

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Letter Report:

DHS's Implementation of Protective Measures for Personally Identifiable Information (Redacted)



Notice: The Department of Homeland Security, Office of Inspector General, has redacted this report for public release. A review under the Freedom of Information Act will be conducted upon request.




Homeland
Security

January 30, 2007

MEMORANDUM FOR: Hugo Teufel III
Chief Privacy Officer

Scott Charbo
Chief Information Officer

FROM: 
Richard L. Skinner
Inspector General

SUBJECT: *DHS's Implementation of Protective Measures for Personally Identifiable Information*

We evaluated the Department of Homeland Security's (DHS) implementation of the recommendations set forth in the Office of Management and Budget's (OMB) Memorandum 06-16, *Protection of Sensitive Agency Information*. Our objective was to determine whether DHS has effectively implemented safeguards to protect sensitive and personally identifiable information (PII). We transmitted the results of our evaluation to the President's Council on Integrity and Efficiency (PCIE), using the format it suggested. In addition, we are providing the findings of our review to the department in this report (See Appendix F).

DHS and its components are in the process of implementing OMB's recommended security controls for sensitive data and PII. DHS has issued updated policies and procedures to address OMB's recommendations. Further, DHS is in the process of identifying PII systems, encrypting laptop computers, and implementing remote access security and offsite transportation and storage controls. Until all systems collecting, processing, or storing PII are identified, and adequate controls for protecting remote access and storage of PII are implemented, DHS lacks assurance that sensitive data are properly protected.

In response to our draft report, DHS concurred and plans to take steps to implement each of the recommendations. DHS' response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix A. In addition, we incorporated DHS' comments, including the identification of the recommendations by the responsible office.

We hope our observations will be of assistance as you move forward to implement OMB's recommendations for the protection of sensitive agency information. Should you have any questions

or concerns, please call me, or your staff may contact Frank Deffer, Assistant Inspector General, Information Technology, at 202-254-4100.

Background

OMB has defined PII as:¹

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

Various laws and regulations have addressed the need to protect sensitive information such as PII held by government agencies. These laws and regulations include the Federal Information Security Management Act of 2002 (FISMA), the E-Government Act of 2002, the Privacy Act of 1974, and OMB Circular A-130, Management of Federal Information Resources. Following several recent incidents involving the compromise or loss of sensitive personal information, OMB issued Memorandum 06-16 on June 23, 2006. The memorandum recommends measures to compensate for the lack of physical security controls when information is removed from or accessed from outside the agency location.² These measures include (1) verifying the adequacy of agency policies and procedures; (2) identifying systems processing PII; (3) encrypting data on laptops and mobile computing devices; and, (4) implementing remote access security and offsite transportation and storage controls. Agencies were to ensure that these safeguards had been reviewed and implemented by August 7, 2006.

DHS Has Issued Updated Policies and Procedures

DHS issued *Sensitive Systems Policy Directive 4300A* and *National Security Systems Policy Directive 4300B* to provide guidance to DHS components regarding the protection of information technology (IT) systems and data. These policies outline the management, operational, and technical controls necessary for ensuring confidentiality, integrity, availability, and authenticity for DHS IT systems. The department, with the *DHS 4300A Sensitive Systems Handbook* and the *DHS 4300B National Security Systems Handbook*, provides specific techniques and procedures for implementing the requirements of DHS policy. In addition, DHS separately issued policies and procedures for complying with the privacy requirements of the Privacy Act of 1974, E-Government Act of 2002, and the Homeland Security Act of 2002, including Management Directive 0470.2, *Privacy Act*

¹ 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.

² OMB Memorandum 06-16 outlines four specific actions that agencies are to take to ensure the protection of sensitive data. The memorandum also includes a checklist developed by the National Institute of Standards and Technology addressing protections for PII that is accessed remotely or physically transported outside of the agency's secured, physical perimeter.

Compliance, and guidance on the completion of privacy impact assessments (PIA) for systems and programs.³

In September 2006, the DHS Office of the Chief Information Officer (CIO), in conjunction with the DHS Privacy Office, updated the department's 4300 policy directives and handbooks to reflect the recommendations outlined in OMB Memorandum 06-16. DHS policy was updated to (1) require the encryption of PII when removed from a DHS facility; (2) require that remote access to PII be two-factor authentication mechanisms based on agency-controlled certificates or hardware tokens; (3) prohibit remote downloading and storage of PII unless documented in the system security plan (SSP).⁴ In addition, DHS policy requires that user sessions be terminated after 20 minutes of inactivity, and that sensitive information stored on any laptop computer that may be used in a residence or on travel be encrypted using Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements For Cryptographic Modules*, approved encryption. The updated policy requirements were incorporated into the department's certification and accreditation (C&A) tool in August 2006.

PII System Identification Is Still In Progress

DHS has integrated the identification of PII systems, as well as the determination of necessary protection mechanisms for these systems, into the department's C&A process. DHS requires that privacy threshold assessments (PTA),⁵ PIAs, SSPs, system risk assessments,⁶ and information security categorization⁷ be completed as part of the system C&A process. DHS began requiring PTAs in January 2006 to ensure that systems collecting, processing, or storing PII are identified. DHS component officials are responsible for developing draft PTAs, which are then validated by the DHS Privacy Office. The PTA validation process determines whether a system must be covered by a PIA, in accordance with the E-Government Act of 2002 and the Homeland Security Act of 2002. PIAs, in conjunction with SSPs, security categorizations, and risk assessments, ensure that system security controls are implemented to address the risk associated with PII.

³ A PIA is an analysis of how PII is collected, stored, protected, shared, and managed. Under the E-Government Act of 2002, a PIA should (1) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form via an electronic information system; and (2) evaluate protections and alternative processes for handling information to mitigate potential privacy risks. The E-Government Act of 2002 requires the Chief Privacy Officer to ensure that components complete PIAs for all new technologies, new collections of personal information, and new systems or existing systems that are being substantially updated.

