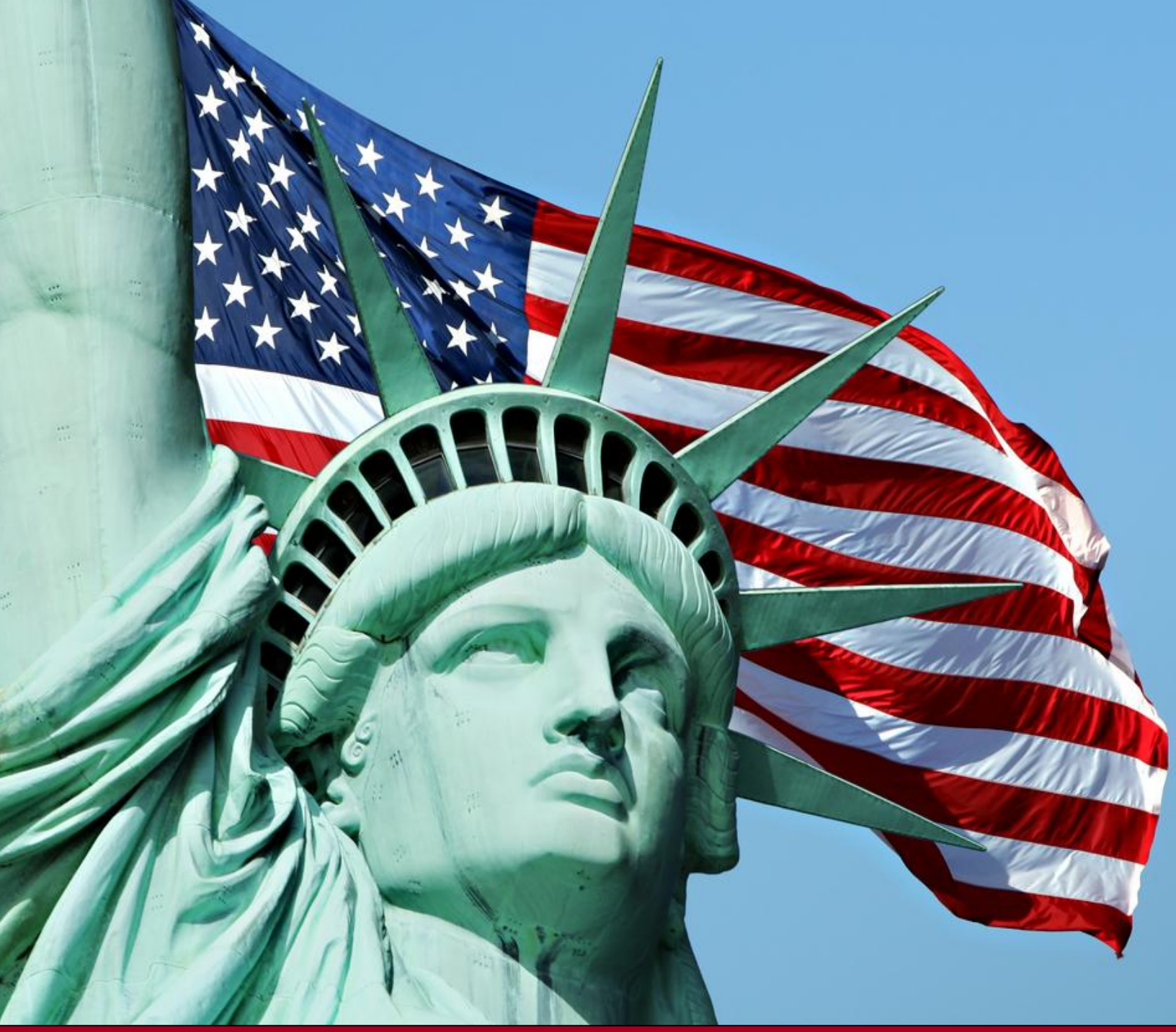

DHS Privacy Office

OIG Privacy Incident Report and Assessment

February 2011

Homeland Security

Executive Summary

The Chief Privacy Officer issues this report regarding a serious multi-Component Privacy Incident that occurred on March 30, 2010, involving the loss of DHS Financial Records Audit data. The financial audit data lost included Sensitive Personally Identifiable Information (PII) for records for the DHS Headquarters Management (DHSHQ), the United States Citizenship and Immigration Services (USCIS), and Immigration and Customs Enforcement (ICE) Components for Fiscal Year (FY) 2009.

In accordance with the Homeland Security Act of 2002, Section 222a (1) (as modified), the DHS Chief Privacy Officer is authorized to "make such investigations and reports relating to the administration of the programs and operations of the Department as are, in the senior official's judgment, necessary or desirable."[1] In addition, Section 222a (1) also states the Chief Privacy Officer must first refer any Privacy Incident to the Inspector General of the Department; if the OIG accepts the referral, the OIG investigates first.[2]

The OIG conducted an independent review of this Privacy Incident and submitted their report to the DHS Privacy Office. Because of the serious nature of the privacy policy and data security violations identified in the OIG report, the Chief Privacy Officer has prepared this report, including findings and recommendations, based on the facts and statements submitted by the OIG.

The DHS Privacy Office has identified potential and actual violations of federal acquisition regulations, federal privacy laws, Office of Management and Budget (OMB) Memoranda related to privacy, as well as DHS management directives and policies. The DHS Privacy Office has identified several privacy policy recommendations to avoid and ameliorate similar Privacy Incidents in the future. This report documents findings and provides recommendations to ensure consistent and ongoing privacy policy compliance and to prevent another occurrence of this type of incident.

[1] *See* 6 U.S.C. § 142(b)(1)(B).

[2] *Id.* at (c)(2).

Page intentionally left blank.

Table of Contents

Background

This background material was prepared by the Office of the Inspector General (OIG) as part of its investigation.[3] The DHS Privacy Office uses these facts as the basis of its privacy policy findings and recommendations.

SYNOPSIS

On March 30, 2010, KPMG LLP (KPMG), in the course of performing an annual financial statement audit as a contractor of the OIG, lost an unencrypted flash drive containing Personal Identifiable Information (PII)[4] from the Fiscal Year (FY) 2009 financial statement audit performed at Immigration and Customs Enforcement (ICE).

KPMG notified OIG in a timely manner of the loss, conducted its own internal investigation, provided documents and electronic copies of the data it believed was lost, and arranged for and funded credit monitoring services for affected individuals.

OIG interviewed KPMG employees involved in the use and loss of the flash drive and several Citizenship and Immigration Services (CIS) employees responsible for providing to the KPMG auditors with data believed to be on the flash drive. After review of documents and files that KPMG identified as likely being on the flash drive, OIG made notifications to about 350 affected individuals, offering credit monitoring services paid for by KPMG.

KPMG had numerous written policies to protect client data, as well as specific policies with respect to protecting privacy sensitive data, consistent with contract requirements. Additionally, KPMG employees involved in this incident had received prior privacy training, as required by the contract. However, compliance with the policies was not monitored or enforced by KPMG or the OIG, and the employees handling the lost flash drive did not follow them.

DETAILS

On April 1, 2010, KPMG notified the OIG that it had lost an unencrypted flash drive[5] containing information from the Fiscal Year (FY) 2009 financial statement audit performed at ICE. Because ICE provides financial services for other components, including Citizenship and Immigration Services (CIS), the Management Directorate, and the Science and Technology Directorate, information on the flash drive was not limited to ICE. The flash drive was last observed in an unlocked conference room in KPMG offices where it had been left at the end of the work day on Tuesday, March 30, by a team of KPMG auditors.

[3] OIG Report of Investigation, *Loss of Personally Identifiable Information by an Office of Inspector General Contractor*. The Synopsis and Details herein are taken verbatim from the report.

[4] DHS Privacy Office Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security defines PII as "…any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S. or employee or contractor to the Department."

[5] A flash drive is a data storage device integrated with a Universal Serial Bus interface. Flash drives are typically removable and rewritable. Flash drives are also known by trademark names such as ThumbDrive. http://dictionary.reference.com/browse/flash+drive.

It was reported that KPMG employees [Employee 1, Employee 2, Employee 3, Employee 4, and Employee 5] were in and out of the conference room during the week of March 28, 2010. Employee 1 realized the flash drive was missing around noon on March 31, 2010, when she determined that it was not where it was left in the conference room the previous day. The room was thoroughly searched for the missing flash drive without result. A notice was sent to KPMG management, and searching continued for days afterwards. Employees were also asked to search at home. The flash drive has not been recovered.

On the same day that OIG received notification of the incident from KPMG, OIG notified the DHS OneNet Security Operations Center (SOC)[6] of the missing flash drive, although OIG initially did not identify the incident as PII related. On April 2, 2010, the Chief Information Security Officer at ICE directed the SOC to transfer the incident response to ICE.

According to KPMG, they immediately began their own internal investigation, attempting to reconstruct what data may have been on the missing flash drive, and then reviewing the records to determine the extent of PII loss. On April 7, 2010, KPMG provided OIG with paper copies of files it believed to be on the flash drive and which contained Sensitive PII, including names, home addresses, social security numbers (SSNs), and bank account information of DHS employees.

On April 7, 2010, OIG reported to SOC that the flash drive might have contained PII. This was confirmed by an OIG SOC entry on April 13, 2010, which should have triggered a system generated notice to the Chief Privacy Officer about the incident. Neither of the entries on April 7 or April 13 triggered SOC's automatic notification of privacy incidents as discussed in section 5 of the DHS Privacy Incident Handling Guidance. The notification to privacy contacts was made by SOC staff on April 14, 2010.

