and witness information;
- Grand Jury information subject to the Federal Rules of Criminal Procedure, Rule 6(e), Grand Jury Secrecy Proceedings and Disclosure;
- Investigative material;
- Law enforcement sources and undercover operations;
- Law enforcement intelligence sources and methods;
- Federal law enforcement agency activities;
- Federal support to state and local law enforcement activities;
- Information pertaining to the judiciary, to include investigations of inappropriate communications; and
- Personnel information pertaining to employees of the USMS.

While the USMS does not currently have a definition for PII, it considers those records requiring protection under the Privacy Act to be a subset of Limited Official Use information. The USMS defines Limited

[144] DOJ Memorandum, Reporting Incidents Involving Data Loss and Personally Identifiable Information, Vance Hitch, CIO, August 7, 2006.

[145] USMS Directive 2.34, Security Programs Manager, November 9, 2005.

Official Use information as unclassified information of a sensitive, proprietary, or personally private nature that must be protected against release to unauthorized individuals. The following categories of information are designated as Limited Official Use information:

- Tax information subject to 26 U.S.C. § 6103, Confidentiality and Disclosure of Returns and Return Information;
- Information that could be sold for profit;
- Personal information subject to the Privacy Act;
- Memorandums or reports that disclose security vulnerabilities;
- Information that could result in physical risk to individuals;
- Company proprietary information;
- Audit staff work papers;
- Draft audit reports;
- Information offered in confidence during the conduct of internal audits, comprehensive assessments, program reviews, and evaluations;
- Program and budget information on intelligence-related activities; and
- Sensitive Antideficiency Act material.[146]

The USMS uses the definition of classified information contained in Executive Order 12958, as Amended, Classified National Security Information, dated March 25, 2003.

Reporting Procedures

Reporting Procedures for Non-Classified Incidents

The USMS relies on four policies when reporting computer security incidents:

- USMS Incident Response Plan, December 8, 2005;
- USMS Directive 2.34, Security Programs Manager, November 9, 2005;
- USMS Directive 12, Information Resources Management, effective October 6, 2003, updated April 3, 2006; and
- USMS Directive 7.1, Management of Personal Property, October 6, 2003.

It should be noted that the four policies provide conflicting chain-of-command reporting procedures. For example, the policies instruct employees to report computer security incidents to staff titles

[146] USMS Directive 2.34, Security Programs Manager, November 9, 2005, Attachment III F.2.

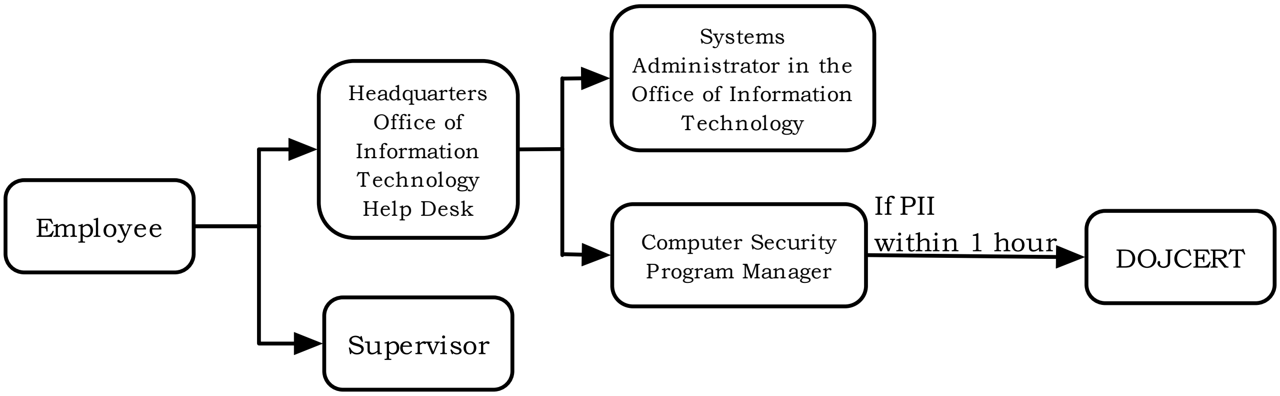
and internal departments that either no longer exist or are incorrect. Therefore, the reporting procedures described here are the actual practices as described in interviews with USMS officials, supplemented by the policies.

USMS employees are to immediately report suspected computer security incidents involving sensitive information loss including PII to the Office of Information Technology's Help Desk at USMS Headquarters and the employee's supervisor. If the incident involves lost or stolen property, the employee is also required to notify the office property custodian (as required by USMS Property Management regulations for reporting lost or stolen property) and the Office of Investigations (as appropriate for stolen property).[147] The Help Desk should then notify the appropriate Systems Administrator in the Office of Information Technology as soon as possible to help evaluate the incident.[148] The Help Desk, after recording general information about the incident, should then notify the Computer Security Program Manager, also at Headquarters, who interviews the employee involved about the circumstances surrounding the event. With the information gathered during the interview, the Computer Security Program Manager is required to report the incident to DOJCERT via a telephone call. The USMS does not currently use their electronic access to DOJCERT's Archer Database for reporting incidents online. Chart 20 shows the USMS's procedures for reporting sensitive information loss, including PII.

[147] USMS Directive 12, Information Resources Management, Appendix H, effective October 6, 2003, updated April 3, 2006. The Office of Investigations is also known as Internal Investigations.

[148] There are 50 Systems Administrators to support 400 locations in 94 USMS districts. While the majority of the USMS offices do not have a Systems Administrator, in the locations where one exists the employee reports a data loss first to the Systems Administrator, who then reports the incident to the Help Desk. In locations where no Systems Administrator exist, the employee calls the Help Desk at Headquarters and the employee's supervisor.

Chart 20: Flowchart of the USMS's Procedures for Reporting Sensitive Information Loss, Including PII


Employee
Headquarters Office of Information Technology Help Desk
Supervisor
Systems Administrator in the Office of Information Technology
Computer Security Program Manager
If PII within 1 hour
DOJCERT

Reporting Procedures for Data Loss that Include PII

As of April 2007, the USMS had not yet updated its Incident Response Plan to reflect requirements for investigating and reporting data loss incidents that include the loss of PII. DOJCERT added the data loss and PII requirements to its Incident Response Plan template in November 2006 with the requirement that all components incorporate this update by December 29, 2006. The USMS stated that it planned to update its Incident Response Plan and include this revision by mid-March 2007. The USMS did e-mail its staff on August 29, 2006, informing them of their responsibility to report all known incidents of sensitive data loss and PII "within 1 hour of discovery or detection."[149] The USMS does not have procedures for reporting computer security incidents after hours.

Reporting Procedures for Classified Information

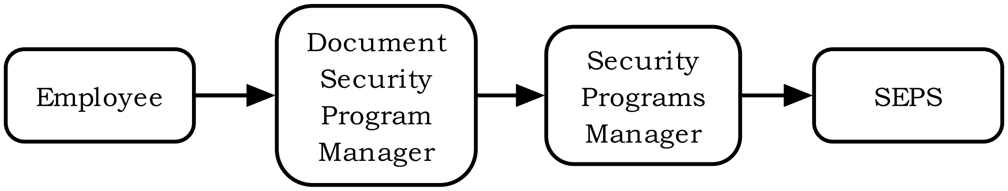
If classified information is involved in a computer security incident, employees must promptly report by telephone and confirm in writing the circumstances of the incident to the USMS Document Security Program Manager, who is responsible for the receipt, handling, safeguarding, and storage of all classified material within the USMS.[150] The Document Security Program Manager is responsible for notifying the USMS Security Programs Manager. The USMS Security Programs Manager is required to

[149] USMS E-Mail to All Staff, Notice From OSD Re: Reporting Incidents Involving Data Loss and Personally Identifiable Information, August 29, 2006.

[150] USMS Directive 2.34, Security Programs Manager, Attachment C, November 9, 2005, pp. 13-14.

then notify the Department's Security Officer, Security and Emergency Planning Staff (SEPS). Chart 21 shows the USMS's procedures for reporting classified information loss.

Chart 21: Flowchart of the USMS's Procedures for Reporting Classified Information Loss



Additional Reporting Requirements

According to the USMS policy on Management of Personal Property, employees are required to notify the property custodian through their supervisor if an incident involves lost or missing electronic equipment, including a laptop or desktop computer or a BlackBerry device.[151] The property custodian should complete a form/affidavit with descriptive information about the event and forwards that form to the Office of Property Management. The Office of Property Management is required to refer reports of loss to the Board of Survey if the loss is likely to have been the result of willful intent, gross negligence, neglect, misuse, theft, or misconduct. If the loss involves sensitive property such as desktop and laptop computers or BlackBerry devices that possibly contain classified or investigative case-sensitive information, a copy of the report should be provided to the Office of Internal Affairs (also known as Internal Investigations).[152] The property custodian should also report lost sensitive property to the NCIC. In the event of stolen property, the employee should notify the local police department.

Indications of Compliance with Reporting Procedures

USMS officials told us that they believed their employees were following the correct reporting procedures. While we did not validate this statement, our analysis of the Archer Database showed that the USMS

[151] The property custodian is the Chief Deputy U.S. Marshal within a district office or the head of office within a Headquarters component. See USMS Directive 7.1, Management of Personal Property, October 6, 2003.