⁴ The SSP provides a complete description of the information system, including purposes and functions, system boundaries, architecture, user groups, interconnections, hardware, software, encryption techniques, and network configuration. The SSP also provides an overview of the security requirements of the system and describes the controls in place or planned for meeting those requirements

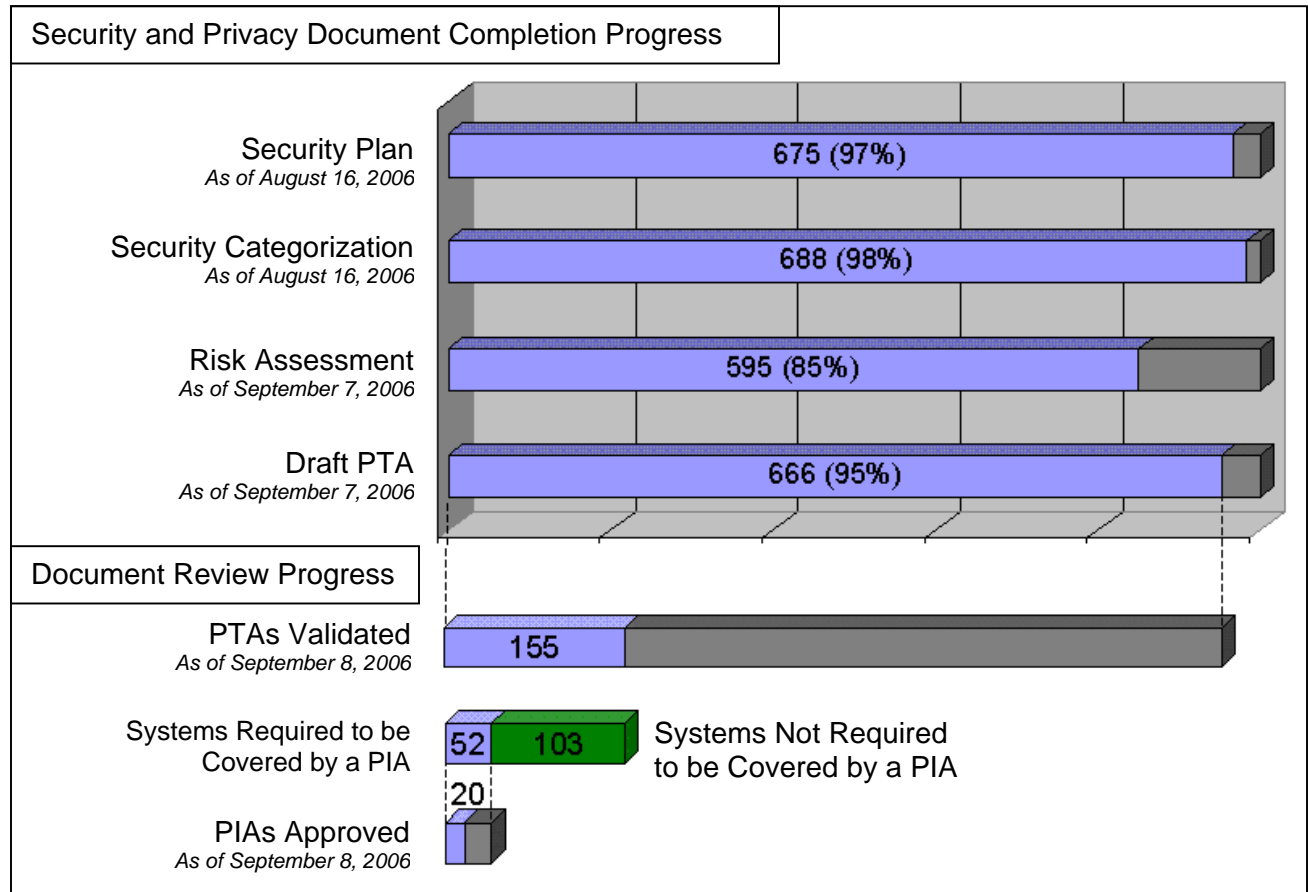
⁵ The PTA consists of a series of questions designed to aid system owners and program managers in determining if a system must be covered by a PIA. Whereas PIAs are usually completed for programs and a PIA can cover a number of systems, all DHS systems are required to have a

⁶ Risk Assessment is the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact

⁷ Information security categorization, as required by FISMA and outlined in FIPS Publication 199, is the process of identifying the potential impact (low, moderate, or high) to organizations or individuals in the event of a security breach, i.e., loss of data confidentiality, integrity, or availability. In September 2006, DHS updated its information security policy to require that all PII systems be given a potential impact level of at least moderate for data confidentiality.

DHS has completed SSPs, security categorizations, risk assessments, and draft PTAs for most of the department's 699 systems. DHS is in the process of validating the completed PTAs and PIAs. The DHS Privacy Office planned to complete the validation of the existing PTAs by the end of October 2006. In addition, DHS component officials are to complete all PIAs for DHS Privacy Office approval by the end of fiscal year (FY) 2007. Until DHS completes and validates the security documentation, PTAs, and PIAs for its systems and programs, the department lacks assurance that the risks associated with sensitive data and PII have been determined and appropriate security controls have been identified.

Graph 1: Completion of Security and Privacy Documentation



Source: Office of Inspector General (OIG), based on DHS FISMA and Privacy Office documentation

Encryption of Laptop Computers Has Not Been Completed

DHS has not encrypted sensitive data or PII stored on laptop computers. Of the 16 DHS components, only four had implemented laptop computer encryption. Specifically, -----

 ----- reported that they had implemented full hard drive encryption on many of their laptop computers. ----- officials stated that they plan to encrypt the remaining laptop computers once hardware limitations and inventory issues are resolved, and sufficient software licenses are obtained. -----

-----) officials stated that hard drive encryption had been implemented on all laptop computers, but they were not able to confirm that this actually had been accomplished.

Officials from the remaining 12 DHS components stated that they are in the process of implementing the encryption mechanisms recommended by OMB and required by DHS. For example, the ----- began implementing laptop encryption in September 2006.

In addition, the ----- is in the process of implementing full hard drive encryption on -----

----- laptop computers. Until adequate encryption mechanisms have been implemented, there is increased risk that sensitive data or PII may be compromised through the loss or theft of laptop computers and mobile computing devices.

PII Remote Access and Storage Controls Need Strengthening

DHS has not implemented the OMB recommended controls over remote access to, and offsite transportation and storage of, sensitive and PII data. We interviewed DHS component officials and reviewed security documents for a sample of 25 DHS systems that collect, use, or store PII.⁹ DHS components have not:

- Encrypted PII for offsite transportation and storage. For 21 of the systems, component officials transport backup media containing PII to an alternate storage facility. The data for only two systems is encrypted during transportation, and the data for only one system is encrypted while stored offsite.
- Established adequate remote access security controls for PII. For each of the 23 systems with remote access capabilities, DHS components employ an encrypted VPN connection for remote access connections to PII. DHS components have implemented two-factor remote access authentication for 18 (78 percent) of the 23 systems. In addition, DHS components require re-authentication after 20 minutes of inactivity on 14 (61 percent) of the 23 systems, and after 30 minutes of inactivity on an additional seven systems (30 percent).
- Implemented sufficient controls over PII copies or extracts. DHS components have not implemented a process to verify that extracts are erased within 90 days if no longer required on any of the 11 systems that allow users to download PII data. In addition, DHS components reportedly enforce encrypted remote storage of downloaded data on only 3 of the 11 systems, through the use of measures such as hard drive encryption on the workstations connecting to the system. Further, a process has been implemented on only 1 of the 25 systems to ensure that any computer-readable data extracts made by administrators are erased within 90 days if no longer required.