After review of the documents provided by KPMG, OIG identified 93 individuals whose PII was included. By May 26, 2010, OIG completed notifications to all 93 affected individuals, providing information about credit monitoring services paid for by KPMG. Banks with customer account information on the lost flash drive for ten individuals were separately notified by CIS to be alert to unusual activity in those accounts. This bank notification was made by CIS in accordance with the DHS Privacy Incident Handling Guidance because the individuals whose bank account information was believed to be on the flash drive were CIS employees.

In June 2010, KPMG provided electronic copies of additional files that may have been contained on the lost flash drive. The OIG review of those files revealed an additional 250 names and SSNs related to individual background investigations performed by an ICE contractor. Sensitive information revealing bank routing and account numbers for numerous companies doing business with DHS was also discovered. By July 2010, notifications were made and credit monitoring was offered to all affected individuals. Companies were notified that their bank information was contained on the lost flash drive.

The Chief Financial Officers Act of 1990,[7] as amended (CFO Act) requires an annual audit of the financial statements of the department and authorizes the OIG to contract for the annual

[6] The SOC, now referred to as the Enterprise Operations Center (EOC), is a DHS entity created to track and report on data security incidents.

[7] Pub. L. No. 101-576, as amended Chief Financial Officers Act of 1990, http://www.cfoc.gov/documents/PL101-576.pdf.

audits. In the course of performing the annual financial statement audits, the contractor handles Sensitive PII provided to it by the department. The contractor is required to protect this information according to departmental policies and procedures. KPMG was the incumbent contractor performing the audit services. In the course of performing the annual financial statement audits, KPMG handles Sensitive PII, as well as other types of sensitive information.

DHS Privacy Office Investigation

The DHS Privacy Office independently reviewed the March 30 Privacy Incident. In addition to relying on the OIG's report for factual matters, the Director of Privacy Incidents and Inquiries reviewed all available documentation provided by the OIG and conducted interviews with the individuals involved. The DHS Privacy Office used this information to make findings and recommendations associated with the loss of the KPMG unencrypted flash drive.

I. Laws, Directives, Policies, and Guidance Implicated by the Privacy Incident

This section identifies relevant laws, federal directives, policies and guidance (whether federal, OMB, or DHS) that resulted in, and/or were related to, the March 30, 2010, data breach and subsequent Privacy Incident. The findings and recommendations related to non-compliance with these authorities are summarized in Sections II and III below.

A. Federal Regulations and Federal Contract Clauses

1. Privacy Act of 1974[8]

The Privacy Act of 1974 provides, in part, that, "[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to who the record pertains, unless disclosure of the record would be…to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable."[9]

The Privacy Act further provides that, "[e]ach agency that maintains a system of records shall…maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President."[10]

2. E-Government Act of 2002[11]

The E-Government Act of 2002 enhances the management and promotion of electronic Government services and processes by establishing a federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to government information and services.

a. Title III of the E-Government Act (Federal Information Security Management Act of 2002)

This subchapter provides, among other requirements, a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets, and the

[8] 5 U.S.C. § 552a.

[9] 5 U.S.C § 552a(b)(5).

[10] 5 U.S.C. § 552a(e)(1).

[11] Pub. L. No. 107-347, 116 Stat. 2899.

development and maintenance of minimum controls required to protect Federal information and information systems.

Federal Information Security Management Act (FISMA) further tasked the National Institute of Standards and Technology (NIST) with the responsibility of developing security standards and guidelines for the federal government. Based upon this requirement, NIST developed the following:

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*. Requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability.[12]
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems.* Specifies minimum security requirements for information and information systems supporting the executive agencies of the federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements.[13]
- Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations.* Provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government to meet the requirements of FIPS 200. The guidelines apply to all Components of an information system that process, store, or transmit federal information.[14]

3. Federal Acquisition Regulation (FAR),[15] Part 42 – Contract Administration and Audit Services, Subpart 42.11, Production and Surveillance Reporting

The Federal Acquisition Regulation (FAR) details the duties required for maintaining oversight and surveillance of contractors' performance. All surveillance assignments of contract oversight personnel must be made in writing.

The FAR states, "[p]roduction surveillance is a function of contract administration used to determine contractor progress and to identify any factors that may delay performance. Production surveillance involves Government review and analysis of—(a) Contractor performance plans, schedules, controls, and industrial processes; and

[12] http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[13] http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

[14] http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

[15] https://www.acquisition.gov/far/current/html/FARTOCP42.html.

(b) The contractor's actual performance under them."

4. FAR, Part 52.224-2 – Privacy Act[16]

As prescribed in 24.104, insert the following clause in solicitations and contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function:

(a) The Contractor agrees to—

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function.

5. General Services Administration (GSA) Federal Acquisition Regulation (FAR) Clause 1052.201.70 Contracting Officer's Technical Representative (COTR) Appointment and Authority (APR 2004) (Deviation) (DTAR)[17]

The General Services Administration (GSA) FAR Clause states, "[t]he Contracting Officer (CO) designates the COTR and any alternate COTR(s) in writing. This designation can only be accomplished in writing and cannot be delegated without written approval and a list of COTR duties being issued by the CO."

B. Office of Management and Budget (OMB) Memoranda

1. OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*[18]

Provides a checklist based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 outlining specific actions (controls) to be taken by federal agencies for the protection of Personally Identifiable Information (PII) categorized in accordance with FIPS 199 as moderate or high impact that is either: (1) accessed remotely; or (2) physically transported outside of the agency's secured, physical perimeter (this includes information transported on removable media and on portable/mobile devices such as laptop computers and/or personal digital assistants).

2. OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*[19]

[16] https://www.acquisition.gov/far/current/html/52_223_226.html#wp1168981.

[17] FAR Clause 1052.201.70 *Contracting Officer's Technical Representative Appointment and Authority* is not available via an external link.

[18] http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m06-16.pdf.

This memorandum provides updated guidance on the reporting of security incidents involving personally identifiable information and reminds agencies of existing requirements, and explain new requirements agencies will need to provide addressing security and privacy in budget submissions for information technology.

3. OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*[20]

This memorandum requires agencies to develop a breach notification policy while ensuring proper safeguards are in place to protect the information in both paper and electronic form. Specifically, OMB M-07-16 requires agencies to develop policies and procedures for reporting and mitigating PII incidents and notification of incidents to the United States Computer Emergency Readiness Team (US-CERT)[21] within one hour of discovery.

C. DHS Privacy Directives, Policies and Guidance

1. DHS Management Directive Number 0470.2 *Privacy Act Compliance*[22]

Privacy Act compliance is established through DHS Management Directive Number 0470.2 *Privacy Act Compliance*.

Page 1 of the Directive contains the following information:

> "This MD applies to all DHS Components, with the exception of the Office of Inspector General (OIG). However, the DHS OIG complies with all statutory requirements."

2. Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS[23]

The Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS provides minimum standards for how DHS employees, contractors, detailees, and consultants should handle Sensitive PII in paper and electronic form during their

[19] http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m06-19.pdf.

[20] http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-16.pdf.

[21] US-CERT serves as the designated central reporting organization within the federal government and the central repository for federal incident data.

[22] http://www.dhs.gov/xlibrary/assets/foia/mgmt-directive-0470-2-privacy-act-compliance.pdf.

[23] http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_spii_handbook.pdf.

everyday work activities at the Department.[24] The Handbook explains, among other items, how to identify Sensitive PII, how to protect Sensitive PII in different contexts and formats, and what to do if you believe Sensitive PII may have been compromised.

The Handbook also includes definitions for PII and Sensitive PII and details the responsibilities required to protect information that has been entrusted to DHS.

Among other instructions, the Handbook instructs those entrusted with Sensitive PII not to take Sensitive PII to any non-DHS approved worksite in paper or electronic form unless properly secured. Proper security includes the use of encryption.[25] It also instructs those in possession of Sensitive PII to physically secure Sensitive PII, either in a locked drawer, safe, or other lockable format when not in use and/or when not under the control of a person with a need to know.

3. DHS Privacy Incident Handling Guidance, September 2007[26]

The DHS Privacy Incident Handling Guidance establishes governing policies and procedures for Privacy Incident handling at DHS. The policies and procedures are based on applicable laws, Presidential Directives, and Office of Management and Budget (OMB) directives.[27] The DHS Privacy Incident Handling Guidance informs DHS organizations, employees, senior officials, and contractors of their obligation to protect PII and establishes procedures delineating how they must respond to the potential loss or compromise of PII.

In accordance with applicable laws, Presidential directives, and OMB directives, the DHS Privacy Incident Handling Guidance requires any Component discovering a suspected or confirmed Privacy Incident to coordinate with the Component Privacy Officer or Privacy Point of Contact (PPOC) and Component Information Security Officer (CISO)/Information Systems Security Manager to evaluate and subsequently report the incident to the DHS Enterprise Operations Center (EOC) immediately upon discovery and in no event later than one hour after discovery.

4. DHS Privacy Policy Guidance Memorandum 2007-02, *Use of Social Security Numbers at the Department of Homeland Security*, June 4, 2007[28]

[24] As required by OMB M-07-16, these rules also apply to DHS licensees, certificate holders, and grantees who handle or collect PII, including Sensitive PII, for or on behalf of DHS.

[25] Appendix A to the Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS provides instructions on encrypting files.

[26] http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_Privacy Incident Handling Guidance.pdf.

[27] OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006, (OMB M-06-19), and OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007 (OMB M-07-16) outline specific requirements for agencies to follow when reporting Privacy Incidents.