[152] USMS Memorandum to All USMS Employees, Reporting Losses of USMS Property, Director, November 5, 2002.

was not always reporting computer security incidents within the required timeframes specified in both the DOJCERT and USMS Incident Response Plans. Between December 2005 and November 2006, the USMS reported 62 percent of its computer security incidents to DOJCERT within the required timeframes. We did not analyze any USMS PII incidents for timeliness because the USMS did not report any incidents involving PII. Table 15 shows the USMS's reporting in each category.[153]

Table 15: The USMS's Timeliness in Reporting Incidents to DOJCERT

Category	Reporting timeframe*	Incidents reported	Reported within timeframe	Reported after timeframe	Could not compute timeliness**
Category 0 (Exercise/Test)	None	0	N/A	N/A	N/A
Category 1 (Unauthorized Access)	1 hour	2	0	2	0
Category 2 (Denial of Service)	2 hours	0	N/A	N/A	N/A
Category 3 (Malicious Code)	1 day	4	1	2	1
Category 4 (Improper Usage)	1 week	2	2	0	0
Category 5 (Scans/Probes)	1 month	0	N/A	N/A	N/A
Category 6 (Investigation)	None	0	N/A	N/A	N/A
Category 7 (Spam)	1 month	7	5	1	1
Total		**15**	**8**	**5**	**2**
PII incidents occurring on or after 7/12/06***	1 hour	0	N/A	N/A	N/A

* For purposes of this table, reporting timeframes for Categories 0-7 refer to the timeframes defined in the Incident Response Plan. Reporting timeframe for PII incidents refers to the timeframe defined in OMB Memorandum M-06-19.

** Some records did not include information to indicate when DOJCERT received the reports. Category 0 and 6 incidents, for which there are no reporting timeframes, are also included in this category.

*** PII incidents were reported in varying incident categories.

Source: Archer Database

[153] Our calculations are based on Categories 1 through 5 and Category 7. We did not include incidents found in Categories 0 and 6 because they had no associated time criteria, nor did we include incidents for which the Archer Database contained no information to indicate when DOJCERT received the report that an incident had occurred.

Ensuring All Incidents Are Reported

The USMS stated that it relies primarily on the Department's required annual Computer Security Awareness Training to educate and remind staff of their reporting responsibilities as well as what is considered a reportable incident. However, we were informed during an interview that employees did not have access to this training in 2006 due to technical difficulties the USMS had in supporting the Computer Security Awareness Training online. The USMS also said that it relies on several written policies and memorandums to inform staff of their responsibilities to report lost or stolen government-issued equipment that may contain sensitive information.

In August 2006, the USMS e-mailed a memorandum to all USMS employees informing them of their responsibility to report all incidents involving known loss of sensitive data and PII within 1 hour of discovery or detection.[154] Additionally, the memorandum stated that the loss of any data storage devices, such as laptops, flash drives, disks, and tapes, should be reported within the same 1-hour timeframe.

As stated above, the USMS policy on Management of Personal Property requires employees to make the loss of property known immediately through his or her supervisor to the property custodian. Property custodians are required to maintain accountability for all property on the accountable property record through physical inventories and the maintenance of current property records. A comprehensive physical inventory of all accountable property is required every 2 years.

USMS Rules of Behavior, which all employees must read and sign, require employees to report all actual or suspected security violations, vulnerabilities, and incidents to the first-line supervisor and other appropriate staff.[155]

Notification to Affected Parties

The USMS has not developed policies concerning notification to affected parties in the event of a loss of PII.

[154] USMS e-mail to all staff, Notice From OSD Re: Reporting Incidents Involving Data Loss and Personally Identifiable Information, August 29, 2006.

[155] USMS Directive 12, Information Resources Management, Appendix C, Rules of Behavior, effective October 6, 2003, updated April 3, 2006.

Determining the Type of Data Lost

To determine the type of data lost or compromised, the USMS primarily relies on the Chief of Enterprise Management at Headquarters interviewing the employee involved. The Chief said that she questions the employee using an internal form containing 23 questions. Several of the questions ask about applications accessed from the lost laptop or BlackBerry device, whether information was saved to the hard drive, and the type of information the lost device contained. The Chief said that she intends to eventually train the Help Desk to conduct these initial interviews and complete the interview forms. However, the Chief or a member of her staff will remain the point of contact for notifying DOJCERT.

APPENDIX X: ACTS, DIRECTIVES, AND STANDARDS

- **Federal Information Security Management Act (FISMA) of 2002** – This Act actually is Title III of the E-Government Act of 2002. It defines federal requirements for securing information and information systems that support federal agency operations and assets and requires agencies to develop agency-wide information security programs. Under FISMA, civilian agencies are required to notify the U.S. Computer Emergency Readiness Team (US-CERT) in the Department of Homeland Security, within certain timeframes based on the type of incident, e.g., data breaches, unauthorized access, or suspicious activity on their networks. In July 2006, OMB expanded the rule to cover all incidents that include PII. FISMA also requires the Inspectors General to conduct an annual independent evaluation of the information security program and practices of every agency. To support agencies in conducting their information security programs, FISMA called for the National Institute of Standards and Technology (NIST) to develop federal standards for the security categorization of federal information and information systems according to risk levels and for minimum security requirements for information and information systems in each security category.

- **E-Government Act of 2002** – This Act ensures sufficient protection for the privacy of personal information in electronic government systems by requiring that agencies conduct Privacy Impact Assessments (PIA). A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. FISMA is Title III of the E-Government Act.

- **Privacy Act of 1974** – limits agencies' collection, maintenance, use, and dissemination of information maintained in a system of records. The purpose of the Privacy Act is to balance the government's need to maintain information about individuals with the right of those individuals to be protected against unwarranted invasions of their privacy. The Act restricts disclosure of protected information; grants individuals the right to access and amend such records; and establishes a code of "fair information practices" that requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.[156]

[156] See www.usdoj.gov/oip/04_7_1.html for an overview of the Privacy Act.

- **OMB Memorandum M-06-20** (July 17, 2006) – Fiscal year 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. This memorandum provides instructions to all departments and agencies for meeting the fiscal year 2006 requirements of the FISMA Act of 2002. It also adds the requirements that all Inspectors General provide a list of any systems they have found missing from the agency's inventory of major information systems (as required under the E-Government Act of 2002) and the identification of any physical or electronic incidents involving the loss or unauthorized access to PII and reporting of such in accordance with OMB Memorandum M-06-19.

- **OMB Memorandum M-06-19** (July 12, 2006) – Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments. This memorandum defines PII and provides updated guidance on the reporting of security incidents involving PII. By issuing this memorandum, OMB required that all security incidents involving PII be reported within 1 hour of the incident's discovery. US-CERT is required to forward all agency reports to the appropriate Identity Theft Task Force point-of-contact also within 1 hour of notification by an agency. Agencies are also required to identify specific funds they are requesting for correcting any security weaknesses identified by their Inspectors General or the Government Accountability Office.

- **OMB Memorandum M-06-16** (June 23, 2006) – Protection of Sensitive Agency Information. This memorandum advises heads of Departments and agencies of the NIST Checklist for protection of remote information and recommends additional action to take such as encrypting all data on mobile computers and other devices, allowing remote access only with two-factor authentication, using a time-out function after 30 minutes for remote access, and logging all extractions of sensitive information and verifying that each extract has been erased within 90 days or that its use is still necessary.

- **OMB Memorandum M-06-15** (May 22, 2006) – Safeguarding Personally Identifiable Information. This memorandum reminds heads of Departments and agencies of their responsibilities under law and policy to safeguard sensitive PII and to train employees on their responsibilities in this area.

- **OMB Circular A-130** (November 28, 2000) – Management of Federal Information Resources. This circular established policies for the management, collection, and dissemination of federal information resources, as required by the Paperwork Reduction Act of 1980.

- **DOJ Order 2740.1** (November 7, 2005) – Use and Monitoring of DOJ Computers and Computer Systems. This order states the Department's policy on the use of departmental computers and computer systems, the lack of expectation of privacy with respect to such use, and authorized monitoring of or access to information on departmental computers and computer systems.

- **DOJ Order 2880.1B** (September 27, 2005) – Information Resources Management Program. This order establishes Department policy governing the planning, management, operation, and use of information technology (IT) resources. It includes a section on information technology security that states in part that, quote:

  - The Department shall develop and manage an agency wide Information Technology Security Program consistent with the laws and regulations affecting IT Security.

  - Department IT systems processing Sensitive Compartmentalized Information (SCI) shall have controls implemented consistent with the IT security controls established by the intelligence community. All IT systems that process, store, or transmit SCI shall be coordinated with the CIO prior to development and approved by the Department Security Officer prior to their operation.

- **DOJ Order 2640.2E** (November 28, 2003) – Information Technology Security. This order establishes uniform policy, responsibilities, and authorities for the implementation and protection of Department IT systems that store, process, or transmit classified and unclassified information.

- **Information Technology Security Approved Standards** (December 2003–July 2005) – JMD's Information Technology Security Staff standards establish the management, operational, and technical controls for the Department's information systems.

- **NIST Special Publication 800-53A** (April 2006) – *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft). This publication provides methods and procedures to assess the effectiveness of security controls in federal information systems. The guidance allows federal agencies to develop more secure information systems.