DHS components are in the process of implementing the OMB-recommended remote access security and offsite transportation and storage controls. For example, ----- is developing an encryption plan for backup media containing PII sent to a remote location and the ----- is currently implementing two-factor authentication for remote access VPN connections.

⁸ -----

⁹ See Appendices B – E.

According to DHS component officials, the implementation of enhanced remote access and storage controls has been hindered by uncertainty regarding the applicability and scope of the OMB recommendations and new DHS requirements. For example, the Information System Security Managers (ISSM) for USSS and USCIS were uncertain whether the electronic transfer of data to a remote site through a network connection constitutes offsite transportation and storage, or whether hardcopy printouts of PII data should be considered downloads under the new requirements. Component officials also requested clarification on whether the OMB and DHS requirements applied equally to all PII data, including PII data limited to DHS employee contact information. Until adequate controls are implemented for protecting remote access to, and offsite transportation and storage of, sensitive data and PII, DHS lacks assurance that sensitive data is properly protected.

Recommendations

We recommend that the Chief Privacy Officer (CPO):

1. Ensure completion of the identification of systems that collect, process, or store personally identifiable information, as well as the assessment of the risk associated with the systems and data.

We recommend that the CIO: Encrypt personally identifiable information stored on laptop computers and mobile computing devices, as well as data transported and stored at an alternate facility.

3. Establish proper remote access security controls for access to PII, including two-factor authentication for remote access connections and session termination after 20 minutes of inactivity.
4. Implement sufficient controls over electronic copies and extracts of personally identifiable information, including procedures to ensure that copies or extracts made by users or administrators are erased within 90 days if no longer required.
5. Identify aspects of the updated DHS policies and procedures requiring clarification, and provide additional guidance to component officials on the requirements.

Management Comments and OIG Analysis

DHS agreed with recommendation 1. The CPO is reviewing all component systems to determine whether PII is collected, processed, or stored. The DHS Privacy Office has developed a corrective action plan to complete and approve all remaining PTAs by June 30, 2007 and all PIAs by the end of FY 2008.

We agree that the steps CPO has taken, and plans to take, satisfy this recommendation.

DHS agreed with recommendation 2. The CISO will direct the component ISSMs with systems identified as non-compliant to implement encryption on systems with PII data.

We agree that the steps DHS plans to take satisfy this recommendation.

DHS agreed with recommendation 3. The CISO will direct the component ISSMs with systems identified as non-compliant to implement two-factor authentication and session termination after 20 minutes of inactivity.

We agree that the steps DHS plans to take satisfy this recommendation.

DHS agreed with recommendation 4. The CISO will recommend policy improvement to DHS MD 4300A and 4300B before July 31, 2007. The CISO will direct the component ISSMs with systems identified as non-compliant to implement controls to ensure that data extracts are monitored and deleted within 90 days.

We agree that the steps DHS plans to take satisfy this recommendation.

DHS agreed with recommendation 5. The CISO will review all recommendations to DHS MD 4300A and 4300B to update or clarify PII requirements or guidance.

We agree that the steps DHS plans to take satisfy this recommendation.

We conducted our audit from August to September 2006 under the authority of the Inspector General Act of 1978, as amended, and according to generally accepted government audit standards.

Appendix A: Management Response

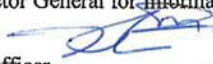
U.S. Department of Homeland
Security
Washington, DC 20528





Homeland Security

December 19, 2006

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General for Information Technology

VIA: Hugo Teufel III 
Chief Privacy Officer

Scott Charbo 
Chief Information Officer

FROM: Robert West 
Chief Information Security Officer

SUBJECT: *OIG-07-XXX, Draft DHS's Implementation of Protective Measures for Personally Identifiable Information, Dated November 15, 2006.*

Thank you for providing a copy of the draft Letter Report describing the implementation status of the Department of Homeland Security (DHS) Personally Identifiable Information (PII) protective measures.

The Department generally concurs with the recommendations included in the OIG's draft letter report. General comments concerning the body of the report and specific action plans for each recommendation are included in Attachment A to this letter.

The Department is concerned that the short deadline (45 days) prescribed by the Office of Management and Budget (OMB) in M-06-16, *Protection of Sensitive Agency Information* has not allowed adequate time to fully implement all of the required operational and technical controls. While the management team is actively taking steps to bring systems into compliance, DHS is a large and complex agency supporting nearly 700 systems.

Should you have any questions or need further clarification, please contact Rebecca J. Richards at the Privacy Office (571) 227-3813 or Wayne Bavry at the Office of Information Security (OIS) Compliance Office (202) 282-9506.

cc: Madeline Griggs, CIO Audit Liaison
Steve Pecinovsky, Director Department GAO/OIG Liaison Office

Attachment A: Management Comments on OIG-07-XXX, *DHS's Implementation of Protective Measures for Personally Identifiable Information.*

Appendix A: Management Response

Attachment A: Management Comments on OIG-07-XXX, DHS's Implementation of Protective Measures for Personally Identifiable Information, Dated November 15, 2006.

General Comments:

1. The report should be directed to the DHS Chief Privacy Officer in addition to the CIO. DHS MD 0470.2 assigns responsibility for protecting Personally Identifiable Information (PII) to the DHS Privacy Officer, who reports directly to the Secretary of Homeland Security.
2. OIG recommendations need to be more clearly aligned to the Department's organizational structure in order for responsibilities to be clearly identified and tracked to closure.
3. Recommendations 2 and 3 should be limited to PII and not include other sensitive [but unclassified] (SBU) information. The OIG analysis was limited to systems processing PII. While it is important to secure all SBU information, PII was the focus of this audit.

Finding and OIG Recommendation 1:

"Acting Under Secretary for Management instruct the CIO and Chief Privacy Officer to ensure completion of the identification of systems that collect, process, or store personally identifiable information, as well as the assessment of the risk associated with the systems and data."

Privacy Office Response:

Note the Chief Privacy Officer reports to the Secretary. The Chief Privacy Officer, not the CIO, is responsible for validation of privacy threshold assessment (PTA) approval and publishing of privacy impact analysis (PIA) and System of Record Notices.

The Chief Privacy Officer has been working with the components to review all systems to determine whether or not Personally Identifiable Information (PII) is collected, processed, or stored. As of December 1, 2006 the Privacy Office metrics are:

- 588 PTAs validated, 112 PTAs in progress
- 417 PIAs not required, 171 PIAs required
- 60 PIAs approved, 60 PIAs in progress, 51 PIAs pending
- 289 System of Record Notices published in the Federal Register

The DHS Privacy Office Corrective Action Plan (CAP) is to:

- A. Complete and approve all remaining PTAs by June 30, 2007.
- B. Complete, approve and publish thirty percent (30%) of the PIAs by December 31, 2007.
Work toward PIA and SORN compliance by the end of Fiscal Year 2008.