[28] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-2.pdf.

DHS Privacy Policy Guidance Memorandum 2007-02 *Use of Social Security Numbers at the Department of Homeland Security* provides guidance regarding the use of SSNs at the Department of Homeland Security. Specifically, this memorandum requires that DHS programs not collect or use a SSN as a unique identifier unless required by statute, regulation, or when pursuant to a specific authorized purpose.[29] This guidance further requires specific security controls be implemented in order to mitigate the risk of inappropriate or unauthorized disclosure, including, but not limited to encryption, restricting access, and implementing audit logs to track access to the SSN. The guidance also outlines for programs proper destruction of paper containing SSNs as well as retention requirements.

5. DHS Privacy Policy Guidance Memorandum 2008-01, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, December 29, 2008[30]

DHS Privacy Policy Guidance Memorandum 2008-01 articulates the Fair Information Practice Principles (FIPPs) as the foundation for the Department's privacy policy. This memorandum states that the FIPPs must be considered whenever a DHS program or activity raises privacy concerns or involves the collection of personally identifiable information from individuals, regardless of their status. Appendix A contains the text of the DHS FIPPs.

These principles and their applicability to this incident are discussed throughout this report.

D. DHS Security Directives, Policies, and Guidance

1. DHS Sensitive Systems Policy Directive 4300A and Handbook[31]

The DHS Sensitive Systems Policy Directive 4300A (DHS Directive 4300A) is the official series of publications relating to Departmental standards and guidelines adopted and promulgated under the provisions of DHS Management Directive 140-01 *Information Technology Systems Security*.[32]

DHS Directive 4300A articulates the Department's Information Security Program policies for sensitive systems. Procedures for implementing these policies are outlined in a companion publication, *DHS 4300A Sensitive Systems Handbook* (DHS 4300A Handbook). The handbook serves as a foundation for Components to develop

[29] This report assumes that the data that was on the lost flash drive was initially collected, used, and retained pursuant to an authorized purpose.

[30] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[31] DHS Directive 4300A is not available via an external link.

[32] http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_140-01_information_technology_systems_security.pdf

and implement their information security programs. The baseline security requirements (BLSRs) included in the handbook must be addressed when developing and maintaining information security documents.

The DHS Information Security Program provides a baseline of policies, standards, and guidelines for DHS Components. DHS Directive 4300A provides direction to managers and senior executives for managing and protecting sensitive systems. It also outlines policies relating to management, operational, and technical controls necessary for ensuring confidentiality, integrity, availability, authenticity, and non-repudiation within the DHS information system infrastructure and operations.

DHS Directive 4300A and the DHS 4300A Handbook implement requirements outlined in statutes and guidance including, but not limited to Public Law 107-347, E-Government Act of 2002, including Title III, FISMA, Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, NIST Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, and NIST SP 800-53, *Recommended Security Controls for Federal Information Systems.*

2. DHS Management Directive 4900, Individual Use and Operation of DHS Information Systems/Computers and Appendix A, Information Systems/Computer Access Agreement[33]

This Directive establishes the DHS policy for the use and operation of DHS information systems and computers by individual users.

This Directive applies to all individual users of DHS-owned or provided information systems, including personal and desktop computers. This document provides the minimum DHS level of information systems/computer security requirements.

All DHS individual users of DHS information systems are responsible for complying with the requirements of DHS Management Directive 4900 including:

Training: All users will complete a government approved security training course prior to being given access to government information systems. This training course must address the security aspects unique to the particular system as well as the functionality of desktop hardware and standard suite of software applications.

Computer Access Agreements: (Appendix A to DHS Management Directive 4900) All users must read, sign and provide to their IT Support organization, a user agreement prior to being granted access to DHS systems. The document delineates the user's specific responsibilities and duties of individual users.

The Computer Access Agreement is a written agreement from all personnel signifying understanding and acceptance of applicable policy and legal requirements concerning the use and operation of information systems and access to network resources within the DHS. This policy applies to all staff, interns, volunteers,

[33] http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4900_individual_use_and_operation_of_dhs_information_systems_computers.pdf

partners, and contractors assigned or detailed to DHS and obligates to user to comply with specific responsibilities and duties including data protection.

Protection of Data: Users will protect storage magnetic media in accordance with the highest level of data sensitivity contained. Whenever possible, stored data will be encrypted on removable media and in portable devices when not in government facilities.

3. DHS Management Directive 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information

This Directive establishes DHS policy regarding the identification and safeguarding of sensitive but unclassified (SBU) information originating within DHS. It also applies to other sensitive but unclassified information received by DHS from other government and non-government activities. Sensitive PII is considered SBU information and, as such, requires the necessary controls for proper protection.

This Directive is applicable to all DHS Headquarters, Components, organizational elements, detailees, contractors, consultants, and others to whom access to information covered by this Directive is granted.

This Directive requires employees and contractors (among others) to comply with safeguarding requirements for SBU information including, but not limited to, applying the necessary controls to SBU designated information in order to afford appropriate protection. This Directive also requires contractors to participate in formal classroom or computer based training sessions that outline the requirements for safeguarding and destroying For Official Use Only (FOUO) and other SBU designated information. These trainings put contractors on notice that divulging information without proper authority could result in administrative or disciplinary action.

Finally, DHS Management Directive 11042.1 requires contractors to execute DHS Form 11000-6 Sensitive But Unclassified Information Non-Disclosure Agreement (NDA), as a condition of access to such information.

E. KPMG Policies

While Department employees are not subject to KPMG's policies, they are relevant to the actions of KPMG's employees. They are included in an effort to provide a complete understanding of the privacy framework, but have not been integrated into the findings and recommendations given they are not federal requirements.

1. KPMG's Code of Conduct

Every KPMG employee regardless of title or position within the firm must confirm in writing annually that he or she has read KPMG's Code of Conduct, and understands and agrees to adhere to it. The code specifically requires KPMG employees to ensure that laptops are encrypted and to use only approved data transfer and storage devices. Employees are cautioned against sharing electronic storage devices containing confidential information and downloading confidential or private information onto

temporary storage devices (such as flash drives) that may not contain encryption software. In addition, the code requires employees to review information received to determine if it is privacy sensitive and only gather the minimum amount of information necessary to meet legitimate business purposes. Employees are warned to be alert to leaving data storage devices or documents in non-secure locations, even temporarily, and cautioned against storing or transferring unencrypted files containing confidential or private information.

2. KPMG Audit Instructions

KPMG Audit Instructions provided to each KPMG Audit Team member require:

> Every KPMG employee regardless of title or position within the firm must confirm in writing annually that he or she has read KPMG's Code of Conduct, and understands and agrees to adhere to it as noted above.

In addition, all KPMG partners, managers, and senior associates working on the DHS audit are required to read and acknowledge detailed instructions specific to DHS. The following security related instructions are included:

> All team members must protect and maintain confidentiality of all documents, data, and other information supplied to [KPMG] by DHS, in accordance with all applicable federal guidelines, regulations, and internal DHS/DHS component policies.
>
> Each engagement team must obtain direction from the component in which audit work is performed to identify SBU information and to ensure each components' [sic] established policies and procedures for handling such information are adhered to [sic].
>
> Do not store any personally identifiable information on KPMG computers. If PII is required to complete the audit, it must be approved by the component engagement partner prior to being put on any computer.

KPMG's instructions outline certain steps to be taken by the audit team to ensure KPMG compliance with the Privacy Act including: 1) do not remove records about individuals from DHS; 2) do not store any PII on KPMG computers; 3) dispose of PII appropriately-use burn bags and erase electronic records; 4) at the end of the engagement, complete a computer purge; 5) scan computers used in previous years to ensure that PII has been removed; and 6) keep the use of SSNs to an absolute minimum. KPMG notes that it does not anticipate requiring PII for the audit and that the Component engagement partner is to be notified before any requests for PII are made to DHS.

According to the audit instructions, "[i]t is each person's responsibility to diligently work through his/her own laptop and other records to ensure compliance..." with the computer purge policy. The instructions list numerous applications and folders that need to be checked, including flash drives which the instructions provide are not acceptable for storing client files unless stored on client premises as the official audit record.

The audit instructions address external storage devices (i.e., flash drives, CDs, etc) specifically. They state, "[i]t is not acceptable under the Risk Management Manual policy to simply move files from your laptop to an external device in order to retain files-unless that device is stored securely on client premises as the official audit record. Check your flash drives and other storage devices for any files you might have saved to it during the year for file sharing purposes."

3. KPMG Administrative Releases

During the course of this audit, KPMG issued supplements to the audit instructions referred to as administrative releases (ARs) to emphasize or clarify rules and procedures. During the FY 2009 audit, KPMG issued several ARs related to protecting client data. KPMG's AR 09-01, issued April 2, 2009, required each Component audit team to meet with the Component's IT security staff during the audit planning phase to obtain IT security policies and procedures.

KPMG's AR 09-06, issued July 1, 2009, directs audit teams to review information received from the Components specifically for PII and other sensitive information before transferring it to KPMG computers. This release also reminds the auditors to follow KPMG's data confidentiality and computer purge policies found in the annual audit instructions.