- **NIST Special Publication 800-53** (February 2005) – *Recommended Security Controls for Federal Information Systems.* This publication defines minimum security controls needed to provide cost-effective protection for low-, moderate-, and high-impact information systems and the information processed, stored, and transmitted by those systems. These are the standards used for certification and accreditation of federal IT systems.

- **NIST Special Publication 800-61** (January 2004) – *Computer Security Incident Handling Guide.* This guide discusses how to organize a security incident response capability and how to handle incidents, including denial of service, malicious code, unauthorized access, and inappropriate use of systems incidents.

- **Federal Information Processing Standards Publication (FIPS) 200** (March 2006) – *Minimum Security Requirements for Federal Information and Information Systems.* FIPS Publication 200 specifies minimum security requirements for federal information and information systems and a risk-based process for selecting the security controls necessary to satisfy the minimum requirements. In applying the FIPS 200 provisions, agencies categorized their information systems as required by FIPS Publication 199 and selected an appropriate set of security controls from NIST Special Publication 800-53 to satisfy the minimum security requirements. FIPS 200 specifies minimum security requirements for federal information and information systems that represent a broad-based, balanced information security program. The requirements are organized into 17 areas, encompassing the management, operational, and technical aspects of protecting federal information and information systems: access control; audit and accountability; awareness and training; certification, accreditation and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; personnel security; physical and environmental protection; planning; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity.

- **Federal Information Processing Standards Publication 199** (February 2004) – *Standards for Security Categorization of Federal Information and Information Systems.* FIPS 199 is the first standard that was specified by FISMA. It requires agencies to categorize their information and information systems as low-, moderate-, or high-impact based on the potential impact of a loss of confidentiality, integrity, or availability of information or an information system.

APPENDIX XI: COMPONENT POLICIES

ATF	● Computer Security Incident Response Capability Incident Response Plan, July 24, 2006 ● Automated Information System Security Program, ATF Policy H 7250.1, July 26, 2006 ● Computer Security Incident Response Capability, ATF Order O 7500.4A, April 12, 2005
BOP	● Incident Response Plan, December 2006 ● Information Resources Protection, BOP Directive 1237.12, February 20, 2001 ● Information Security Programs for Sensitive But Unclassified (SBU) Information, BOP Directive 1237.13, March 31, 2006 ● Property Management Manual, BOP Directive 4400.05, May 26, 2004 ● Release of Information, BOP Directive 1351.05, September 19, 2002
CRM	● Incident Response Plan, December 1, 2006 ● Criminal Division Administrative Policy Memorandum 80-8, Classified Processing, January 14, 2003 ● Criminal Division Security Acknowledgement Statement for System Administrators and Privileged Users, November 2006
DEA	● Computer Incident Response Plan, December 29, 2006 ● DEA Policy: Control and Decontrol of DEA Sensitive Information, REF 99-001, June 2, 1999 ● Broadcast E-mail Message to all DEA employees: Personally Identifiable Information (PII) Media Loss Reporting Requirements and Procedures, October 12, 2006 ● Safeguarding Personally Identifiable and Other Sensitive Information, Chief Inspector's Bulletin, DEA Inspection Division, October 20, 2006 ● Memorandum to DEA Deputy Assistant Administrator, Office of Information Systems, Amendment to the Interim Information Technology Rules of Behavior – Protecting Sensitive and Personally Identifiable Information, November 6, 2006 ● Employee Responsibilities and Conduct

EOUSA

- Incident Response Plan, December 13, 2006
- Memorandum to Anti-Terrorism Task Force Officials, Limited Official Use (Sensitive) Information Designation, January 14, 2003
- U.S. Attorney's Manual, Chapter 3-15, Security Programs Management, August 2004
- U.S. Attorneys' Procedures (USAP 3-13.300.001), Records Management and Case File Disposition, October 24, 2006
- U.S. Attorneys' Procedures (USAP 3-16.000.001), Computer Assisted Legal Research, October 4, 2006
- U.S. Attorneys' Procedures (USAP 3-16-200.003), Access to Sensitive But Unclassified (SBU) IT Resources, January 13, 2006
- U.S. Attorneys' Procedures (USAP 3-16.200.008), Sensitive But Unclassified Laptop Computer Security, January 26, 2006
- U.S. Attorneys' Procedures (USAP 3-16.300.006), Personal Digital Assistants (PDAs), September 13, 2006
- U.S. Attorneys' Procedures (USAP 3-15.120.002), Handling and Safeguarding Federal Tax Information, November 7, 2006
- U.S. Attorneys' Manual, Chapter 3-13, Procurement/Property Management, July 2000
- EOUSA Resource Manual, Sections 119-126

FBI

- Incident Response Plans for the Criminal Justice Information Services Division; SCI Operational Network; FBI Secret; and Unclassified Network, all updated December 2006
- FBI Security Policy Manual, Chapters 17, 21, 22, and Appendix A, April 2006
- Systems User Rules of Behavior
- Memorandum to All FBI Divisions, Reiterating Policy for the Safeguarding of Government Property Outside of FBI Office Space, FBI Finance Division, August 23, 2002
- Memorandum to All FBI Divisions, Reiterate Policy Requirement to Place Property on the Property Management Application Upon Receipt, FBI Finance Division, August 23, 2002

	● Memorandum to All FBI Divisions, Policy Change for Submission of FD-500s, Report of Lost or Stolen Property, FBI Finance Division, November 4, 2005 ● Procedures for Reporting Lost or Stolen Property, Accountable Property Manual ● Memorandum to All FBI Divisions, Reiterating Mandatory Policy for the Assignment and Charge-Out of Laptop Computers, FBI Finance Division, March 15, 2006 ● Memorandum to All FBI Divisions, Security Incident Program, Security Compliance Unit, Security Division, FBI Security Division, February 9, 2006 ● Manual of Investigative Operational Guidelines, Part 1, Section 52, Government Property – Theft, Robbery, Embezzlement ● Manual of Administrative Operations and Procedures, Part 2, Section 6-7.5, Lost or Stolen Government Property/Lost or Stolen Personal Property in Government Space
JMD[157]	● Incident Response Plan for Systems Operated by the Personnel Staff, December 1, 2006 ● Rules of Behavior for Systems Operated by the Personnel Staff ● Incident Response Plan for Systems Operated by the Security and Emergency Planning Staff, November 2006
TAX	● Incident Response Plan, December 20, 2006 ● Tax Division Directive No. 101, Physically Protecting Portable Computers While On Official Travel ● Tax Division Directive No. 130, Use of Mass Storage Devices Within The Tax Division, March 9, 2006 ● Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information, IRS Publication 1075 ● Memorandum to Members of the Tax Division, Computer Security, November 17, 2005

[157] Each subcomponent within JMD develops its own Incident Response Plan and other policies for responding to computer security incidents. The policies identified in this table were provided to the OIG as examples of the types of policies developed by all subcomponents of JMD.

- Tax Division Security Features User Guide for JCON II/TaxDoc, October 3, 2006
- Memorandum to All Tax Division Personnel, Personally Identifiable Information: Safeguarding It and Reporting Its Loss, September 5, 2006