Appendix A: Management Response

- C. Review the PIA process, which assesses risks associated with programs, systems and data to determine how best to update guidance to reflect OMB M-06-16 requirements.
- D. Increase Departmental PII awareness training. The DHS Privacy Office has prepared an interactive Privacy Awareness training that will be hosted on the DHS on-line Learning Management System (LMS) in 2007. All DHS employees and contractors will be required to complete this training as part of the new employee and contractor orientation.
- E. Additional programs to train program managers and system users on Privacy Act requirements are also under development. These programs will be used to reinforce and broaden understanding about DHS obligations to protect PII, particularly for remote access, off site transportation and storage of PII, and procedures to ensure that copies or extracts of PII are erased within 90 days if no longer needed as well as PII incident reporting. The CIO and CISO will be requested by the Privacy Office to review recommended training materials before fielding.

Finding and OIG Recommendation 2:

“Acting Under Secretary for Management instruct the CIO and Chief Privacy Officer to encrypt sensitive or personally identifiable information stored on laptop computers and mobile computing devices, as well as data transported and stored at an alternate facility.”

Office of Information Security Response:

Note the CISO reports to the CIO.

The Department’s CISO will direct the component ISSMs to open system POA&Ms for each System identified as non-compliant in order to track implementation of the following controls:

- A. Encrypting PII data stored on laptop computers
- B. Encrypting PII data stored on mobile devices (Portable Electronic Devices and Personal Digital Assistants)
- C. Offsite Transportation and Storage of PII (See OIG Report Appendix B)

Finding and OIG Recommendation 3:

“Acting Under Secretary for Management instruct the CIO and Chief Privacy Officer to establish proper remote access security controls for access to PII, including two-factor authentication for remote access connections and session termination after 20 minutes of inactivity.”

Office of Information Security Response:

Note the CISO reports to the CIO.

- A. The Department’s CISO will direct the component ISSMs to open system POA&Ms for each System identified (See OIG Report Appendix C) as non-compliant in order to track implementation of the following controls: *“Two-factor authentication for remote access to PII.”*

Appendix A: Management Response

- B. The Department's CISO will direct the component ISSMs to open system POA&Ms for each System identified (See OIG Report Appendix C) as non-compliant in order to track implementation of the following controls: *"20 minute or less time-out function."*

Finding and OIG Recommendation 4:

"Acting Under Secretary for Management instruct the CIO and Chief Privacy Officer to implement sufficient controls over copies and extracts of sensitive or personally identifiable information, including procedures to ensure that copies or extracts made by users or administrators are erased within 90 days if no longer needed"

Office of Information Security Response:

Note the CISO reports to the CIO.

The CISO will recommend policy improvements to DHS MD 4300 A and B before July 31, 2007 to define requirements to support manual procedures along with Information System Security Office (ISSO) tracking controls and responsibilities. A POA&M with OIS will be identified to track policy progress.

The Department's CISO will direct component ISSMs to open system POA&Ms for each System identified (See OIG Report Appendix D) as non-compliant in order to track implementation of the following controls: *"Are data extracts by administrators monitored & deleted within 90 days."*

Office of the Chief Information Security Officer Response:

Note the CIO reports to the Acting Under Secretary for Management.

Recommend the office of the CIO review current technologies which may be capable of providing automated controls in support of this function. A POA&M with a CIO office point of contact (POC) will be identified to track progress.

Finding and OIG Recommendation 5:

"Acting Under Secretary for Management instruct the CIO and Chief Privacy Officer to identify aspects of the updated DHS policies and procedures requiring clarification, and provide additional guidance to component officials on the requirements."

Office of Information Security Response:

Based on requests from the Chief Privacy Officer, CIO, OIG or Components, the CISO will review all recommendations to DHS MD 4300 A and B to update or clarify PII requirements or guidance. If necessary the Office of Information Security will open POA&M's to support any necessary updates. At this point no POA&M will be opened to support this recommendation.

Appendix B: DHS Component Systems Reviewed

Component	System(s)
[Redacted]	<ul style="list-style-type: none"> [Redacted] [Redacted]
[Redacted]	<ul style="list-style-type: none"> [Redacted] [Redacted]
[Redacted]	<ul style="list-style-type: none"> [Redacted] [Redacted]
[Redacted]	<ul style="list-style-type: none"> [Redacted] [Redacted]
[Redacted]	<ul style="list-style-type: none"> [Redacted] [Redacted]
[Redacted]	<ul style="list-style-type: none"> [Redacted]
[Redacted]	<ul style="list-style-type: none"> [Redacted]
[Redacted]	<ul style="list-style-type: none"> [Redacted] [Redacted]
[Redacted]	<ul style="list-style-type: none"> [Redacted] [Redacted]
[Redacted]	<ul style="list-style-type: none"> [Redacted] [Redacted]
[Redacted]	<ul style="list-style-type: none"> [Redacted] [Redacted]
[Redacted]	<ul style="list-style-type: none"> [Redacted] [Redacted]
[Redacted]	<ul style="list-style-type: none"> [Redacted] [Redacted]
[Redacted]	<ul style="list-style-type: none"> [Redacted]

Appendix C: Offsite Transportation and Storage of PII

Component PII System(s)	Offsite Transportation and Storage of PII		
	Is PII data:		
	Transported/stored at an offsite location?	Encrypted during offsite transportation?	Encrypted during offsite storage?
[Redacted]			
• [Redacted]	Yes	No	No
• [Redacted]	Yes	No	No
[Redacted]			
• [Redacted]	Yes	No	No
• [Redacted]	Yes	Yes	No
[Redacted]			
• [Redacted]	Yes	No	No
• [Redacted]	Yes	No	No
[Redacted]			
• [Redacted]	Yes	No	No
• [Redacted]	Yes	No	No
[Redacted]			
• [Redacted]	No	N/A	N/A
• [Redacted]	Yes	No	No
[Redacted]			
• [Redacted]	Yes	No	No
[Redacted]			
• [Redacted]	Yes	No	No
• [Redacted]	Yes	No	No
[Redacted]			
• [Redacted]	Yes	Yes	Yes
• [Redacted]	Yes	No	No
[Redacted]			
• [Redacted]	No	N/A	N/A
• [Redacted]	No	N/A	N/A
[Redacted]			
• [Redacted]	Yes	No	No
• [Redacted]	Yes	No	No
[Redacted]			
• [Redacted]	Yes	No	No
• [Redacted]	Yes	No	No
[Redacted]			
• [Redacted]	Yes	No	No
• [Redacted]	Yes	No	No
[Redacted]			
• [Redacted]	No	N/A	N/A