KPMG's AR 09-08, issued August 26, 2009, is a reminder about handling and storing electronic files. This AR reminds the KPMG auditors that they are required to comply with all laws, regulations, guidelines, and DHS policies for handling, storing, and safeguarding DHS information. It also reminds the auditors that, "[p]ersonal computers and personal email accounts (e.g. Gmail, yahoo, hotmail, etc.) should **never** [emphasis in original] be used to transmit, receive, store, or work on DHS-related work." The AR cautions that use of external storage devices, such as flash drives, is generally not acceptable unless the device is stored securely on client premises as the official audit record. Of note, the AR does not address encryption of external devices. Finally, the AR instructs that, when auditors use an external storage device to transfer large files from one computer to another, the auditors must immediately erase the data from the external drive when the transfer is finished.

In addition, KPMG employees may review information about the firm's information security policies on its internal website and in other internal communications vehicles such as its newsletter, KPMGToday.

II. Findings Related to March 30, 2010 Privacy Incident

This section details the findings associated with non-compliance with the privacy framework identified in Section I above.

A. KPMG Actions

The OIG investigation into the Privacy Incident revealed that KPMG auditors had insufficient understanding of applicable OMB and DHS directives. This lack of understanding was the reason that KPMG auditors used the flash drive for unauthorized purposes and failed to properly secure it electronically and physically.

Finding A.1: Non-compliance with OMB Memorandum M-06-16, DHS Policy Directive 4300A, and FIPS 200 occurred when the KPMG audit team used the flash drive to store and share documents. It also occurred when the KPMG audit team lost the flash drive. The OIG contract requires KPMG to comply with "[a]ll laws, regulations, federal guidelines, and internal DHS/DHS Component policies regarding the handling, storage, and safeguarding of DHS information." KPMG did not comply with these authorities when it used, and subsequently lost, the flash drive. KPMG did not use a DHS-approved and encrypted flash drive or have appropriate controls securing the sensitive information. Specifically, KPMG employees did not comply with the following OMB memoranda, DHS directives, and FIPS 200:

- **OMB Memorandum M-06-16** ***Protection of Sensitive Agency Information*** which requires compliance with NIST SP 800-53 security controls for sensitive agency information in those instances where personally identifiable information is transported to a remote site. NIST Special Publication 800-53 requires the use of security controls ensuring that information is transported only in encrypted form.
- **DHS Policy Directive 4300A, Policy I.D. 3.14.5.a** requires PII and Sensitive PII removed from a DHS facility on removable media, such as CDs, DVDs, laptops, PDAs, shall be encrypted, unless the information is being sent to the individual as part of a Privacy Act or Freedom of Information Act (FOIA) request.
- **DHS Policy Directive 4300A, Policy ID 4.3.1.c** prohibits DHS personnel, contractors, and others working on behalf of DHS from using any non-Government issued removable media (USB drives, in particular) or connecting them to DHS equipment or networks or to store DHS sensitive information.
- **DHS Policy Directive 4300A, Policy ID 4.8.2.a** requires information stored on any laptop computer or other mobile computing device that may be used in a residence or on travel shall use encryption in accordance with Section 5.5.1, Encryption.
- **FIPS 200** states, "…organizations must develop and promulgate formal, documented policies and procedures governing the minimum security requirements set forth in this standard and must ensure their effective implementation."

Finding A.2: As part of the contract terms, KPMG employees executed Computer Access Agreements and thereby agreed to comply with all the requirements outlined in DHS Management Directive 4900, including training and data protection. The events that led up to the data breach and Privacy Incident indicate that the KPMG employees did not understand or appreciate and subsequently disregarded the significance of these requirements. The KPMG employees used an unencrypted flash drive to store Sensitive PII in contradiction with DHS Management Directive 4900 and the Computer Access Agreement.

KPMG employees failed to comply with DHS Management Directive 11042.1 and the executed DHS Form 11000-6, which these employees signed. By signing this form, they agreed to protect the data properly, including at a minimum, storing the information on a DHS-approved encrypted flash drive and properly cleaning the flash drive of information no longer required in the performance of the contract.

- **DHS Management Directive 4900** states, "[u]sers will protect storage magnetic media in accordance with the highest level of data sensitivity contained. Whenever possible, stored data will be encrypted on removable media and in portable devices when not in Government facilities."
- **DHS Office of Inspector General Computer Access Agreement Section 4, Privacy & OIG Data Protection** states that the signer, "…will protect displayed, stored, data, magnetic media, and printouts in accordance with the highest level of data sensitivity contained on the media…. [and] will follow OIG policy for transmitting sensitive data… by utilizing WinZip or other OIG standard encryption software."
- **DHS Office of Inspector General Computer Access Agreement Section 4, Privacy & OIG Data Protection** states that the signer, "…will use only DHS IT equipment to access DHS & OIG systems and information…. [and] will not install any personally owned hardware (printers, flash/thumb drives, wireless cards, etc)…."
- **DHS Management Directive 11042.1** states that DHS contractors must, "[b]e aware of and comply with the safeguarding requirements for FOUO information as outlined in this directive."

1. KPMG Audit Instructions to Audit Team Members

Finding A.1.1: KPMG employees did not comply with the Audit Instructions, Section 7.9, (and possibly KPMG's Code of Conduct) when several employees used the flash drive to share confidential and private information.

- **The KPMG U.S. Department of Homeland Security Integrated Audit Instructions September 30, 2009 Section 7.9** states, "[i]t is not acceptable under the Risk Management Manual policy to simply move files from your laptop to an external device in order to retain files – unless that device is stored securely on

client premises as the official audit record. Check your flash drives and other storage devices for any files you might have saved to it during the year for file-sharing purposes."

Finding A.1.2: KPMG's Code of Conduct advised KPMG employees to review information received to determine if it was privacy sensitive and only gather the minimum amount needed for business purposes. KPMG failed to follow DHS Privacy Policy Guidance Memorandum 2008-01 and the FIPP of Data Minimization.

- **DHS Privacy Policy Guidance Memorandum 2008-01** states, "DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfil the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA)."

Finding A.1.3: Non-compliance with DHS Management Directive 0470.2 and thus the Privacy Act occurred when KPMG misplaced a non-encrypted flash drive containing PII. Given that the flash drive was unencrypted and did not contain any access security controls, the PII contained on the flash drive may have been exposed or made available to third parties without the individuals' prior written consent.

- **DHS Management Directive 0470.2** states, "[b]y virtue of the Inspector General Act of 1978, the DHS OIG may be exempt from compliance with DHS policies, directives, instructions, guidance, etc. However, the DHS OIG complies with all statutory requirements."
- **The Privacy Act of 1974** states that, "[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to who the record pertains, unless disclosure of the record would be…to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable."
- **FIPS 200** states "[o]rganizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse."

Finding A.1.4: The practice of sharing flash drives among KPMG employees hindered the OIG's ability to comply with the Privacy Incident Handling Guidance including beginning immediate mitigation. The investigation revealed that although the audit team initially used the flash drives for file transfers, it appears that KPMG did not erase the drives, and deleted files infrequently and without documentation. This factor made it difficult for KPMG to determine exactly what data was on the flash drive at the time of its loss.

- **DHS Policy Directive 4300A Section 4.3** states, "[s]torage media that contain sensitive information must be controlled so that the information is protected."

2. KPMG Management

Finding A.2.1: The KPMG manager did not comply with DHS security directives. Non-compliance with DHS Management Directive 11042.1 occurred when the KPMG manager failed to properly review, identify, and safeguard the SBU information in its possession. The manager reviewed work papers, but not the supporting documentation where the sensitive information was frequently found in this case. Non-compliance with DHS Privacy Policy Guidance Memorandum 2007-02 and DHS Privacy Policy Guidance Memorandum 2008-01 occurred when the KPMG manager failed to ensure SSNs and other Sensitive PII were protected and required for the audit.

- **DHS Management Directive 11042.1** states that DHS contractors must, "[b]e aware of and comply with the safeguarding requirements for FOUO information as outlined in this directive."
- **DHS Privacy Policy Guidance Memorandum 2007-02** states, "[s]ufficient security controls must be implemented in order to mitigate the risk of inappropriate or unauthorized disclosure of data containing SSN. Any access to SSNs shall be restricted with an appropriate application of security controls. Any program collecting, using, maintaining, and/or disseminating SSNs must maintain audit logs tracking the access to the SSNs, and the program must perform periodic reviews of these audit logs." It continues, "Encryption, the application of which is encouraged, will minimize the risk of unauthorized disclosure. Other security controls, such as password protection may also mitigate the risk associated with authorized disclosure. The appropriate controls will be determined by the program in coordination with the Privacy Office, Chief Information Officer, the component Privacy Officer, and the Information System Security Manager (ISSM)."
- **DHS Privacy Policy Guidance Memorandum 2008-01** includes a Security FIPP which states, "DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure."

Finding A.2.2: During the course of this audit, KPMG provided appropriate guidance and tools for the KPMG audit teams through the issuance of the administrative releases (ARs), supplements to the audit instructions to emphasize or clarify rules and procedures. Despite specific reminders to protect client information through KPMG's AR 09-06, KPMG's AR 09-08 and Audit Instructions, Section 7.3, Confidentiality of Data, Classified and Sensitive Information, KPMG employees failed to review information received from the Components specifically for PII and other sensitive information before transferring to KPMG computers. The employees

also failed to follow computer purge policies as specified in KPMG's AR 09-08 and Audit Instructions, Section 7.9, Computer Purge Guidance.

- **The KPMG U.S. Department of Homeland Security Integrated Audit Instructions September 30, 2009 Section 7.3** states, "[w]e [KPMG] need to ensure that we treat personally identifiable information (PII) respectfully and in compliance with the requirements of the Privacy Act and other applicable statutory privacy requirements."
- **FIPS 200** states, "[o]rganizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities."

