

# Audit Report

**IMPROVEMENTS TO THE GSA PRIVACY ACT  
PROGRAM ARE NEEDED TO ENSURE THAT  
PERSONALLY IDENTIFIABLE INFORMATION  
(PII) IS ADEQUATELY PROTECTED  
REPORT NUMBER A060228/O/T/F08007**

March 31, 2008

**Office of Inspector General  
General Services Administration**



**Office of Audits**



U.S. GENERAL SERVICES ADMINISTRATION  
Office of Inspector General

---

Date: March 31, 2008

Reply to: Gwendolyn A. McGowan  
Deputy Assistant Inspector General for Information Technology Audits  
(JA-T)

To: Gail T. Lovelace  
Chief Human Capital Officer (C)

Casey Coleman  
Chief Information Officer (I)

Subject: Improvements to the GSA Privacy Act Program Are Needed to Ensure  
that Personally Identifiable Information (PII) is Adequately Protected  
Report Number A060228/O/T/F08007

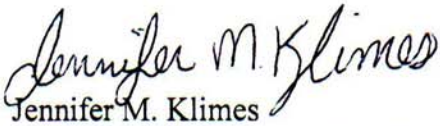
This report presents the results of our review of the General Services Administration's (GSA) Privacy Act Program and select controls for PII. The GSA Privacy Act Program is managed by the Chief Human Capital Officer (CHCO) who is responsible for ensuring that the Agency fulfills the requirements of the Privacy Act of 1974, which was enacted to balance a person's right to privacy with the Federal government's need for information to carry out its responsibilities. The Chief Information Officer (CIO) manages the GSA Information Technology (IT) Security Program, and as such, shares responsibility for protecting PII. The objective of our review was to determine if GSA: (1) manages sensitive personal information pursuant to legal and regulatory requirements, including e-Government provisions for privacy controls; (2) has implemented technical, managerial, and operational privacy-related controls to effectively mitigate risks inherent to Privacy Act systems of records; and (3) has established procedures and automated mechanisms to verify control efficacy. If not, what additional measures are needed to improve protection of such sensitive data at GSA?

Our review found that, while improvements have been made to the GSA Privacy Act Program, additional improved management controls are needed to ensure that PII is consistently protected and to reduce risk of unauthorized or unintentional disclosure of privacy information. Improved management controls, including a program implementation plan to guide the Agency's Privacy Act Program, will help ensure successful coordination of privacy responsibilities at all levels within GSA. Specifically, the Privacy Act Program has not yet ensured that all required privacy controls are in place and operating effectively and that GSA Associates and contractors are fully aware of key roles, responsibilities, and accountability for protecting PII across GSA's IT infrastructure. GSA also needs to ensure that all IT support contracts include the



appropriate privacy related clauses and provide role-based privacy training to GSA Associates and contractors who are responsible for the protection of PII to ensure that they are aware of restrictions on Privacy Act data and their responsibilities for protecting PII. Vulnerability scans performed on a sample of major IT systems that collect and store PII revealed security weaknesses that require management attention, such as the need to consistently apply hardening guides to reduce the risk of inadvertent or unauthorized access to PII and promptly apply software security patches to mitigate the risk of exposure to vulnerabilities and potential unauthorized access to PII. Taking steps to strengthen the GSA Privacy Act Program will ensure that goals for preventing, detecting, and/or recovering from a PII security breach are established and achieved to manage escalating risks in this area.

I wish to express my appreciation to you and your staffs for your cooperation during the audit. If you have any questions, please contact me or Gwen McGowan, Deputy Assistant Inspector General for IT Audits, on 703-308-1223.

A handwritten signature in cursive script that reads "Jennifer M. Klimes".