Appendix D: Remote Access to PII

Component PII System(s)	Remote Access to PII		
	Are the following established for remote access connections:		
	Encrypted VPN?	Two-factor authentication?	20-minute or less time-out function?
[REDACTED]			
[REDACTED]	Yes	Yes (ID/password+token)	No (30 minutes)
[REDACTED]	Yes	Yes (ID/password+token)	No (30 minutes)
[REDACTED]			
[REDACTED]	Yes	Yes (ID/password+IP address)	Yes (5 minutes)
[REDACTED]	Yes	Yes (ID/password+IP address)	No (60 minutes)
[REDACTED]			
[REDACTED]	Yes	Yes (ID/password+certificate)	Yes (5 minutes)
[REDACTED]	N/A (no remote access)	N/A	N/A
[REDACTED]			
[REDACTED]	Yes	Yes (ID/password+token)	Yes (20 minutes)
[REDACTED]	Yes	Yes (ID/password+token)	Yes (20 minutes)
[REDACTED]			
[REDACTED]	Yes	Yes (ID/password+token)	No (30 minutes)
[REDACTED]	Yes	Yes (ID/password+certificate)	Yes (20 minutes)
[REDACTED]			
[REDACTED]	Yes	Yes (ID/password+token)	No (30 minutes)
[REDACTED]			
[REDACTED]	Yes	No (ID/password only)	Yes (20 minutes)
[REDACTED]			
[REDACTED]	Yes	No (ID/password only)	No (30 minutes)
[REDACTED]	Yes	Yes (ID/password+IP address)	No (30 minutes)
[REDACTED]			
[REDACTED]	Yes	No (ID/password only)	Yes (15 minutes)
[REDACTED]	Yes	No (ID/password only)	No (120 minutes)
[REDACTED]			
[REDACTED]	Yes	Yes (ID/password+IP address or certificate)	Yes (20 minutes)
[REDACTED]	Yes	Yes (ID/password+IP address or certificate)	Yes (20 minutes)
[REDACTED]			
[REDACTED]	Yes	Yes (ID/password+token)	Yes (20 minutes)
[REDACTED]	Yes	Yes (ID/password+token)	Yes (20 minutes)
[REDACTED]			
[REDACTED]	Yes	Yes (ID/password+token)	Yes (20 minutes)
[REDACTED]	N/A (no remote access)	N/A	N/A
[REDACTED]			
[REDACTED]	Yes	Yes (ID/password+token)	Yes (15 minutes)
[REDACTED]	Yes	Yes (ID/password+token)	No (30 minutes)
[REDACTED]			
[REDACTED]	Yes	No (token being implemented)	Yes (15 minutes)

Appendix E: Downloading PII Copies or Extracts

Component PII System(s)	Downloading PII Copies or Extracts		
	If users can copy or extract data:		Are data extracts by administrators monitored & deleted within 90 days?
	Are extracts tracked & deleted within 90 days?	Is data encrypted when stored remotely?	
[REDACTED]			
[REDACTED]	No	Partial (if stored on laptop)	No (not deleted)
[REDACTED]	N/A (cannot copy)	N/A	No (not deleted)
[REDACTED]			
[REDACTED]	N/A (cannot copy)	N/A	No (not monitored or deleted)
[REDACTED]	N/A (cannot copy)	N/A	No (not monitored or deleted)
[REDACTED]			
[REDACTED]	No	Yes	No (not deleted)
[REDACTED]	No	No	No (not monitored or deleted)
[REDACTED]			
[REDACTED]	N/A (cannot copy)	N/A	No (not deleted)
[REDACTED]	N/A (cannot copy)	N/A	No (not monitored or deleted)
[REDACTED]			
[REDACTED]	N/A (cannot copy)	N/A	Yes
[REDACTED]	No	Yes	No (not monitored or deleted)
[REDACTED]			
[REDACTED]	N/A (cannot copy)	N/A	No (not monitored or deleted)
[REDACTED]			
[REDACTED]	No	No	No (not monitored or deleted)
[REDACTED]			
[REDACTED]	N/A (cannot copy)	N/A	No (not deleted)
[REDACTED]	N/A (cannot copy)	N/A	No (not deleted)
[REDACTED]			
[REDACTED]	No	No	No (not monitored or deleted)
[REDACTED]	N/A (cannot copy)	N/A	No (not deleted)
[REDACTED]			
[REDACTED]	No	Partial (if stored on laptop)	No (not deleted)
[REDACTED]	N/A (cannot copy)	N/A	No (not deleted)
[REDACTED]			
[REDACTED]	N/A (no users)	N/A	No (not monitored or deleted)
[REDACTED]	No	Yes	No (not monitored or deleted)
[REDACTED]			
[REDACTED]	No	No	No (not monitored or deleted)
[REDACTED]	No	No	No (not monitored or deleted)
[REDACTED]			
[REDACTED]	No	No	No (not deleted)

Appendix F: DHS OIG Response To PCIE Data Collection Instrument

Office of Inspector General

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



**Homeland
Security**

September 22, 2006

Mr. Charles Coe
AIG for Technology Audits and Computer Investigations
550 Potomac Center Plaza
12th Street SW, Suite 8129
Washington, DC 20024-6122

Dear Mr. Coe:

Per the Office of Management and Budget (OMB) and in accordance with the guidance provided by your office to agency Inspectors General, I am pleased to transmit to you the completed data collection instrument (DCI) detailing the Department of Homeland Security's (DHS) progress in implementing the recommendations in OMB Memorandum 06-16, *Protection of Sensitive Agency Information*. To complete the DCI, we interviewed officials from the DHS Office of the Chief Information Officer (OCIO) and DHS Privacy Office, and reviewed DHS policy and procedure documents related to the protection of personally identifiable information (PII). In addition, we interviewed DHS component officials and reviewed security documents for a sample of 25 DHS systems that collect, use, or store PII. Finally, we conducted technical testing of the laptop encryption configuration being deployed to 5 of DHS' 16 component organizations.

Should you have any questions, please call me, or your staff may contact Frank Deffer, Assistant Inspector General, Information Technology, at (202) 254-4100.

Sincerely,

A handwritten signature in black ink, appearing to read "R. L. Skinner".