USMS

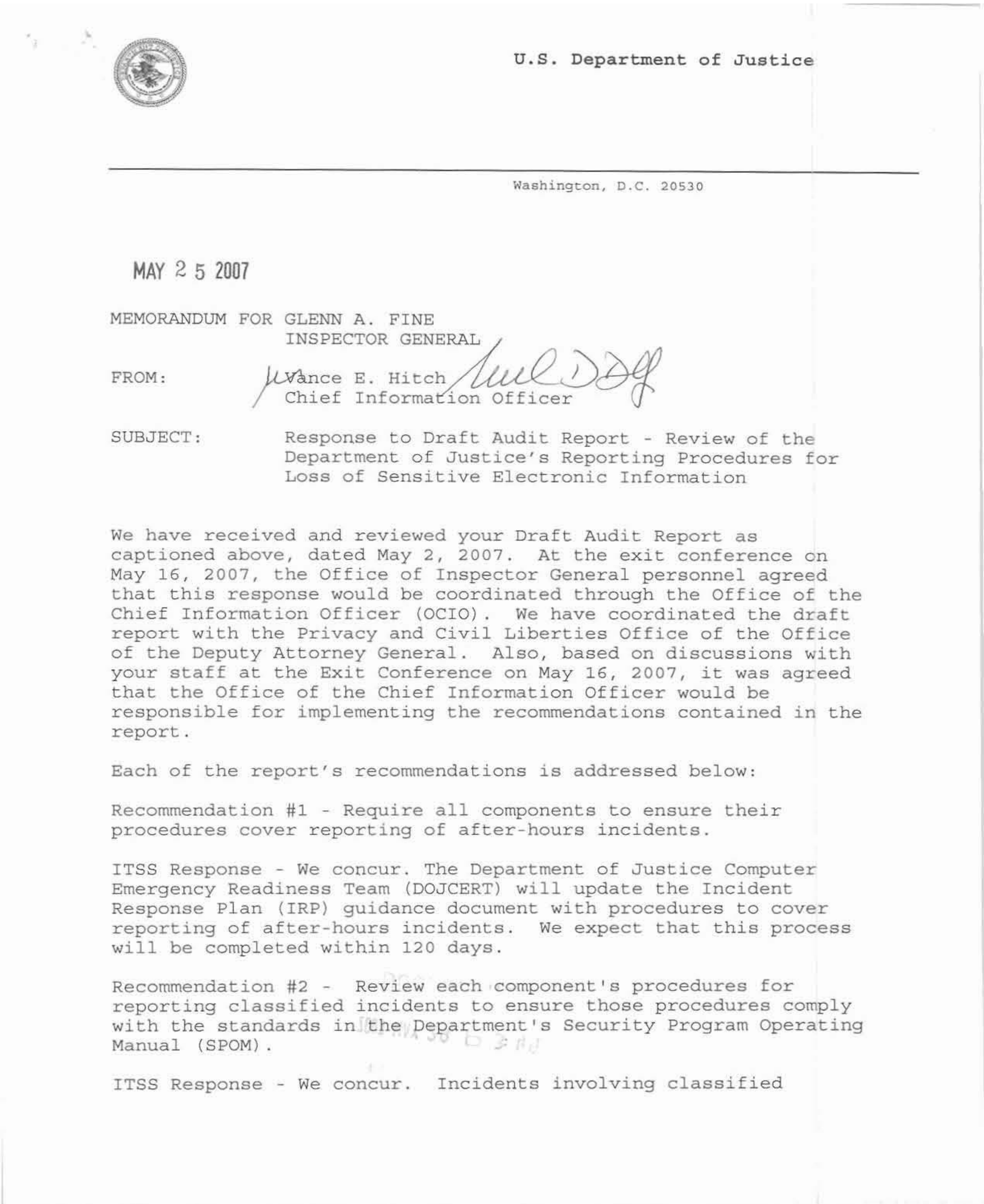
- Incident Response Plan, December 8, 2005
- USMS Directive 2.34 and Attachments B and C, Security Programs Manager, November 9, 2005
- USMS Directive 7.1, Management of Personal Property, October 6, 2003
- Broadcast e-mail from USMS Security Programs Manager, Notice from OSD re: Reporting Incidents Involving Data Loss and Personally Identifiable Information, August 29, 2006
- Memorandum from the Director, Reporting Losses of USMS Property, November 5, 2002
- USMS Directive 12, Information Resources Management, effective October 6, 2003, updated April 3, 2006

APPENDIX XII: SEVEN CATEGORIES OF SECURITY INCIDENTS AND REQUIRED TIMEFRAMES FOR REPORTING INCIDENTS

Category	Name	Description	Reporting timeframe
0	Exercise/ Network Defense Testing	This category is used during Department exercises activity testing of internal/external network defenses or responses.	As defined in the exercise requirements.
1	Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.	Within 1 hour of discovery/detection, followed by written report within 24 hours.
2	Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within 2 hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity, followed by written report within 24 hours.
3	Malicious Code	*Successful* installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Components are NOT required to report malicious logic that has been *successfully quarantined* by antivirus software.	Daily Note: Within 1 hour of discovery/detection if widespread across agency, followed by written report within 24 hours.
4	Improper Usage	A person violates acceptable computing use policies.	Weekly
5	Scans/Probes/ Attempted Access	This category includes any activity that seeks to access or identify a Department computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within 1 hour of discovery.
6	Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Periodically as information is developed. This category is for each component's use in categorizing a potential incident that is currently being investigated.

Category	Name	Description	Reporting timeframe
7	Spam	Commercial advertising, inappropriate content, or other non-phishing spam.	Monthly

APPENDIX XIII: OFFICE OF THE CHIEF INFORMATION OFFICER RESPONSE



U.S. Department of Justice

Washington, D.C. 20530

MAY 2 5 2007

MEMORANDUM FOR GLENN A. FINE
INSPECTOR GENERAL

FROM: Vance E. Hitch
Chief Information Officer

SUBJECT: Response to Draft Audit Report - Review of the Department of Justice's Reporting Procedures for Loss of Sensitive Electronic Information

We have received and reviewed your Draft Audit Report as captioned above, dated May 2, 2007. At the exit conference on May 16, 2007, the Office of Inspector General personnel agreed that this response would be coordinated through the Office of the Chief Information Officer (OCIO). We have coordinated the draft report with the Privacy and Civil Liberties Office of the Office of the Deputy Attorney General. Also, based on discussions with your staff at the Exit Conference on May 16, 2007, it was agreed that the Office of the Chief Information Officer would be responsible for implementing the recommendations contained in the report.

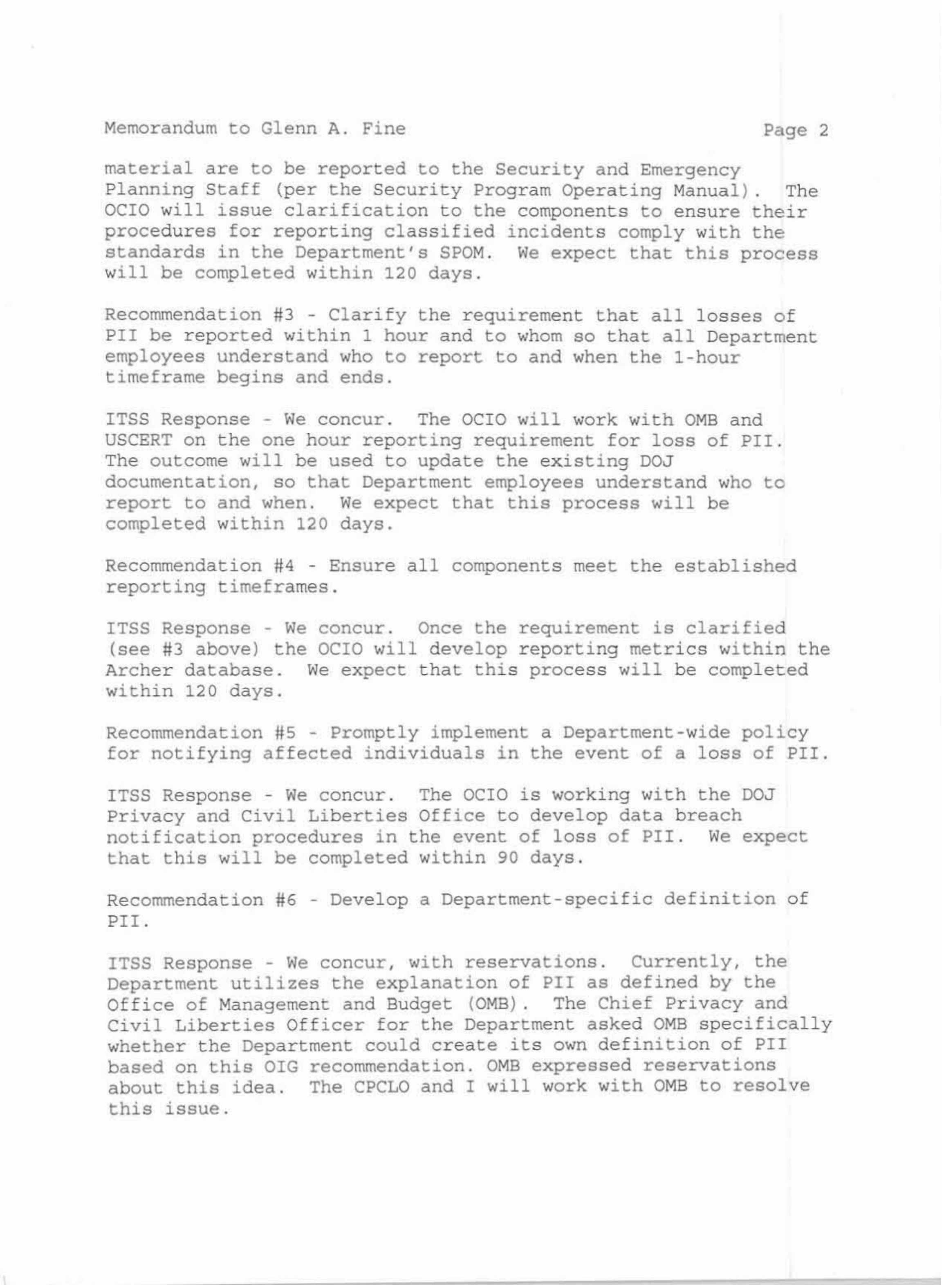
Each of the report's recommendations is addressed below:

Recommendation #1 - Require all components to ensure their procedures cover reporting of after-hours incidents.

ITSS Response - We concur. The Department of Justice Computer Emergency Readiness Team (DOJCERT) will update the Incident Response Plan (IRP) guidance document with procedures to cover reporting of after-hours incidents. We expect that this process will be completed within 120 days.

Recommendation #2 - Review each component's procedures for reporting classified incidents to ensure those procedures comply with the standards in the Department's Security Program Operating Manual (SPOM).

ITSS Response - We concur. Incidents involving classified



material are to be reported to the Security and Emergency Planning Staff (per the Security Program Operating Manual). The OCIO will issue clarification to the components to ensure their procedures for reporting classified incidents comply with the standards in the Department's SPOM. We expect that this process will be completed within 120 days.

Recommendation #3 - Clarify the requirement that all losses of PII be reported within 1 hour and to whom so that all Department employees understand who to report to and when the 1-hour timeframe begins and ends.