Jennifer M. Klimes

Audit Manager, Information Technology Audit Officer (JA-T)

IMPROVEMENTS TO THE GSA PRIVACY ACT  
PROGRAM ARE NEEDED TO ENSURE THAT  
PERSONALLY IDENTIFIABLE INFORMATION  
(PII) IS ADEQUATELY PROTECTED  
REPORT NUMBER A060228/O/T/F08007

TABLE OF CONTENTS

	<u>PAGE</u>
EXECUTIVE SUMMARY .....	i
Purpose.....	i
Background.....	ii
Results-in-Brief.....	ii
Recommendations.....	iii
Management Comments .....	iv
INTRODUCTION .....	1
Objectives, Scope, and Methodology .....	2
RESULTS OF AUDIT.....	4
GSA’s Privacy Act Program Has Not Yet Established Needed Safeguards .....	4
Improved Management Controls Are Needed to Guide the Agency’s Privacy Act Program .....	5
Privacy Policies and Procedures Have Not Fully Considered PII Maintained Outside of Major IT Systems that Collect and Store PII.....	7
Appropriate Privacy-Related Clauses Are Needed in All IT Contracts .....	8
Role-Based Training Is Necessary to Clarify Privacy Responsibilities .....	8
System Vulnerability Tests Revealed Weaknesses in Configuration and Patch Management ..	9
System Configuration Settings Improvements Are Needed.....	9
Timely Patch Management Could Reduce Security Vulnerabilities .....	10
Implementing Specific Controls for PII Requires Additional Actions.....	10
Conclusion .....	12
Recommendations.....	13
Management Comments .....	13
Internal Controls .....	14

APPENDICES

Appendix A – GSA Data Collection Instrument .....	A-1
Appendix B – Timeline of GSA Activities Related to Privacy Controls .....	B-1
Appendix C –Vulnerability Scanning Results .....	C-1
Appendix D – CHCO/CIO Consolidated Response to Draft Report.....	D-1
Appendix E – Report Distribution .....	E-1

IMPROVEMENTS TO THE GSA PRIVACY ACT  
PROGRAM ARE NEEDED TO ENSURE THAT  
PERSONALLY IDENTIFIABLE INFORMATION  
(PII) IS ADEQUATELY PROTECTED  
REPORT NUMBER A060228/O/T/F08007

**EXECUTIVE SUMMARY**

**Purpose**

The General Services Administration's (GSA) Chief Human Capital Officer (CHCO) has primary responsibility for the Agency's Privacy Act Program, including development and implementation of privacy data protection policies. The GSA Privacy Act Program is intended to ensure that the Agency fulfills the requirements of the Privacy Act of 1974, which was enacted to balance a person's right to privacy with the Federal Government's need for information to carry out its responsibilities. All Federal agencies are required to establish and implement comprehensive privacy and data protection procedures governing the collection, use, sharing, disclosure, transfer, storage, and security of information in an identifiable form relating to the Agency's employees and the public. The objective of our audit of the Agency's Privacy Act Program was to determine if GSA: (1) manages sensitive personal information pursuant to legal and regulatory requirements, including e-Government provisions for privacy controls; (2) has implemented technical, managerial, and operational privacy-related controls to effectively mitigate risks inherent to Privacy Act systems of records; and (3) has established procedures and automated mechanisms to verify control efficacy. If not, what additional measures are needed to improve protection of such sensitive data at GSA?

The E-Government Act of 2002 addresses privacy protections when citizens interact with the Federal government and was enacted to improve the methods by which government information, including information on the Internet, is organized, preserved, and made accessible to the public. Guidance on implementing the E-Government Act of 2002 directs agencies to conduct reviews of how information about individuals is handled within their agency when they use information technology (IT) to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information (PII). Agencies are also directed to describe how the government handles information that individuals provide electronically, so that the American public has assurances that personal information is protected. With the implementation of the E-Government Act of 2002, agencies are now required to: (1) inform and educate employees and contractors of their responsibility for protecting information in identifiable form; (2) identify those individuals in the agency that have day-to-day responsibility for implementing section 208 of the E-Government Act, the Privacy Act, or other privacy laws and policies; (3) designate an appropriate senior official or officials to serve as the agency's principal contact(s) for information technology/web matters and for privacy policies and coordinate implementation of Office of Management and Budget (OMB) web and privacy policy and guidance; and (4) designate an appropriate official (or officials, as appropriate) to serve as the "reviewing official(s)" for agency Privacy Impact Assessments (PIAs). Additional controls for electronic files, including those that may contain PII are required to manage increasing risks in this area.