Richard L. Skinner
Inspector General

Attachment

cc: Secretary
Deputy Secretary
Chief of Staff

Appendix F: DHS OIG Response To PCIE Data Collection Instrument

General Counsel
Executive Secretary
Robert West, Chief Information Security Officer, OCIO
Hugo Teufel, Chief Privacy Officer, Privacy Office
Madeline Griggs, Audit Liaison, OCIO
Steven Pecinovsky, Director, GAO/OIG Liaison Office

Appendix F: DHS OIG Response To PCIE Data Collection Instrument

APPENDIX I: IG DATA COLLECTION INSTRUMENT

This data collection instrument (DCI) was developed by the FAEC IT Committee of the PCIE/ECIE to assist IGs in determining their agency's compliance with OMB Memorandum M-06-16. The data collection instrument contains three parts. The first part is based on a security checklist developed by NIST (see Section 1 below). Questions in the DCI are designed to assess Agency requirements in the memorandum, which are linked to NIST SP 800-53 and 800-53A. Each IG can use the associated checklist and the relevant validation techniques for their own unique operating environment. Section 2 is the additional actions required by OMB M-06-16. Section 3 should document your overall conclusion as well as detailed information regarding the type of work completed and the scope of work performed.

For each overall Step and Action Item, please respond **yes, no, partial, or not applicable**. For no, partial, and not applicable responses, please provide additional information in the comments sections. After the yes, no, partial, or not applicable response, IG's have the option to provide an overall response using the six control levels as defined below for the overall Step. Each condition for the lower level must be met to achieve a higher level of compliance and effectiveness. For example, for the control level to be defined as "Implemented", the Agency must also have policies and procedures in place. The determination of the control level for each step should be based on the responses provided to the Action Items included in that step.

Controls Not Yet in Place - The answer would be "Controls Not Yet in Place" if the Agency does not yet have documented policy for protecting PII.

Policy - The answer would be "Policy" if controls have been documented in Agency policy.

Procedures - The answer would be "Procedures" if controls have been documented in Agency procedures.

Implemented - The answer would be "Implemented" if the implementation of controls has been verified by examining procedures and related documentation and interviewing personnel to determine that procedures are implemented.

Monitor & Tested - The answer would be "Monitor and Tested" if documents have been examined & interviews conducted to verify that policies and procedures for the question are implemented and operating as intended.

Integrated - The answer would be "Integrated" if policies, procedures, implementation, and testing are continually monitored and improvements are made as a normal part of agency business processes.

Appendix F: DHS OIG Response To PCIE Data Collection Instrument

APPENDIX I: IG DATA COLLECTION INSTRUMENT

PLEASE PROVIDE YOUR RESPONSES USING THE DROP DOWN MENU IN GRAY		
Section One		
Security Controls and Assessment Procedures		
Security Checklist For Personally Identifiable Information That is To Be Transported and/ or Stored Offsite, Or That is To Be Accessed Remotely		
	REQUIRED RESPONSE	OPTIONAL RESPONSE
<i>Procedure</i>	Yes No Partial Not Applicable	<i>Controls Not Yet in Place</i> Policy Procedures Implemented Monitor & Tested Integrated
STEP 1: Has the Agency confirmed identification of personally identifiable information protection needs? If so, to what level?	Partial	Implemented
<i>Action Item 1.1: Has the Agency verified information categorization to ensure identification of personal identifiable information requiring protection when accessed remotely or physically removed?</i>	Partial	
<i>Comments:</i>		
<p>DHS has integrated the identification of personally identifiable information (PII) into the department's certification and accreditation (C&A) process. DHS requires that information categorization be completed, based on Federal Information Processing Standards (FIPS) Publication 199, as part of the C&A for each system. In September 2006, DHS updated its information security policy to require that all PII systems have a confidentiality rating of at least moderate. In addition, beginning in January 2006, DHS required that a privacy threshold assessment (PTA) be completed for each system to identify systems collecting, using, or storing PII. These requirements have been implemented in the department's C&A tool, Risk Management System (RMS). Based on the PTA, the DHS Privacy Office determines whether a system must be covered by a privacy impact assessment (PIA), in accordance with the <i>E-Government Act of 2002</i> and the <i>Homeland Security Act of 2002</i>. The DHS Privacy Office is responsible for reviewing PIAs for completeness and accuracy, as well as approving and publishing final PIAs.</p>		
<p>Based upon our analysis of data in DHS' enterprise management and FISMA reporting tool, Trusted Agent FISMA, as of August 16, 2006, FIPS information categorization has been completed for 688 (98 percent) of DHS' 699 operational major applications and general support systems. In addition, DHS component officials had completed a PII self-identification review for 604 (86 percent) of DHS' 699 operational systems. For those systems with a completed self-identification review, 149 (25 percent) were identified as collecting, using, or storing PII.</p>		
<p>As of September 8, 2006, PTAs had been validated by the DHS Privacy Office for 155 of DHS' 699 operational systems (22 percent), of which 71 collect, use, or store PII. For the 71 PII systems, 52 are required under the <i>E-Government Act of 2002</i> to be covered by a PIA. Twenty of the 52 DHS systems (39 percent) are covered by an approved PIA. The DHS Privacy Office plans to complete the validation of the existing PTAs by the end of October 2006. In addition, DHS component officials are required to complete all PIAs for DHS Privacy Office approval by the end of fiscal year 2007.</p>		
<i>Action Item 1.2: Has the Agency verified existing risk assessments?</i>	Partial	
<i>Comments:</i>		
<p>DHS assesses the risk associated with PII as part of the C&A process through the use of PTAs, PIAs, system risk assessments (RA), and system security plans (SSP). DHS developed PTAs to ensure that systems collecting, using, or storing PII are identified and that system security controls are implemented to address the risk associated with privacy data. For systems that collect, use, or store PII, a PIA may also be required under the <i>E-Government Act of 2002</i>. Further, in September 2006 DHS updated its information security policy to reflect the recommendations outlined in Office of Management and Budget (OMB) Memorandum 06-16, <i>Protection of Sensitive Agency Information</i>. These policy changes have been incorporated into the department's C&A process through enhancements to DHS' C&A tracking tool, which were completed in August 2006.</p>		
<p>Based upon our analysis of data in Trusted Agent FISMA as of August 16, 2006, SSPs have been completed for 675 (97 percent) of DHS' 699 operational systems, including 146 of the 149 DHS systems self identified by DHS component officials as collecting, using, or storing PII. As of September 7, 2006, current risk assessments have been completed for 596 (85 percent) of DHS' 699 operational systems. As noted above, the DHS Privacy Office plans to complete the validation of the existing PTAs by the end of October 2006, and plans to have all required PIAs approved by the end of fiscal year 2007.</p>		
OVERALL STEP 1 COMMENTS:		