ITSS Response - We concur. The OCIO will work with OMB and USCERT on the one hour reporting requirement for loss of PII. The outcome will be used to update the existing DOJ documentation, so that Department employees understand who to report to and when. We expect that this process will be completed within 120 days.

Recommendation #4 - Ensure all components meet the established reporting timeframes.

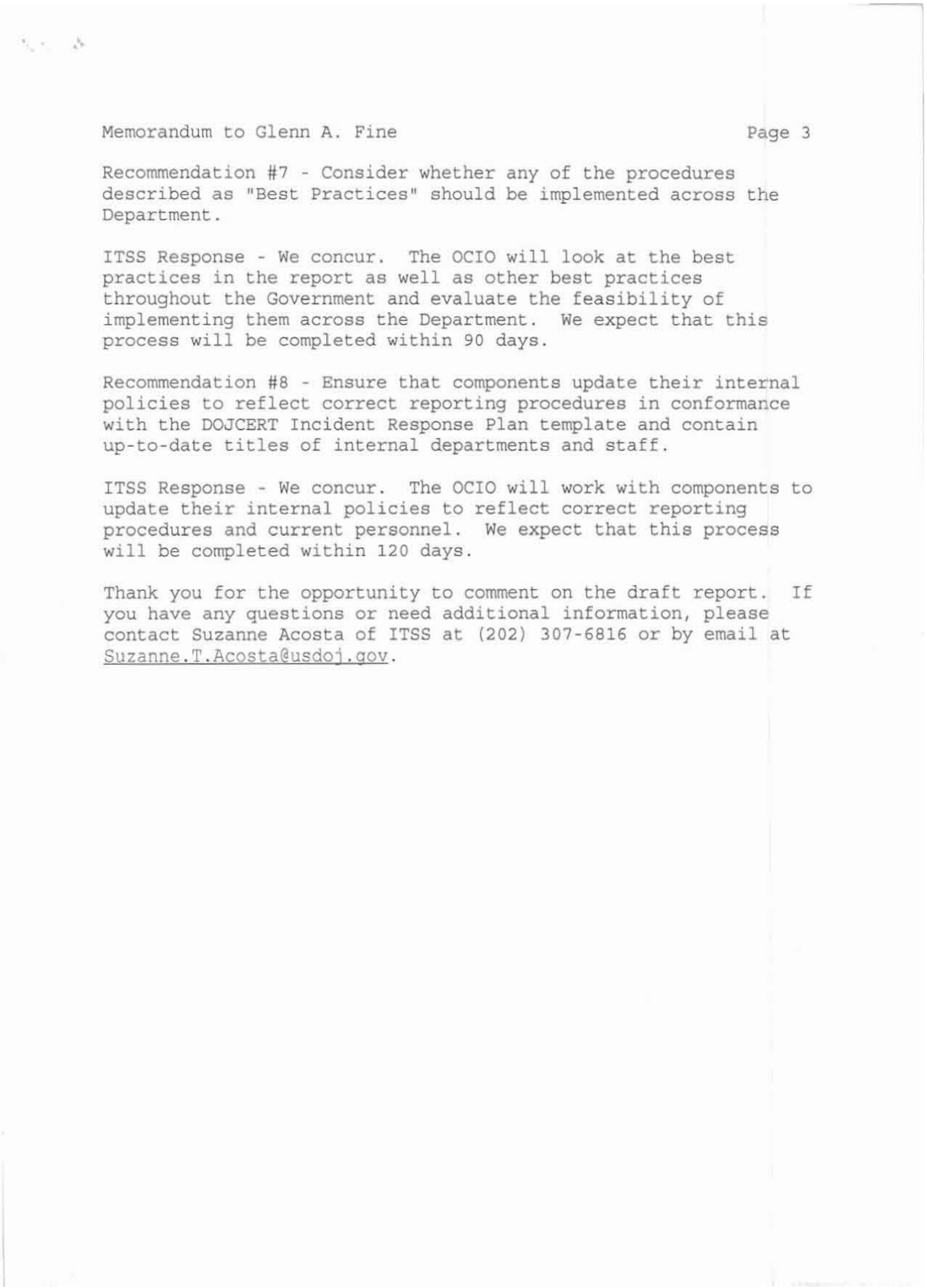
ITSS Response - We concur. Once the requirement is clarified (see #3 above) the OCIO will develop reporting metrics within the Archer database. We expect that this process will be completed within 120 days.

Recommendation #5 - Promptly implement a Department-wide policy for notifying affected individuals in the event of a loss of PII.

ITSS Response - We concur. The OCIO is working with the DOJ Privacy and Civil Liberties Office to develop data breach notification procedures in the event of loss of PII. We expect that this will be completed within 90 days.

Recommendation #6 - Develop a Department-specific definition of PII.

ITSS Response - We concur, with reservations. Currently, the Department utilizes the explanation of PII as defined by the Office of Management and Budget (OMB). The Chief Privacy and Civil Liberties Officer for the Department asked OMB specifically whether the Department could create its own definition of PII based on this OIG recommendation. OMB expressed reservations about this idea. The CPCLO and I will work with OMB to resolve this issue.



Memorandum to Glenn A. Fine Page 3

Recommendation #7 - Consider whether any of the procedures described as "Best Practices" should be implemented across the Department.

ITSS Response - We concur. The OCIO will look at the best practices in the report as well as other best practices throughout the Government and evaluate the feasibility of implementing them across the Department. We expect that this process will be completed within 90 days.

Recommendation #8 - Ensure that components update their internal policies to reflect correct reporting procedures in conformance with the DOJCERT Incident Response Plan template and contain up-to-date titles of internal departments and staff.

ITSS Response - We concur. The OCIO will work with components to update their internal policies to reflect correct reporting procedures and current personnel. We expect that this process will be completed within 120 days.

Thank you for the opportunity to comment on the draft report. If you have any questions or need additional information, please contact Suzanne Acosta of ITSS at (202) 307-6816 or by email at Suzanne.T.Acosta@usdoj.gov.

APPENDIX XIV: OIG ANALYSIS OF THE OFFICE OF THE CHIEF INFORMATION OFFICER RESPONSE

On May 4, 2007, the OIG sent copies of the draft report to the Office of the Deputy Attorney General, the Privacy and Civil Liberties Office of the Deputy Attorney General, the Office of the Chief Information Officer (CIO), and the nine components involved in the review with a request for comments. In a memorandum dated May 25, 2007, the Office of the CIO responded to the report's eight recommendations on behalf of the Department of Justice (Department). As a result of that response, Recommendation 7 is closed, and Recommendations 1 through 6 and 8 are resolved and remain open.

In addition to the comments received from the Office of the CIO, we received formal comments from the DEA and the USMS. We address their comments in Appendices XV through XVIII below. The Criminal Division, EOUSA, the FBI, and the Tax Division sent informal comments discussing technical and factual matters, and we made revisions to the report where appropriate to address these comments. ATF, the BOP, and JMD did not offer any technical or factual corrections to the report.

Summary of the Office of the CIO Response and OIG Analysis

Recommendation 1. Require all components to ensure their procedures cover reporting of after-hours incidents.

Status. Resolved – open.

Summary of the Office of the CIO Response. The Office of the CIO concurred with this recommendation and stated that the Department of Justice Computer Emergency Readiness Team (DOJCERT) will update the Incident Response Plan template with procedures to cover reporting of after-hours incidents within 120 days.

OIG Analysis. The action proposed by the Office of the CIO is responsive to our recommendation. So that we may close this recommendation, please provide the OIG with a copy of the revised Incident Response Plan template reflecting these updates by October 1, 2007.

Recommendation 2. Review the components' procedures for reporting classified incidents to ensure those procedures comply

with the standards in the Department's *Security Program Operating Manual*.

Status. Resolved – open.

Summary of the Office of the CIO Response. The Office of the CIO concurred with this recommendation and stated that it would issue a clarification to the components within 120 days to ensure their procedures for reporting classified incidents comply with the standards in the Department's *Security Program Operating Manual*.

OIG Analysis. The action proposed by the Office of the CIO is responsive to our recommendation. So that we may close this recommendation, please provide the OIG with a copy of the clarification to the components by October 1, 2007.

<u>Recommendation 3</u>. Clarify the requirement that all losses of PII be reported within 1 hour and to whom so that all Department employees understand who to report to and when the 1-hour timeframe begins and ends.

Status. Resolved – open.

Summary of the Office of the CIO Response. The Office of the CIO concurred with this recommendation and stated that it would work with the Office of Management and Budget (OMB) and the United States Computer Emergency Readiness Team (US-CERT) to clarify the 1-hour reporting requirement. The Office of the CIO stated that existing Department documentation will be updated within 120 days to reflect the results of these discussions.

OIG Analysis. The action proposed by the Office of THE CIO is responsive to our recommendation. So that we may close this recommendation, please provide the OIG with a copy of the revised Incident Response Plan template reflecting these updates by October 1, 2007.

<u>Recommendation 4</u>. Ensure all components meet the established reporting timeframes.

Status. Resolved – open.

Summary of the Office of the CIO Response. The Office of the CIO concurred with this recommendation and stated that once it has completed the actions proposed for Recommendation 3, it will develop reporting metrics within the Archer Database to track the components' compliance with the reporting timeframes.