B. OIG Office of Audits Actions

The OIG Office of Audits conducts and coordinates audits and program evaluations of the management and financial operations of DHS. As part of its duties, the Chief Financial Officers Act of 1990[34] (CFO Act) requires the OIG to audit the financial statements of the Department annually. The CFO Act authorizes the OIG to contract with an independent public accountant to perform the annual audits. The OIG, through an interagency agreement with the Department of Treasury's Bureau of Public Debt, contracts with KPMG to perform the annual audits of DHS' financial statements. Employees in the OIG Office of Audits serve as COTRs to manage the contract.

1. OIG Office of Audits FAR Clause Requirements

Finding B.1.1: The Department of Treasury's Bureau of Debt contracting officer designated in writing specific individuals in the OIG Office of Audits to serve as the primary and alternate COTRs on the contract with KPMG. According to GSA Optional FAR clause 1052.210-70, a government agency cannot delegate these responsibilities under any circumstances without a contractual modification. The COTR responsibilities were not appropriately maintained by the OIG Office of Audits.

- **GSA Optional FAR clause 1052.210-70** states, "…the Contracting Officer (CO) designates the COTR and any alternate COTR(s) in writing. This designation can only be accomplished in writing and cannot be delegated without written approval and a list of COTR duties being issued by the CO."

[34] Pub. L. No. 101-576, as amended Chief Financial Officers Act of 1990, http://www.cfoc.gov/documents/PL101-576.pdf.

Finding B.1.2: The OIG Office of Audits failed to comply with DHS Directive 4300A, which requires Components to conduct reviews of their contractors to ensure they implement and enforce information security requirements.

- **DHS Policy Directive 4300A, Policy I.D. 3.3.e** requires Components to conduct reviews to ensure that the information security requirements are included within the contract language and are implemented and enforced.
- **DHS Office of Inspector General Performance Work Statement dated 16 October 2009 Section 1.5** states, "[t]he OIG…reserves[s] the right to conduct onsite visits to review the Contractor's documentation and in-house procedures for protection of information."
- **FIPS 200** states "[o]rganizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse."

Finding B.1.3: The OIG Office of Audits failed to audit the contractor to monitor the actual use of PII. It also failed to ensure that KPMG followed the FIPPs outlined in DHS Privacy Policy Guidance Memorandum 2008-01.

- **DHS Privacy Policy Guidance Memorandum 2008-01** states, "DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements."

Finding B.1.4: The Department of Homeland Security, Office of Inspector General, Performance Work Statement (PWS), dated 16 October 2009, Section 1.5 "Information Security and Confidentiality," requires the OIG Office of Audits to maintain sufficient oversight of contractor personnel. The OIG Office of Audits did not enforce or maintain this oversight. At no time during the investigation was there evidence that the OIG Office of Audits coordinated or verified Component or KPMG compliance with the above statement.

- **DHS Office of Inspector General Performance Work Statement dated 16 October 2009 Section 1.5** states, "[t]he OIG…reserve[s] the right to conduct onsite visits to review the Contractors documentation and in-house procedures for protection of information."

Finding B.1.5: The OIG Office of Audits failed to ensure KPMG employees complied with DHS Management Directive 4900 regarding data protection and the use of flash drives. Section 4, Privacy & OIG Data Protection of the Computer Access Agreement specifically addresses data protection and further refers to the OIG policy for transmitting sensitive data (such as name, SSN, home address, etc) by utilizing WinZip or other standard encryption software. Additionally, the OIG Office of Audits failed to ensure compliance with Section 9, Non-Government of the

Computer Access Agreement, which prohibits the installation of any personally owned hardware (printers, flash drives, wireless, etc) on OIG-owned equipment.

- **DHS Management Directive 4900** states, "[u]sers will protect storage magnetic media in accordance with the highest level of data sensitivity contained. Whenever possible, stored data will be encrypted on removable media and in portable devices when not in Government facilities."

Finding B.1.6: The OIG Office of Audits did not issue or maintain control of the flash drive reported missing during the Privacy Incident as specified in DHS Directive 4300A.

- **DHS Policy Directive 4300A Section 4.3** states, "[s]torage media that contain sensitive information must be controlled so that the information is protected."
- **DHS Policy Directive 4300A Policy I.D. 4.3.1.a** states, "[c]omponents shall ensure that all media containing sensitive information, including hard copy media, backup media, and removable media such as USB drives, are stored in a secure location (e.g., a locked office, room, desk, bookcase, file cabinet, locked tape device, or other storage prohibiting access by unauthorized persons) when not in use."
- **DHS Policy Directive 4300A Policy I.D. 4.3.1.c** states, "DHS personnel, contractors, and others working on behalf of DHS are prohibited from using any non-Government issued removable media (USB drives, in particular) or connecting them to DHS equipment or networks or to store DHS sensitive information."
- **FIPS 200** states "[o]rganizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse."

Finding B.1.7: The OIG Office of Audits failed to comply with DHS Privacy Policy Guidance Memorandum 2008-01 and the FIPP Security principle when it failed to ensure that KPMG implemented specific encryption on any portable media utilized to store PII.

- **DHS Privacy Policy Guidance Memorandum 2008-01** includes a Security FIPP which states, "DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure."

2. OIG Privacy Incident Reporting

Finding B.2.1: Despite having comprehensive internal guidance, there was insufficient understanding by the OIG regarding the immediate Privacy Incident

reporting requirements and the associated responsibilities as the Component Privacy Office and Privacy Point of Contact.

- **DHS Privacy Incident Handling Guidance Section 3.4** states that the Component Privacy Office and Privacy Point of Contact shall, "[u]nderstand the Privacy Incident handling process and procedures."
- **DHS Privacy Incident Handling Guidance Section 3.4** requires Component Privacy Offices and Privacy Points of Contact to, "[n]otify and update the DHS CPO of the status of a potential Privacy Incident."
- **FIPS 200** states, "[o]rganizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities."

Finding B.2.2: The OIG did not comply with the requirements outlined within the DHS Privacy Incident Handling Guidance when it failed to notify the DHS EOC of a suspected Privacy Incident in a timely manner.

- **DHS Privacy Incident Handling Guidance Section 5.1** states, "DHS personnel must inform the PM immediately upon discovery or detection of a Privacy Incident, regardless of the manner in which it occurred."

Finding B.2.3: Non-compliance with the DHS Privacy Incident Handling Guidance Sections 3.4 and 8.1 occurred when the OIG failed to notify and update the Chief Privacy Officer of the status of a potential Privacy Incident in accordance with its duties as the Component Privacy Office and Privacy Point of Contact.

- **DHS Privacy Incident Handling Guidance Section 3.4** requires Component Privacy Offices and Privacy Points of Contact to, "[n]otify and update the DHS CPO of the status of a potential Privacy Incident."[35]
- **DHS Privacy Incident Handling Guidance Section 8.1** states, "[i]nternal notifications will take two forms: (1) Privacy Incident Notifications automatically generated by the DHS SOC Online Incident Handling System; and (2) Notifications sent by email or voicemail."

Finding B.2.4: Non-compliance with the DHS Privacy Incident Handling Guidance Sections 3.7, 5.7.1 and 8.1 occurred when the OIG failed to ensure that DHS EOC followed procedures regarding notification to DHS senior officials.

- **DHS Privacy Incident Handling Guidance Section 3.7** states the DHS Security Operations Center, "[i]nform DHS senior official of matters concerning Privacy Incidents through the use of automated Privacy Incident Notifications, conference calls, reports, and other methods."

[35] CPO is an acronym for Chief Privacy Officer.

- **DHS Privacy Incident Handling Guidance Section 5.7.1** states, "[w]hen DHS SOC transmits the Privacy Incident Report to US-CERT, the DHS SOC will simultaneously and automatically issue a Privacy Incident Notification to the Deputy Secretary, DHS CPO, DHS CIO, DHS OGC-GLD, DHS Deputy CIO, and DHS CISO, alerting them of the transmission of the Privacy Incident report to US-CERT."[36]
- **DHS Privacy Incident Handling Guidance Section 8.1** states, "[i]nternal notifications will take two forms: (1) Privacy Incident Notifications automatically generated by the DHS SOC Online Incident Handling System; and (2) Notifications sent by email or voicemail."

Finding B.2.5: Non-compliance with the DHS Privacy Incident Handling Guidance occurred when the OIG failed to convene a timely Privacy Incident Response Team. A Privacy Incident Response Team would have ensured all the Components affected by the incident were aware of their roles and mitigation responsibilities, and established the OIG as the lead on the incident response and notification to the affected parties. This failure resulted in a delayed response by the Components to assist the OIG in the external notifications to the affected parties. Based on the DHS Privacy Office investigation and interviews (outside the background provided earlier from the OIG investigation), the Components were unable to obtain specific information from the OIG to determine what information the incident may have compromised.

- **DHS Privacy Incident Handling Guidance Section 3.15** states that the duties of a Component-Level Privacy Incident Response Team, "[p]rovide[s] advice and assistance to the Component Privacy Office/PPOC as needed regarding the investigation, notification, and mitigation of Moderate-Impact Privacy Incidents" and "[c]ommunicates and coordinates, through DHS SOC, with external entities such as law enforcement, the Identity Theft Task Force, SSA, and EOP during the investigation, notification, or mitigation stages as warranted."

C. Findings Associated with Component Actions

The DHS Components played a key role in this audit investigation. Component data provided to the KPMG Audit Team was on the lost flash drive. The OIG Privacy Incident involved Sensitive PII, including SSNs, one or more DHS Components provided in response to KPMG's data request pursuant to the FY 2009 financial statement audit performed at ICE.