Appendix F: DHS OIG Response To PCIE Data Collection Instrument

APPENDIX I: IG DATA COLLECTION INSTRUMENT

	REQUIRED RESPONSE	OPTIONAL RESPONSE
Procedure	Yes No Partial Not Applicable	Controls Not Yet in Place Policy Procedures
STEP 2: Has the Agency verified the adequacy of organizational policy? If so, to what level?	Yes	Procedures
Action Item 2.1: Has the Agency identified existing organizational policy that addresses the information protection needs associated with personally identifiable information that is accessed remotely or physically removed?	Yes	
Comments:		
The DHS Office of the Chief Information Officer (CIO) issued Sensitive Systems Policy Directive 4300A and National Security Systems Policy Directive 4300B to provide direction to DHS components regarding the management and protection of sensitive and classified systems, respectively. In addition, the DHS Privacy Office has issued guidance on PIA requirements, and has established templates for the completion of PTAs and PIAs.		
The DHS Office of the CIO, in conjunction with the DHS Privacy Office, updated the department's information security policies and procedures in September 2006 to reflect the recommendations outlined in OMB M-06-16. In addition, DHS has incorporated the policy changes into the department's C&A process through enhancements to DHS' C&A tracking tool, which were completed in August 2006.		
Action Item 2.2: Does the existing Agency organizational policy address the information protection needs associated with personally identifiable information that is accessed remotely or physically removed?	Yes	
1. For Personally Identifiable Information physically removed:		
a. Does the policy explicitly identify the rules for determining whether physical removal is allowed?	Yes	
b. For personally identifiable information that can be removed, does the policy require that information be encrypted and that appropriate procedures, training and accountability measures are in place to ensure that remote use of this encrypted information does not result in bypassing the protection provided by the encryption?	Yes	
2. For Personally Identifiable Information accessed remotely:		
a. Does the policy explicitly identify the rules for determining whether remote access is allowed?	Yes	
b. When remote access is allowed, does the policy require that this access be accomplished via a virtual private network (VPN) connection established using agency-issued authentication certificate(s) or hardware tokens?	Yes	
c. When remote access is allowed, does the policy identify the rules for determining whether download and remote storage of the information is allowed? (For example, the policy could permit remote access to a database, but prohibit downloading and local storage of that database.)	Yes	
Comments:		
DHS has updated its information security policy to reflect the recommendations outlined in OMB M-06-16, including provisions for physical removal of and remote access to PII. The updated policy identifies the rules for determining whether (1) physical removal or downloading of PII is allowed; or, (2) remote access to PII is permitted. In addition, DHS has incorporated the policy changes into the department's C&A process through enhancements to DHS' C&A tracking tool, which were completed in August 2006.		
Action Item 2.3: Has the organizational policy been revised or developed as needed, including steps 3 and 4?	Yes	
Comments:		
DHS has updated its information security policy to reflect the recommendations outlined in OMB M-06-16, including provisions for physical removal of and remote access to PII. The revised policy, which was issued in September 2006, requires the encryption of PII when removed from a DHS facility. Also, the policy requires that remote access to PII be restricted to virtual private networks (VPN) or equivalent encrypted connections that employ two-factor authentication mechanisms based on agency-controlled certificates or hardware tokens issued directly to each authorized user. The updated policy prohibits the remote downloading and storage of PII unless the requirements for the use of removable media with sensitive information have been addressed. Further, the policy requires that all downloads of PII follow the concept of least privilege and be documented in the SSP for the system.		
OVERALL STEP 2 COMMENTS:		

Appendix F: DHS OIG Response To PCIE Data Collection Instrument

APPENDIX I: IG DATA COLLECTION INSTRUMENT

	REQUIRED RESPONSE	OPTIONAL RESPONSE
<i>Procedure</i>	Yes No Partial Not Applicable	<i>Controls Not Yet in Place Policy Procedures Implemented Monitor & Tested Integrated</i>
STEP 3: Has the Agency implemented protections for personally identifiable information being transported and/or stored offsite? If so, to what level?	Partial	Procedures
<i>Action Item 3.1: In the instance where personally identifiable information is transported to a remote site, have the NIST Special Publication 800-53 security controls ensuring that information is transported only in encrypted form been implemented?</i>	Partial	
<i>* Evaluation could include an assessment of tools used to transport PII for use of encryption.</i>		
Comments:		
DHS component organizations have not encrypted PII transported to a remote site. Of the 25 systems included in our review, 21 (84 percent) transported backup media containing PII to an alternate storage facility. For those systems transporting PII offsite, only two (10 percent) encrypted the data during transportation to the alternate facility.		
<i>Action Item 3.2: In the instance where PII is being stored at a remote site, have the NIST SP 800-53 security controls ensuring that information is stored only in encrypted form been implemented?</i>	Partial	
<i>* Evaluation could include a review of remote site facilities and operations.</i>		
Comments:		
DHS component organizations have not encrypted PII stored at a remote site. Of the 25 systems included in our review, 21 (84 percent) transported backup media containing PII to an alternate storage facility. For those systems storing PII offsite, only one (5 percent) encrypted the data while stored at the alternate location.		
OVERALL STEP 3 COMMENTS:		

*If personally identifiable information is to be transported and/or stored offsite
follow Action Item 4.3, otherwise follow Action Item 4.4*

Appendix F: DHS OIG Response To PCIE Data Collection Instrument

APPENDIX I: IG DATA COLLECTION INSTRUMENT

	REQUIRED RESPONSE	OPTIONAL RESPONSE
<i>Procedure</i>	Yes No Partial Not Applicable	<i>Controls Not Yet in Place Policy Procedures Implemented Monitor & Tested Integrated</i>
STEP 4: Has the Agency implemented protections for remote access to personally identifiable information? If so, to what level?	Partial	Procedures
<i>Action Item 4.1: Have NIST Special Publication 800-53 security controls requiring authenticated, virtual private network (VPN) connection been implemented by the Agency?</i>	Yes	
<i>* Evaluation could include a review of the configuration of VPN application(s).</i>		
<i>Comments:</i>		
DHS component organizations use authenticated, virtual private network (VPN) connections for remote access to PII. Of the 25 systems included in our review, 23 (92 percent) systems allowed remote access to PII. All of these systems used an authenticated VPN for remote access connections.		
<i>Action Item 4.2: Have the NIST Special Publication 800-53 security controls enforcing allowed downloading of personally identifiable information been enforced by the Agency?</i>	Yes	
<i>* Evaluation could include a review of controls for downloading PII.</i>		
<i>Comments:</i>		
DHS component organizations have implemented NIST Special Publication (SP) 800-53 controls for the downloading of PII. Of the 25 systems included in our review, 11 (44 percent) allowed users to download PII. Component officials reported that users' ability to download PII and sensitive data was restricted on all of the systems through measures such as the use of role-based access controls based on the principle of least privilege.		
<i>If remote storage of personally identifiable information is to be permitted follow Action Item 4.3, otherwise follow Action Item 4.4.</i>		
<i>Action Item 4.3: Have the NIST Special Publication 800-53 security controls enforcing encrypted remote storage of personally identifiable information been implemented by the Agency?</i>	Partial	
<i>Comments:</i>		
DHS component organizations have not implemented encrypted remote storage of PII. Of the 25 systems included in our review, 11 (44 percent) allowed users to download PII. Component officials reported that encrypted remote storage was enforced on four (36 percent) of the systems through the use of measures such as hard drive encryption on the workstations connecting to the system.		
<i>Action Item 4.4: Has the Agency enforced NIST Special Publication 800-53 security controls enforcing no remote storage of personally identifiable information?</i>	Yes	
<i>Comments:</i>		
Of the 25 systems included in our review, 14 (44 percent) prevented the downloading of PII through measures such as the use of thin clients or restricting user access to screen views of the data.		
OVERALL STEP 4 COMMENTS:		

(The source for all the control steps above is NIST SP 800-53 and SP 800-53A assessment procedures.)