OIG Analysis. The action proposed by the Office of the CIO is responsive to our recommendation. Please provide by October 1, 2007, the OIG with a description of the reporting metrics and the methods for collecting the necessary information, printed screen views showing how the Archer Database has been modified to incorporate the reporting metrics, and a plan of action describing how DOJCERT will respond if the reporting metrics indicate that a component is failing to meet the required timeframes. If these actions are not completed by October 1, please provide the OIG with a status report at that time.

Recommendation 5. Promptly implement a Department-wide policy for notifying affected individuals in the event of a loss of personally identifiable information (PII).

Status. Resolved – open.

Summary of the Office of the CIO Response. The Office of the CIO concurred with this recommendation and stated that it was working with the Department's Privacy and Civil Liberties Office to develop a Data Breach Notification Policy. The Office of the CIO stated that it would issue the policy within 90 days.

OIG Analysis. The action proposed by the Office of the CIO is responsive to our recommendation. So that we may close this recommendation, please provide the OIG with a copy of the Department's Data Breach Notification Policy by October 1, 2007.

Recommendation 6. Develop a Department-specific definition of PII.

Status. Resolved – open.

Summary of the Office of the CIO Response. The Office of the CIO concurred with this recommendation, with reservations, stating that the Department's Chief Privacy and Civil Liberties Officer had asked OMB specifically if the Department could develop its own definition of PII in response to this recommendation. OMB expressed reservations about the Department's request. The Office of the CIO and the Department's Chief Privacy and Civil Liberties Officer will continue working with OMB on the issue.

OIG Analysis. The action proposed by the Office of the CIO is responsive to our recommendation. Please provide the OIG with either a Department-specific definition of PII or a status report on the discussions with OMB by October 1, 2007.

Recommendation 7. Consider whether any of the procedures described as "Best Practices" should be implemented across the Department.

Status. Resolved – closed.

Summary of the Office of the CIO Response. The Office of the CIO concurred with this recommendation and stated that it would review the "Best Practices" identified in this report, as well as "Best Practices" identified by other government agencies, and evaluate the feasibility of implementing them across the Department. The Office of the CIO anticipated being able to complete this evaluation within 90 days.

OIG Analysis. The action proposed by the Office of the CIO is responsive to our recommendation. This recommendation is closed.

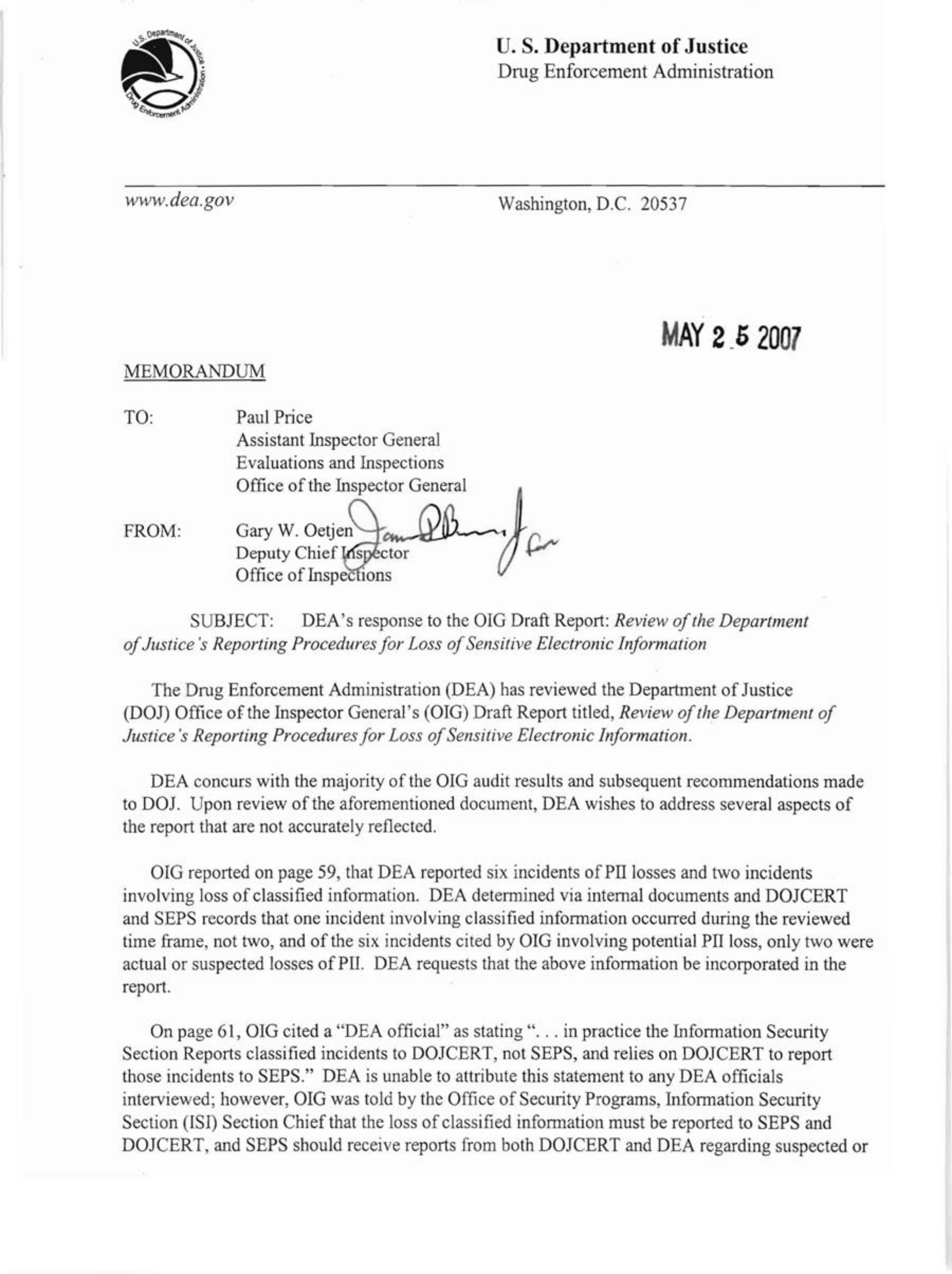
Recommendation 8. Ensure that components update their internal policies to reflect correct reporting procedures in conformance with the DOJCERT Incident Response Plan template and contain up-to-date titles of internal departments and staff.

Status. Resolved – open.

Summary of the Office of the CIO Response. The Office of the CIO concurred with this recommendation and stated that it would work with the components to ensure that the components' internal policies reflected correct procedures and current personnel. The Office of the CIO anticipated that it would complete this process within 120 days.

OIG Analysis. The action proposed by the Office of the CIO is responsive to our recommendation. So that we may close this recommendation, please provide the OIG with a certification from the Office of the CIO confirming that all components have updated their internal policies by October 1, 2007. If these actions are not completed by October 1, please provide the OIG with a status report at that time.

APPENDIX XV: DEA RESPONSE



U. S. Department of Justice
Drug Enforcement Administration

www.dea.gov

Washington, D.C. 20537

MAY 2 5 2007

MEMORANDUM

TO: Paul Price
Assistant Inspector General
Evaluations and Inspections
Office of the Inspector General