Finding C.1: The DHS Component financial management executives relied on KPMG-developed Audit Instructions to set the parameters and data requirements for successful audit data, and failed to provide internal training targeted to the audit or

[36] CIO is an acronym for Chief Information Officer; OGC-GLD is an acronym for Office of General Counsel, General Law Division.

issue additional guidance relating to Sensitive PII in contravention of the Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS.

- **The KPMG U.S. Department of Homeland Security Integrated Audit Instructions September 30, 2009** includes the parameters and data requirements cited above.
- **Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS** states, "[s]ensitive PII…requires special handling because of the increased risk of harm to an individual if it is compromised."

1. USCIS Obligations

Finding C.1.1: There was insufficient understanding at USCIS regarding the definition of PII and what specific data elements comprise PII as defined in the *Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS*. This deficiency resulted in the Components providing Sensitive PII to KPMG inconsistent with the security terms of the contract, DHS Management Directive 11042.1, and DHS Privacy Policy Guidance Memoranda 2007-02 and 2008-01.

- **Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS** states,

> Sensitive PII is *personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual*. Some categories of PII, when maintained by DHS, are sensitive as stand-alone data elements. Examples of such Sensitive PII include: Social Security number (SSN), alien registration number (A-Number), or biometric identifier. Other data elements such as driver's license number, financial account number, citizenship or immigration status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also Sensitive PII. In addition, the context of the PII may determine whether the PII is sensitive, such as a list of employee names with poor performance ratings. Not all PII is sensitive. For example, information on a business card or in a public phone directory of agency employees is PII, but in most cases not Sensitive PII, because it is usually widely available public information.[37]

- **FIPS 200** states, "[o]rganizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that

[37] Emphasis in the original.

organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities."

Finding C.1.2: The Financial Audit Liaison within USCIS acted inconsistently with the provisions of the Performance Work Statement, which required oversight of the responsive documents. Non-compliance with DHS Management Directive 11042.1 occurred when the Financial Audit Liaison failed to properly review, identify, and safeguard the SBU information before it was transmitted to KPMG. Non-compliance with DHS Privacy Policy Guidance Memoranda 2007-02 and 2008-01 occurred when the Financial Audit Liaison failed to ensure SSNs and other Sensitive PII were protected and required for the audit.

- **DHS Office of Inspector General Performance Work Statement dated 16 October 2009 Section 1.5** states, "DHS and its components are responsible for identifying and marking documents, date, and other information that require specific protective measures."
- **DHS Management Directive 11042.1** states that DHS employees must, "[b]e aware of and comply with the safeguarding requirements for FOUO information as outlined in this directive.**"**
- **DHS Privacy Policy Guidance Memorandum 2007-02** states, "[s]ufficient security controls must be implemented in order to mitigate the risk of inappropriate or unauthorized disclosure of data containing SSN. Any access to SSNs shall be restricted with an appropriate application of security controls. Any program collecting, using, maintaining, and/or disseminating SSNs must maintain audit logs tracking the access to the SSNs, and the program must perform periodic reviews of these audit logs." It continues, "[e]ncryption, the application of which is encouraged, will minimize the risk of unauthorized disclosure. Other security controls, such as password protection may also mitigate the risk associated with authorized disclosure. The appropriate controls will be determined by the program in coordination with the Privacy Office, Chief Information Officer, the component Privacy Officer, and the Information System Security Manager (ISSM)."
- **DHS Privacy Policy Guidance Memorandum 2008-01** includes a Security FIPP which states, "DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure."

III. Recommendations[38]

We recommend that:

With regard to contracting practices:

1. DHS contracts contain clauses or provisions that safeguard against disclosure and inappropriate use of all potential types of sensitive information to include Sensitive PII that contractors might access, create, or maintain during contract performance. This includes the responsibility for prompt notification to the agency if unauthorized disclosure or misuse of Sensitive PII occurs. [39]
2. All COTRs improve monitoring of contractor compliance with contract provisions to ensure roles and responsibilities regarding data protection and privacy compliance are executed properly.
3. All contractors that handle Sensitive PII read and certify in writing their understanding of the Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS and also certify their understanding of the rules regarding use of flash drives and other media not provided by DHS.

With regard to social security numbers, handling Sensitive PII, and data minimization:

4. DHS implement its guidance in DHS Privacy Policy Guidance Memorandum 2007-02, which asserts DHS programs shall collect, use, maintain, and disseminate SSNs only when required by statute or regulation or when pursuant to a specific authorized purpose. Absent these requirements, DHS programs shall not collect or use an SSN as a unique identifier; rather, programs shall create their own unique identifiers to identify or link information concerning an individual.
5. Components participating in the audit reviews revise their Financial Management Directives, Financial Audit Responses to Document Requests to ensure the responsibilities and procedures regarding the proper review, collection and transmission of PII are addressed.
6. Components that experience a Privacy Incident involving another Component's PII should immediately notify the affected Component Privacy Officer and continually coordinate the incident response strategy.

With regard to data security:

7. DHS enforce the existing policy as stated in DHS Policy Directive 4300A Policy I.D. 4.3.1. DHS should continue to require DHS flash drives be encrypted whenever used

[38] Recommendations are directed to responsible offices when appropriate, and are written broadly to allow greater flexibility and implementation within the Department.

[39] Appendix B contains a sample for consideration for inclusion in DHS contracts. This sample was developed by the Transportation Security Administration, Office of Privacy Policy and Compliance and has already been incorporated into several TSA and DHS contracts.

by DHS employees, contractors, or other persons with access to Sensitive PII. Whenever flash drives are utilized, Components should implement chain of custody procedures to ensure accountability for flash drives that contain Sensitive PII.

With regard to privacy training:

8. DHS Privacy Office provide targeted, directed training to the Component Privacy Officers and Privacy Points of Contact for requirements included in the DHS Privacy Incident Handling Guidance to ensure the roles and responsibilities related to Privacy Incidents are clearly understood to include immediate notification of all affected Components.
9. Each Component evaluate its privacy awareness and training programs for new and existing employees and contractors and update as necessary.

Appendix A: DHS Implementation of the FIPPs

DHS's implementation of the FIPPs[40] is described below:

- **Transparency**: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.
- **Individual Participation**: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.
- **Purpose Specification**: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- **Data Minimization**: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfil the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).
- **Use Limitation**: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.
- **Data Quality and Integrity**: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.
- **Security**: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- **Accountability and Auditing**: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

[40] *Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (Dec. 29, 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

Appendix B: Sample Language for Contract Clauses Regarding Sensitive PII and Privacy Incident Response

This sample contains language for contract clauses for inclusion in DHS contracts. The Transportation Security Administration, Office of Privacy Policy and Compliance, developed this sample and has already incorporated it into several of their contracts.

Security of Systems Handling Personally Identifiable Information and Privacy Incident Response

(a) Definitions.

"Breach" (may be used interchangeably with "Privacy Incident") as used in this clause means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar situation where persons other than authorized users, and for other than authorized purpose, have access or potential access to Personally Identifiable Information, in usable form whether physical or electronic.

"Personally Identifiable Information (PII)" as used in this clause means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a citizen of the United States, legal permanent resident, or a visitor to the United States.

Examples of PII include: name, date of birth, mailing address, telephone number, Social Security Number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), Internet protocol addresses, biometric identifiers (e.g., fingerprints), photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Personally Identifiable Information (Sensitive PII)" as used in this clause is a subset of Personally Identifiable Information, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Complete social security numbers (SSN), alien registration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint, or iris scan) are considered Sensitive PII even if they are not coupled with additional PII. Additional examples include any groupings of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(1) Driver's license number, passport number, or truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Financial information such as account numbers or Electronic Funds Transfer Information
(5) Medical Information

(6) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other Personally Identifiable information may be "sensitive" depending on its context, such as a list of employees with less than satisfactory performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains Personally Identifiable Information but it is not sensitive.

(b) Systems Access.

Work to be performed under this contract requires the handling of Sensitive PII. The contractor shall provide the Government access to, and information regarding systems the contractor operates on behalf of the Government under this contract, when requested by the Government, as part of its responsibility to ensure compliance with security requirements, and shall otherwise cooperate with the Government in assuring compliance with such requirements. Government access shall include independent validation testing of controls, system penetration testing by the Government, Federal Information Security Management Act (FISMA) data reviews, and access by agency Inspectors General for its reviews.

(c) Systems Security.

In performing its duties related to management, operation, and/or access of systems containing Sensitive PII under this contract, the contractor, its employees and subcontractors shall comply with applicable security requirements described in DHS Sensitive System Publication 4300A or any replacement publication and rules of conduct as described in TSA Management Directive 3700.4

In addition, use of contractor-owned laptops or other media storage devices to process or store PII is prohibited under this contract until the contractor provides, and the contracting officer in coordination with CISO approves, written certification by the contractor that the following requirements are met:

(1) Laptops employ encryption using a NIST Federal Information Processing Standard (FIPS) 140-2 or successor approved product;

(2) The contractor has developed and implemented a process to ensure that security and other applications software are kept current;

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

(4) When no longer needed, all removable media and laptop hard drives shall be processed (i.e., sanitized, degaussed, or destroyed) in accordance with DHS security requirements.