Appendix F: DHS OIG Response To PCIE Data Collection Instrument

APPENDIX I: IG DATA COLLECTION INSTRUMENT

Section Two

Additional Agency Actions Required by OMB M-06-16	
Procedure	Yes No Partial Not Applicable
1. Has the Agency encrypted all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing by Agency Deputy Secretary or an individual he/she may designate in writing?	Partial
<p>Comments:</p> <p>Prior to the issuance of OMB M-06-16, DHS policy required that sensitive information stored on any laptop computer that may be used in a residence or on travel be encrypted using FIPS 140-2-approved encryption. In September 2006, DHS updated this policy to include all mobile computing devices, and to require the encryption of PII when removed from a DHS facility.</p> <p>DHS and its components are in the process of implementing encryption on laptop computers. Specifically, three of the sixteen DHS components ██████████ reported that they had implemented full hard drive encryption on many of their laptop computers. According to component officials, the remaining devices would be encrypted once hardware limitations and inventory issues are resolved, and sufficient software licenses are obtained. ██████████ officials stated that they believed hard drive encryption had been implemented on all laptop computers, but they were not able to confirm that belief. In addition, ██████████ began implementing laptop encryption in September 2006.</p> <p>All of the remaining components reported that they plan to take action to implement encryption on laptop computers. For example, the ██████████ which manages the ██████████ and provides laptop computer support to ██████████ is in the process of implementing full hard drive encryption on laptop computers.</p>	
2. Does the Agency use remote access with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access?	Partial
<p>Comments:</p> <p>In September 2006, DHS updated its information security policy to require that remote access to PII be restricted to VPN or equivalent encrypted connections that employ two-factor authentication mechanisms based on agency-controlled certificates or hardware tokens issued directly to each authorized user. Two-factor authentication for remote access connections to sensitive non-PII data is recommended, but not required.</p> <p>DHS component organizations have not fully implemented two-factor authentication for remote access to sensitive data and PII. Although 23 of the 25 PII systems included in our sample allowed remote access for users or administrators, only 18 (78 percent) used two-factor authentication for access to PII. For those systems using two-factor remote access authentication, seven (37 percent) relied upon a second factor resident on or linked to the computer gaining access, such as a registry identifier on the computer or the computer's internet protocol address. The remaining 11 systems (61 percent) employed hardware tokens or access cards as the second factor.</p>	
3. Does the Agency use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity?	Partial
<p>Comments:</p> <p>Prior to the issuance of OMB M-06-16, DHS policy required that any user sessions be terminated after 20 minutes of inactivity. DHS has also issued guidance on the implementation of passwords and inactivity timeout for Blackberries.</p> <p>DHS component organizations have not fully implemented appropriate session inactivity timeout settings for remote access to sensitive data and PII. Although all of the 25 PII systems included in our sample allowed remote access for users or administrators, only 13 (57 percent) required re-authentication after 20 minutes of inactivity, in accordance with DHS policy. An additional eight systems (35 percent) required re-authentication after 30 minutes of inactivity.</p>	
4. Does the Agency log all computer-readable data extracts from databases holding sensitive information and verifies each extract including sensitive data has been erased within 90 days or its use is still required?	Partial
<p>Comments:</p> <p>In September 2006, DHS updated its information security policy to require components to evaluate the system risks associated with extracts of PII. If the risk is determined to be sufficiently high, components are required to implement a procedure for logging all computer-readable data extracts and for verifying that the extracts have been erased within 90 days unless a need for continued use of the extracts is documented.</p> <p>DHS component organizations have not implemented a process to monitor and delete extracts of sensitive data. For the 25 PII systems included in our sample, 11 (44 percent) allowed users to download sensitive information, but none of these systems had a process in place to verify that extracts including sensitive data are erased within 90 days, or that the extract's use is still required. Further, only one system (4 percent) had a process in place to ensure that computer-readable data extracts made by administrators are erased within 90 days, or that the extract's use is still required.</p>	

Appendix F: DHS OIG Response To PCIE Data Collection Instrument

Section Three

To assist the PCIE/ECIE in evaluating the results provided by individual IGs and in creating the government-wide response, please provide the following information:

Type of work completed (i.e., assessment, evaluation, review, inspection, or audit).

Evaluation

Scope and methodology of work completed based on the PCIE/ECIE review guide Step 2 page 4. (Please address the coverage of your assessment, and include any comments you deem pertinent to placing your results in the proper context.)

We interviewed officials from the DHS Office of the Chief Information Officer (OCIO) and DHS Privacy Office, and reviewed DHS policy and procedure documents related to the protection of PII. In addition, we interviewed DHS component officials and reviewed security documents for a sample of 25 DHS systems that collect, use, or store PII. Finally, we conducted technical testing of the laptop encryption configuration being deployed to five of DHS' sixteen component organizations.

Assessment Methodologies Used to complete the DCI Sections

	Mark All That Apply				
	Section One				Section Two
	Step 1	Step 2	Step 3	Step 4	
Interviews (G/F/C)	C	C	C	C	C
Examinations (G/F/C)	F	F	F	F	F
Tests (independently verified - Y/N)	N	N	N	N	Y

Assessment Method Descriptions consistent with NIST SP 800-53A - Appendix D pages 34 - 36.

G = Generalized. F = Focused. C = Comprehensive. Y = Yes. N = No.

Overall Summary Statement. (Please refer to page five of the review guide for sample language for summary statements.)

DHS and its components are in the process of implementing OMB's recommended security controls for PII, but work remains to ensure that sensitive biographical data is adequately protected. Specifically, although DHS has published updated policies and procedures reflecting the recommendations in OMB M-06-16, DHS components have not implemented the recommended remote access, offsite transportation, remote storage, or encryption security controls.

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or email DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.