FROM: Gary W. Oetjen
Deputy Chief Inspector
Office of Inspections

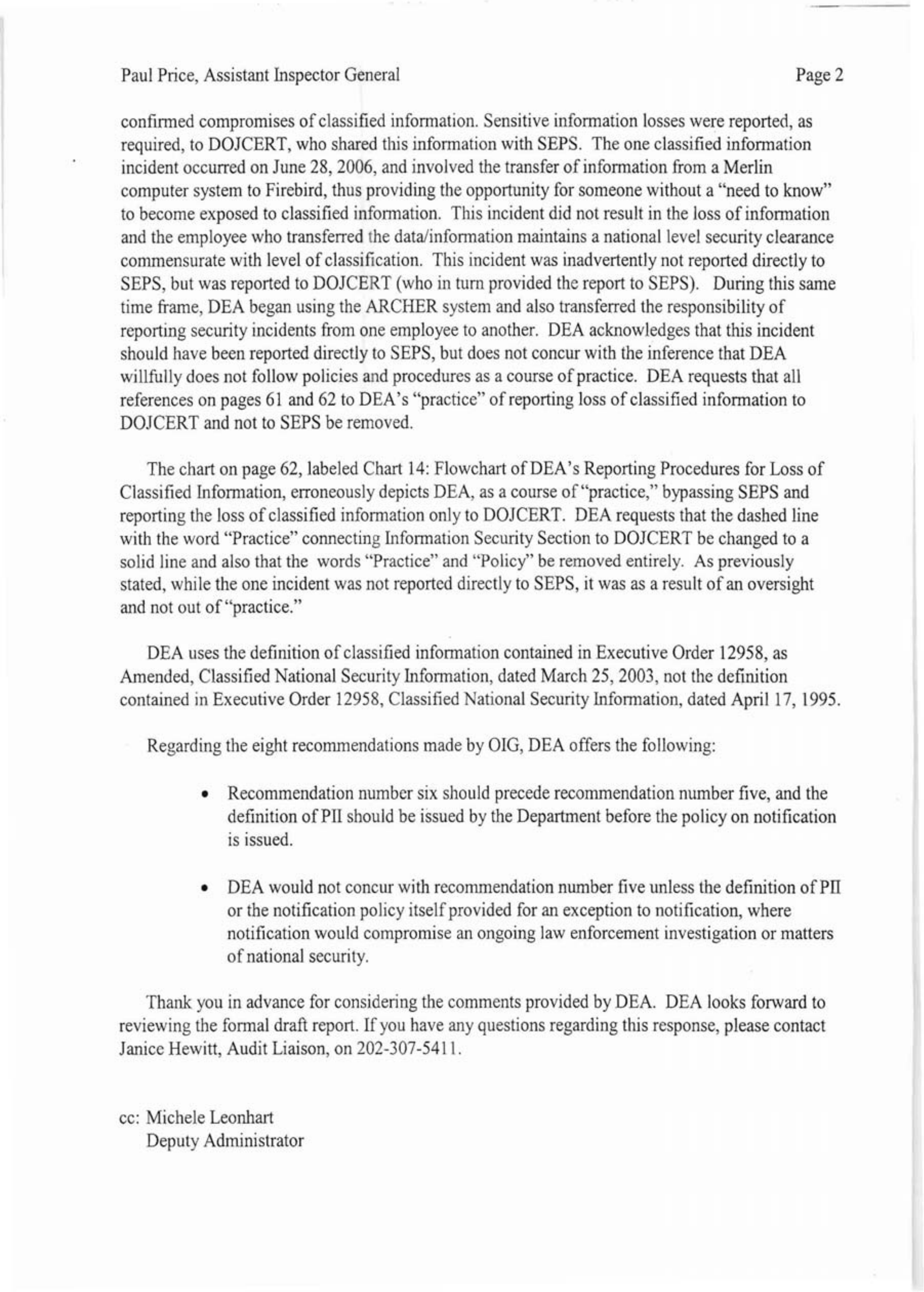
SUBJECT: DEA's response to the OIG Draft Report: *Review of the Department of Justice's Reporting Procedures for Loss of Sensitive Electronic Information*

The Drug Enforcement Administration (DEA) has reviewed the Department of Justice (DOJ) Office of the Inspector General's (OIG) Draft Report titled, *Review of the Department of Justice's Reporting Procedures for Loss of Sensitive Electronic Information*.

DEA concurs with the majority of the OIG audit results and subsequent recommendations made to DOJ. Upon review of the aforementioned document, DEA wishes to address several aspects of the report that are not accurately reflected.

OIG reported on page 59, that DEA reported six incidents of PII losses and two incidents involving loss of classified information. DEA determined via internal documents and DOJCERT and SEPS records that one incident involving classified information occurred during the reviewed time frame, not two, and of the six incidents cited by OIG involving potential PII loss, only two were actual or suspected losses of PII. DEA requests that the above information be incorporated in the report.

On page 61, OIG cited a "DEA official" as stating ". . . in practice the Information Security Section Reports classified incidents to DOJCERT, not SEPS, and relies on DOJCERT to report those incidents to SEPS." DEA is unable to attribute this statement to any DEA officials interviewed; however, OIG was told by the Office of Security Programs, Information Security Section (ISI) Section Chief that the loss of classified information must be reported to SEPS and DOJCERT, and SEPS should receive reports from both DOJCERT and DEA regarding suspected or



confirmed compromises of classified information. Sensitive information losses were reported, as required, to DOJCERT, who shared this information with SEPS. The one classified information incident occurred on June 28, 2006, and involved the transfer of information from a Merlin computer system to Firebird, thus providing the opportunity for someone without a "need to know" to become exposed to classified information. This incident did not result in the loss of information and the employee who transferred the data/information maintains a national level security clearance commensurate with level of classification. This incident was inadvertently not reported directly to SEPS, but was reported to DOJCERT (who in turn provided the report to SEPS). During this same time frame, DEA began using the ARCHER system and also transferred the responsibility of reporting security incidents from one employee to another. DEA acknowledges that this incident should have been reported directly to SEPS, but does not concur with the inference that DEA willfully does not follow policies and procedures as a course of practice. DEA requests that all references on pages 61 and 62 to DEA's "practice" of reporting loss of classified information to DOJCERT and not to SEPS be removed.

The chart on page 62, labeled Chart 14: Flowchart of DEA's Reporting Procedures for Loss of Classified Information, erroneously depicts DEA, as a course of "practice," bypassing SEPS and reporting the loss of classified information only to DOJCERT. DEA requests that the dashed line with the word "Practice" connecting Information Security Section to DOJCERT be changed to a solid line and also that the words "Practice" and "Policy" be removed entirely. As previously stated, while the one incident was not reported directly to SEPS, it was as a result of an oversight and not out of "practice."

DEA uses the definition of classified information contained in Executive Order 12958, as Amended, Classified National Security Information, dated March 25, 2003, not the definition contained in Executive Order 12958, Classified National Security Information, dated April 17, 1995.

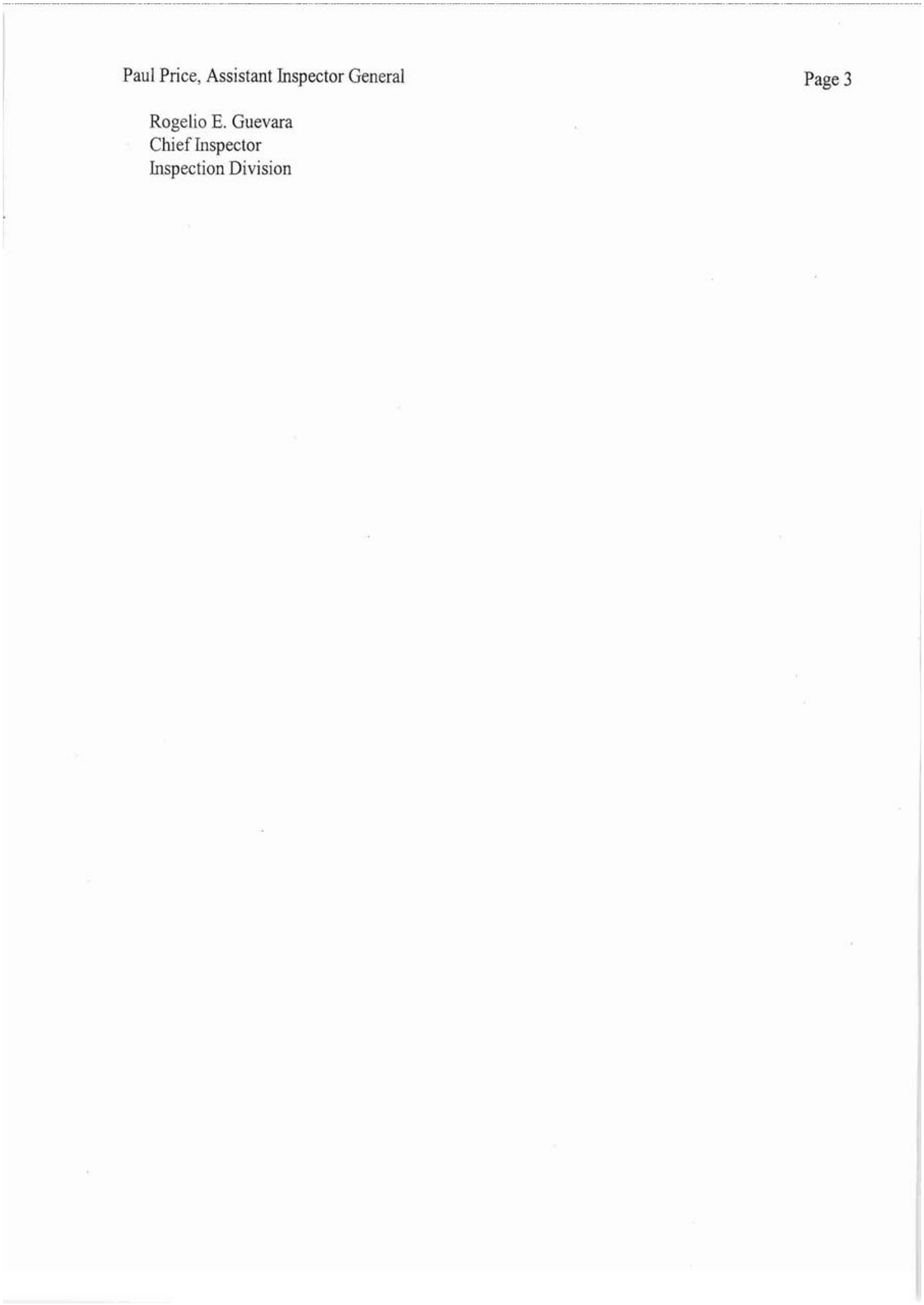
Regarding the eight recommendations made by OIG, DEA offers the following:

- Recommendation number six should precede recommendation number five, and the definition of PII should be issued by the Department before the policy on notification is issued.

- DEA would not concur with recommendation number five unless the definition of PII or the notification policy itself provided for an exception to notification, where notification would compromise an ongoing law enforcement investigation or matters of national security.