(5) The contractor shall maintain an accurate inventory of devices used in the performance of this contract;

(6) Contractor employee annual training and rules of conduct/behaviour shall be developed, conducted/issued, and acknowledged by employees in writing. Training and rules of conduct shall address at minimum:

(i) Authorized and official use;
(ii) Prohibition against use of personally owned equipment to process, access, or store Sensitive PII;
(iii) Prohibition against access by unauthorized users and unauthorized use by authorized users; and
(iv) Protection of Sensitive PII;

(7) All Sensitive PII obtained under this contract shall be removed from contractor-owned information technology assets upon termination or expiration of contractor work. Removal must be accomplished in accordance with DHS Sensitive System Publication 4300A, which the contracting officer will provide upon request. Certification of data removal will be performed by the contractor's Project Manager and written notification confirming certification will be delivered to the contracting officer within 15 days of termination/expiration of contractor work.

(d) Data Security.

Contractor shall limit access to the data covered by this clause to those employees and subcontractors who require the information in order to perform their official duties under this contract. The contractor, contractor employees, and subcontractors must physically secure Sensitive PII when not in use and/or under the control of an authorized individual, and when in transit to prevent unauthorized access or loss. When Sensitive PII is no longer needed or required to be retained under applicable Government records retention policies, it must be destroyed through means that will make the Sensitive PII irretrievable.

The contractor shall only use Sensitive PII obtained under this contract for purposes of the contract, and shall not collect or use such information for any other purpose without the prior written approval of the contracting officer. At expiration or termination of this contract, the contractor shall turn over all Sensitive PII obtained under the contract that is in its possession to the Government.

(e) Breach Response.

The contractor agrees that in the event of any actual or suspected breach of Sensitive PII (i.e., loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), it shall immediately, and in no event later than one hour of discovery, report the breach to the contracting officer, the Contracting Officer's Technical Representative (COTR), and the TSA Director of Privacy Policy &

Compliance (TSAprivacy@dhs.gov). The contractor is responsible for positively verifying that notification is received and acknowledged by at least one of the foregoing Government parties.

(f) Personally Identifiable Information Notification Requirement.

The contractor has in place procedures and the capability to promptly notify any individual whose Sensitive PII was, or is reasonably believed to have been, breached, as determined appropriate. The method and content of any notification by the contractor shall be coordinated with, and subject to the prior approval of the Government, based upon a risk-based analysis conducted by the Government in accordance with DHS Privacy Incident Handling Guidance. Notification shall not proceed unless the Government has determined that: (1) notification is appropriate; and (2) would not impede a law enforcement investigation or jeopardize national security.

Subject to Government analysis of the breach and the terms of its instructions to the contractor regarding any resulting breach notification, a method of notification may include letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. At minimum, a notification should include: (1) a brief description of how the breach occurred; (2) a description of the types of personal information involved in the breach; (3) a statement as to whether the information was encrypted or protected by other means; (4) steps an individual may take to protect themselves; (5) what the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and (6) point of contact information identifying who affected individuals may contact for further information.

In the event that a Sensitive PII breach occurs as a result of the violation of a term of this contract by the contractor or its employees, the contractor shall, as directed by the contracting officer and at no cost to the Government, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not to exceed 12 months from discovery of the breach. Should the Government elect to provide and/or procure notification or identity protection services in response to a breach, the contractor will be responsible for reimbursing the Government for those expenses.

(g) Pass-Through of Security Requirements to Subcontractors.

The contractor agrees to incorporate the substance of this clause, its terms and requirements, in all subcontracts under this contract, and to require written subcontractor acknowledgement of it. Violation by a subcontractor of any provision set forth in this clause will be attributed to the contractor.

Appendix C: OIG Response to Draft Report

The OIG provided this memorandum in response to the DHS Privacy Office Draft Report *OIG Privacy Incident Report and Assessment*. The DHS Privacy Office carefully considered their comments and incorporated changes where appropriate. Therefore, the findings in this final report and the comments provided in response to the draft report may no longer correspond.

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

February 24, 2011

MEMORANDUM FOR: Mary Ellen Callahan
Chief Privacy Officer

FROM: Richard L. Skinner
Inspector General

SUBJECT: DHS Privacy Office Draft Report *OIG Privacy Incident Report and Assessment*

Thank you for the opportunity to review and comment on the February 2011 DHS Privacy Office Draft Report *OIG Privacy Incident Report and Assessment*. Generally, we concur with the findings and recommendations.

Regarding the potential compromise of personally identifiable information (PII) due to KPMG's loss of an unencrypted flash drive containing DHS data, it is clear there were control breakdowns. As stated in the draft report, while KPMG had in place appropriate policies and controls to protect client data, OIG and KPMG did not monitor compliance with certain of these policies to ensure that KPMG's staff complied with requirements to use only encrypted and otherwise properly protected devices to transfer and store data relating to the financial statement audit. Shortly after reporting the loss of the flash drive, however, and throughout the remainder of 2010, KPMG and OIG voluntarily took a number of corrective actions that were completed before issuance of the draft report. Many of these corrective actions were subsequently incorporated into the 2011 Performance Work Statement (PWS). Thus, since the incident, both KPMG and the OIG Office of Audits have taken steps to improve security controls over DHS data.

Office of Audits and KPMG Actions

Since the incident, KPMG and OIG have taken the following steps to improve security controls over DHS data:

a) Both KPMG and OIG are performing periodic spot checks to ensure that the staff is following DHS security requirements and KPMG report its results to OIG. The 2011 PWS now incorporates these periodic spot checks.

b) We have modified the FY 2011 PWS to specify in no uncertain terms that any portable media used to transfer and store DHS data must be encrypted.

c) At each status meeting with components, OIG reiterates that the component is required to redact all sensitive PII unless specifically requested by KPMG to provide it and KPMG continues the practice of reminding component personnel, in writing, of DHS policies to mark sensitive material before it is provided to KPMG.

d) In data requests, KPMG, in writing, specifically states that it does not need sensitive PII and that it is the component's responsibility to ensure that sensitive PII is not provided to KPMG.

e) KPMG has enhanced training, communications, and monitoring regarding information security and privacy; installed new ICE/CIS component engagement team leadership; and the KPMG staff has examined all component provided data in an effort to intercept any sensitive information, including Sensitive PII, that may have been inadvertently provided to KPMG.

f) KPMG has implemented a new software tool on all KPMG-issued computers that automatically prompts the user to encrypt any storage devices plugged in to the computer's USB port. As an additional precaution on Federal engagements, KPMG implemented a feature on this software so that the device becomes "read-only" if a user chooses not to encrypt an external storage device, preventing the transfer of files from the KPMG computer to an unencrypted storage device.

One indication of the efficacy of these corrective actions is that, since April 1, 2010, KPMG's audit team has identified and turned down the attempted provision by DHS of sensitive PII in at least eight instances – including at least two instances by ICE/CIS personnel.

Specific Comments

Our specific comments follow:

Finding B.1. OIG Office of Audits FAR Clause Requirements

1. **Finding B.1.1** – This is a large multi-component contract and the Contracting Officer's Technical Representative (COTR) has multiple Office of Audits personnel assigned as contract monitors to assist – not to supplant -- the COTR with oversight functions. *A Guide to Best Practices for Contract Administration*, published by the Office of Federal Procurement Policy, makes clear that this is an acceptable option, stating that "Enhanced monitoring of contracts can be achieved

by having government quality assurance monitors, technical inspectors and COTRs report on the contractor's technical performance." Moreover, it is not clear what is meant by the statement "COTR responsibilities were not appropriately maintained."

2. **Finding B.1.2** – The Office of Audits has taken several steps to help ensure better compliance with DHS Directive 4300A and to limit future compromise of sensitive PII by our contractor, KPMG. During FY 2010, KPMG voluntarily implemented periodic spot checks of audit areas to ensure its employees were complying with DHS' security policies. Further, we have modified the FY 2011 PWS to require such periodic spot checks to ensure that the staff complies with DHS security requirements and report results of those spot checks to OIG. The FY 2011 PWS also includes language that the OIG may perform spot checks at KPMG work sites.

3. **Finding B.1.3** – Since 2008, KPMG has notified the components verbally and in writing at the beginning of the audit, and periodically during the audit, of their responsibility under DHS policy to identify and properly mark sensitive and classified information, including PII, and to provide handling instructions for such information prior to its release to KPMG. Furthermore, in FY 2009 and 2010, KPMG undertook intermediary review procedures to attempt to intercept any sensitive information, including sensitive PII, which was inadvertently provided to KPMG. Since the summer of 2009, KPMG has monitored, tracked, and reported instances where DHS components have provided unwanted sensitive information to KPMG. From April 2010 (after this incident) through October 2010, the KPMG audit team identified and turned down the attempted provision by DHS components of sensitive PII in at least eight instances, demonstrating the effectiveness of the enhanced controls and training. KPMG immediately notified the OIG Office of Audits upon occurrence of each of these instances.

   The PWS for the FY 2011 audit, as did prior PWSs, requires all KPMG personnel assigned to the DHS audit to complete privacy training to be provided by the OIG. The Office of Audits has requested that the Deputy Assistant Inspector General for Management develop audit related annual privacy training for KPMG employees assigned to the DHS audit. Moreover, we understand that KPMG has enhanced its own internal training for its employees.

4. **Finding B.1.4** – The Office of Audits has a robust contract oversight program of the contractor during the performance of the audit. There is at least one contract oversight monitor assigned to each component during the audit. The monitors often visit the audit locations at component work sites and in most cases are on site while the contractor is conducting field visits to DHS locations. However, we will continue to strengthen the oversight process. The Office of Audits has implemented procedures for the task monitors to conduct periodic spot checks at KPMG audit work areas. Procedures to be performed include:

- verify physical security of KPMG laptops and any external storage media containing DHS data;
- verify KPMG staff are aware of the security requirements for PII; and
- verify implementation of KPMG security procedures.