Thank you in advance for considering the comments provided by DEA. DEA looks forward to reviewing the formal draft report. If you have any questions regarding this response, please contact Janice Hewitt, Audit Liaison, on 202-307-5411.

cc: Michele Leonhart
Deputy Administrator



Paul Price, Assistant Inspector General Page 3

Rogelio E. Guevara
Chief Inspector
Inspection Division

APPENDIX XVI: OIG ANALYSIS OF THE DEA RESPONSE

In a memorandum dated May 25, 2007, the DEA responded to the OIG draft report. The DEA concurred with the majority of the OIG review results and the recommendations made to the Department. The DEA also provided comments on two technical and factual matters and made one comment on the report's recommendations.

Summary of DEA Response and OIG Analysis

Comment 1. The DEA stated that on page 58 of the report the OIG noted that there were six incidents of PII losses at the DEA and two incidents involving losses of classified information. According to the DEA, its internal documents and DOJCERT and SEPS records showed that only one incident involving classified information occurred during the review period. Further, of the six incidents cited by the OIG as involving potential PII loss, only two were actual or suspected losses of PII. The DEA requested that we incorporate these revisions into the report.

OIG Analysis. We declined to incorporate the DEA's suggested changes into the report. The numbers that the DEA cites are not reflected in the DOJCERT's Archer Database, which we used for each of the nine components reviewed in our analysis. To determine whether an incident involved actual or potential loss of PII, we relied on Archer Database records that showed whether components had responded "Yes" or "Unknown," respectively, when asked if an incident involved the loss of PII. To determine whether an incident potentially involved classified information, we relied on the incident descriptions in the database. In this review, we did not verify the database's information with either DOJCERT or the components' internal records. However, we added a footnote to the DEA appendix that includes the DEA's numbers and explains why the OIG's methodology may have produced different numbers.

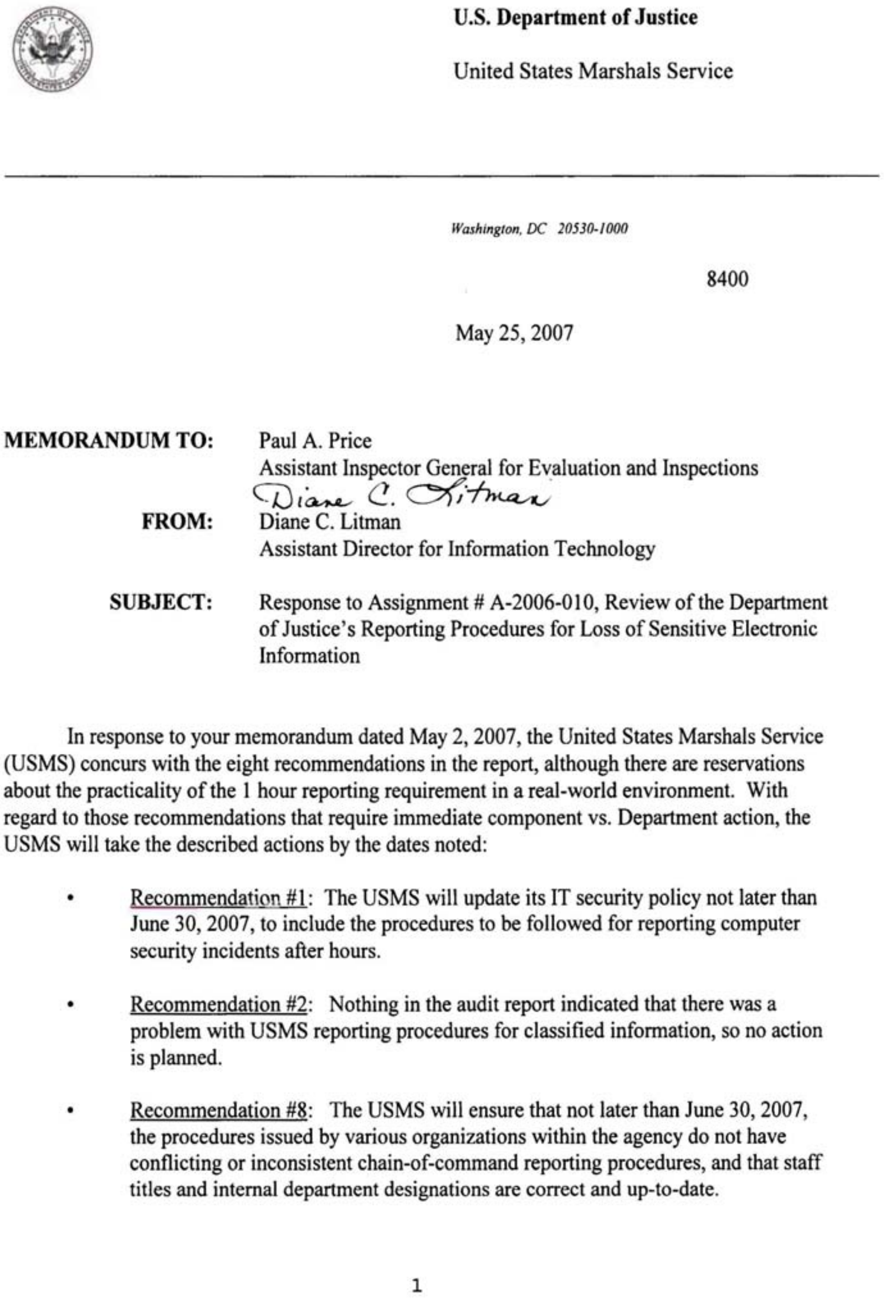
Comment 2. The DEA stated that the report cites a DEA official as stating that ". . . in practice the Information Security Section Reports classified incidents to DOJCERT, not SEPS, and relies on DOJCERT to report those incidents to SEPS." The DEA stated that it was unable to attribute this statement to any DEA official interviewed by the OIG. The DEA did acknowledge that its one classified incident was not directly reported to SEPS and should have been, but stated that it did not concur with the inference that it willfully failed to follow policies and procedures as a course of practice. Further, the DEA requested that all references to the DEA's "practice" of reporting loss of classified information to DOJCERT and not to SEPS be removed from the report.

OIG Analysis. Upon reviewing the notes of the original interview and a follow-up email sent to us by the subject of the interview, we found that his comments could be subject to varying interpretations. We revised the language on pages 60 and 61 of the report to clarify the meaning of the information he provided.

Comment 3. The DEA stated that it "would not concur with recommendation number five [of the report] unless the definition of PII or the notification policy itself provided for an exception to notification, where notification would compromise an ongoing law enforcement investigation or matters of national security."

OIG Analysis. The Department's Privacy and Civil Liberties Office is circulating a draft Department-wide notification policy that should address the DEA's concerns in this matter.

APPENDIX XVII: USMS RESPONSE



U.S. Department of Justice

United States Marshals Service

Washington, DC 20530-1000

8400

May 25, 2007

MEMORANDUM TO: Paul A. Price
Assistant Inspector General for Evaluation and Inspections

Diane C. Litman

FROM: Diane C. Litman
Assistant Director for Information Technology

SUBJECT: Response to Assignment # A-2006-010, Review of the Department of Justice's Reporting Procedures for Loss of Sensitive Electronic Information

In response to your memorandum dated May 2, 2007, the United States Marshals Service (USMS) concurs with the eight recommendations in the report, although there are reservations about the practicality of the 1 hour reporting requirement in a real-world environment. With regard to those recommendations that require immediate component vs. Department action, the USMS will take the described actions by the dates noted:

- Recommendation #1: The USMS will update its IT security policy not later than June 30, 2007, to include the procedures to be followed for reporting computer security incidents after hours.

- Recommendation #2: Nothing in the audit report indicated that there was a problem with USMS reporting procedures for classified information, so no action is planned.

- Recommendation #8: The USMS will ensure that not later than June 30, 2007, the procedures issued by various organizations within the agency do not have conflicting or inconsistent chain-of-command reporting procedures, and that staff titles and internal department designations are correct and up-to-date.

Questions concerning this response should be directed to Claire Adams on 202-307-9566.

cc: Kevin Deeley, DOJ OCIO, ITSS
Claire Adams, USMS, ITS
Alfred (Bud) Clark, USMS, ITS
Maria Alicia Ortiz, USMS, Audit Liaison

APPENDIX XVIII: OIG ANALYSIS OF THE USMS RESPONSE

In a memorandum dated May 25, 2007, the USMS responded to the OIG draft report. The USMS concurred with the eight recommendations in the report and provided a proposed action plan for those recommendations that required component versus Department action. The USMS stated that it would take the following actions by the noted dates for Recommendations 1, 2, and 8:

- Recommendation 1 – The USMS will update its information technology security policy no later than June 30, 2007, to include the procedures to be followed for reporting computer security incidents after hours.

- Recommendation 2 – Because nothing in the report indicated that there was a problem with USMS reporting procedures for classified information, the USMS stated it has no action planned.

- Recommendation 8 – The USMS will ensure that by no later than June 30, 2007, the procedures issued by various organizations within the agency do not have conflicting or inconsistent chain-of-command reporting procedures and that staff titles and internal department designations are correct.

While we appreciate the USMS response to the OIG recommendations, the Office of the CIO is coordinating the resolution process on behalf of the components for all recommendations. Therefore, we forwarded the USMS's response memorandum to the Office of the CIO.