5. **Finding B.1.5** -- The statement that "...the OIG Office of Audits failed to ensure compliance with Section 9, Non-Government of the Computer Access Agreement, which prohibits the installation of any personally owned hardware (printers, flash drives, wireless, etc) on OIG-owned equipment" is not technically accurate. KPMG auditors were not issued OIG-owned equipment and at no time during the audit did KPMG install any personally owned hardware on OIG or component hardware or networks. KPMG auditors used the flash drives to move data between KPMG issued laptops and computers.

   During FY 2010 immediately after this incident, KPMG removed from use and secured all flash drives used by KPMG employees assigned to the DHS audit. KPMG further instructed its engagement team that if any audit team needed to use flash drives during the audit, they were to be procured and provided by the individual DHS components to ensure that they contained the proper encryption. In June 2010, KPMG issued firm wide guidance reminding employees of the firm's policy of mandatory encryption of all portable storage devices (such as flash drives) before they are used to copy or transfer files containing any confidential client or firm information, including sensitive PII. The Office of Audits incorporated changes into the PWS for FY 2011 to include a requirement that "the contractor must ensure that flash/thumb drives and other external storage devices used to transfer or store DHS data in its possession be encrypted to minimize the risk of harm from data loss if the portable media is misplaced." In conjunction with reminding personnel of its mandatory encryption policy, beginning mid-summer of 2010, KPMG rolled out a new software tool to all KPMG-issued computers that automatically prompts the user to encrypt any storage devices plugged in to the computer's USB port. As an additional precaution on Federal engagements, KPMG rolled out a mechanism whereby, if a user chooses not to encrypt an external storage device, the device will become "read-only," preventing the transfer of files from the KPMG computer to the unencrypted storage device. We have confirmed with KPMG that this software tool has been fully implemented.

6. **Finding B.1.6** – We have implemented a policy to require that all flash drives used during the DHS audit be provided by DHS components to ensure they are properly encrypted. In addition, during the OIG periodic spot checks (noted above), the task monitors verify that external storage media containing DHS data are properly secured.

7. **Finding B.1.7** -- The Office of Audits has incorporated changes into the PWS for FY 2011 to include a requirement that "the contractor must ensure that flash/thumb drives and other external storage devices used to transfer or store

DHS data in its possession be encrypted to minimize the risk of harm from data loss if the portable media is misplaced." We also confirmed with KPMG that they have installed a software tool on all KPMG-issued laptops that will automatically prompt the user to encrypt any storage devices plugged in to the computer's USB port and to make any device not encrypted "read only" so that no additional files can be moved onto that unencrypted device.

Finding B.2. OIG Privacy Incident Reporting

The four findings in this section are not accurate and do not recognize the complexity of the data involved in this incident and the many resources used by OIG to determine the nature and extent of the data loss. The data on the flash drive did not come from a single source or database. Rather, the data came from several different sources and ranged from screen prints from a single data system to original invoices from DHS contractors. As best OIG and KPMG were able to reconstruct, the lost flash drive contained over 3 gigabytes of data which had to be reviewed page by page and line by line because the documents were not similar in format nor did they contain the same types of data.

The timeline of events related to notification and reporting is:

March 30--flash drive left overnight in open conference room
March 31--KPMG learns flash drive is missing and begins search
April 1--KPMG notifies OIG that it lost flash drive
April 1--OIG notifies SOC of the missing flash drive, although OIG initially did not identify the incident as PII related or as a significant security incident
April 2--ICE directs SOC to transfer the incident response to ICE
April 7--KPMG provides paper copies of documents it believes were on lost flash drive
April 7--OIG reports to SOC that the flash drive may have contained PII
April 13--OIG confirms to SOC that PII was on flash drive
April 14--SOC staff notifies privacy contacts of incident

From KPMG's initial notification of the loss until April 7, 2010, KPMG was conducting its own internal investigation, attempting to reconstruct what data may have been on the missing flash drive, and then reviewing the records to determine the extent of PII loss. On April 7, KPMG provided OIG with paper copies of files it believed to be on the flash drive and which contained sensitive PII, including names, home addresses, social security numbers (SSNs), and bank account information of DHS employees.

After review of the documents by a team of eight OIG employees, OIG identified 93 individuals whose PII was included. By May 26, 2010, OIG completed notifications to all 93 affected individuals, providing information about credit monitoring services paid for by KPMG.

Additionally, in June 2010, a separate team of six OIG employees with assistance from the Privacy Office reviewed electronic copies of files obtained from KPMG that may

have been on the lost flash drive. That review uncovered an additional 250 names and SSNs related to individual background investigations performed by an ICE contractor; the list had been appended to the contractor's invoice and provided to KPMG. Sensitive information revealing bank routing and account numbers for numerous companies doing business with DHS was also discovered. By July 2010, notifications were made and credit monitoring was offered to all affected individuals and the companies were notified that their bank information was contained on the lost flash drive.

We do not agree that OIG lacks understanding of DHS incident reporting and handling procedures and policies as stated in finding B.2.1. DHS Policy Directive 4300A, Attachment F, Section 2.4.3.1 states, "[c] components shall report significant incidents to the DHS SOC as soon as possible via phone[...], but not later than one hour from 'validation,' e.g., a security event being confirmed as a significant incident." KPMG's notification was made to us at 12:24 pm. The incident was entered in SOC at 5:30 pm on April 1, 2010, the same day that KPMG notified us that a flash drive containing audit work papers had been lost. OIG did not report the incident to SOC within an hour of receiving notification from KPMG as the incident had not yet been confirmed as a significant incident. OIG did not have sufficient information at the time to document the incident as significant; however, we did provide as much information in the initial report as was available to us at the time. It is the SOC's responsibility to notify CERT within an hour of the report to it. SOC did not notify CERT until a day later—April 2, 2010, at 5:05 pm, according to SOC's own report. We do not agree that OIG contributed to this 24 hour delay in notifying CERT.

Upon notification of the incident, the OIG incident team worked closely with KPMG to perform an initial reconstruction and inventory of the data on the lost flash drive. As stated previously, this was not data contained in a single database, nor was it retrievable from a single source. On April 7, KPMG provided OIG with hard copies of the documents that were validated to have been stored on the flash drive, and believed to contain sensitive PII. The OIG incident team began an immediate review of those documents to confirm that sensitive PII existed, and determine what notifications, and to whom, should be made as a result of the data loss. Given the volume of data that had to be reviewed in the hard copy documents, OIG pulled together a team of eight people to facilitate and expedite this review. As a result of the detailed review, OIG identified individuals who could be impacted by the data loss and on April 21, 2010, requests were sent to both ICE and CIS asking for home addresses to make notifications of the loss and extend an offer of credit monitoring to the affected individuals. ICE responded on April 22, 2010; CIS did not respond until May 3, 2010. With regard to the statement that "multiple sources in OIG rather than one single point of contact" were making requests to components for addresses, OIG is unaware that anyone, other than the OIG's incident response lead, made requests directly to components for addresses of individuals affected.

Finding B.2.3. fails to reflect technological problems that delayed reporting. The SOC report indicates that DHS management was notified of the incident on April 2 at 5:08 pm, immediately after SOC's report to CERT. As OIG was posting updates to the incident

report during the week of April 12, OIG became aware that the SOC automatic email distribution which is designed to notify a specific list of recipients, including the Chief Privacy Officer, was not working properly, and that notifications were not, in fact, being properly distributed. We immediately contacted SOC to have this corrected and SOC sent manual emails to the appropriate officials. On April 13, the person serving as OIG's Privacy Point of Contact for the incident initiated contact with the Privacy Office Director of Incidents and Inquiries and worked very closely with that office throughout OIG's incident response. As noted above, OIG was in contact with SOC about the incident from April 1 until the incident report was closed.

Additional confusion was introduced in the incident handling process when, on April 2, 2010, without any consultation with OIG, ICE directed that the incident in SOC be transferred from OIG to ICE for response. That transfer, more than any other action or inaction, created confusion about which component was responsible for handling the incident. Based on this action, it is clear that ICE was aware of the incident on the day following OIG's notification to SOC.

OIG does not agree with the statement in finding B.2.4 that the "OIG failed to convene a timely Privacy Incident Response Team." While OIG has a single Privacy Point of Contact due to its size, a Privacy Incident Response Team with representatives from the Office of Audits, the Office of Management, the Office of Investigations, and Counsel to the Inspector General was immediately identified to begin work on researching the incident, performing necessary corrective actions to contain the data spill, as well as routine reporting required to update all affected parties on progress of the incident review. Upon receiving hard copies of documents from KPMG, the incident team mapped out a strategy for reviewing the documents, obtaining additional information from KPMG, conducting an inquiry to determine the causes of the loss, and determining what notifications to affected individuals would be needed. This team continued working the incident together until all necessary actions were completed. The OIG Privacy Point of Contact was primarily responsible for monitoring progress of the team reviewing the data and notifying affected parties as well as coordinating with the components.

Recommendations

With respect to the recommendations as drafted, we note that with one exception (recommendation 8) none of the recommendations are directed to any particular official. In order to ensure accountability for implementation of the recommendations, we strongly suggest that each be directed to the appropriate DHS official responsible for implementing the particular recommendation. If the Inspector General is identified as the responsible official for implementing any specific recommendation, we would request an opportunity to respond directly to the recommendation before the report is issued.

Should you have any questions about these comments, please contact me or Anne Richards, Assistant Inspector General for Audits, at (202) 254-4100.