To improve safeguards for sensitive information maintained across Federal agencies, OMB issued memorandum M-06-16, Protection of Sensitive Agency Information, on June 23, 2006. The memorandum stresses that Federal agencies need to take all necessary/reasonable measures to swiftly eliminate significant vulnerabilities to the sensitive information entrusted to them. It requires agencies to take certain actions to ensure that safeguards are in place and appropriately reviewed within 45 days (August 7, 2006) from the issuance of the memorandum. In August 2006, the President's Council on Integrity and Efficiency (PCIE)/ Executive Council on Integrity and Efficiency (ECIE) provided a review guide and Data Collection Instrument (DCI) to the Inspectors General (IG) community for use in assessing compliance with OMB requirements for securing sensitive data as identified in M-06-16. We assessed GSA's compliance with OMB M-06-16 as part of this review, and the completed DCI previously provided to the PCIE and the CHCO is included in Appendix A<sup>1</sup>.

## **Background**

OMB defines PII as “information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.”<sup>2</sup> Management activities stress that privacy protection is both a personal and fundamental right of individuals, including GSA Associates, clients, and members of the public, when personal information is collected, maintained, and used by GSA organizations to carry out its responsibilities and provide services. Also, OMB emphasized the need for better protection of PII in OMB Memorandum M-06-16, issued in June 2006, and OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, issued in May 2007. Memorandum M-06-16 stresses the importance of an agency's baseline of privacy activities and requires that agencies properly safeguard their assets while using information technology. The memorandum requires agencies to review their privacy controls against a checklist for protection of remote information and implement additional controls aimed at increased protection of portable devices. Additionally, Memorandum M-07-16 requires that agencies develop and implement a breach notification policy to reduce the risks related to a potential loss of PII or a data breach. The use of social security numbers (SSNs) in agency systems and programs must also be carefully reconsidered to identify instances in which collection or use of PII is superfluous. Appendix B provides a timeline of major milestones related to specific controls required for the protection of PII.

## **Results-in-Brief**

As the GSA Senior Agency Official for Privacy, the CHCO is responsible for establishing and overseeing the Agency's Privacy Act Program and for ensuring compliance with privacy laws, regulations and related Agency policy. With issuance of a benchmark report, the CHCO has

---

<sup>1</sup> Due to sensitive information included in Appendix A, this information is provided only to the Offices of the CHCO and Chief Information Officer.

<sup>2</sup> OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, issued May 2007.

highlighted GSA's use of information in an identifiable form, identified the Agency's privacy and data protection policies and procedures, and required the use of certain technical controls to protect PII. The Office of the CHCO (OCHCO) has worked with the GSA Chief Information Officer (CIO), who manages the Agency's Information Technology (IT) Security Program, to issue a joint instructional letter which introduces Agency-specific policy and direction for protecting PII in GSA IT systems, including associated records of that information, such as printed paper documents or other storage media. GSA also recognizes the need to eliminate unnecessary use of social security numbers in IT systems. However, while improvements have been made to the GSA Privacy Act Program, key components are not yet in place to ensure that PII is adequately protected from inappropriate access or modification. The Privacy Act Program has not yet ensured that all required privacy controls are in place and operating effectively and that GSA Associates and contractors are fully aware of key roles, responsibilities, and accountability for protecting PII across GSA's IT infrastructure. Improved management controls are needed to guide GSA's Privacy Act Program, including a comprehensive assessment of the adequacy of existing controls. Additionally, GSA needs to ensure that all IT support contracts include the appropriate privacy related clauses to ensure that contractors are aware of restrictions on Privacy Act data and their responsibilities for protecting PII. While the OCHCO has provided basic privacy awareness training to the majority of GSA Associates and contractors, role-based privacy training is needed for GSA Associates and contractors who are responsible for the protection of PII. Further, vulnerability scans performed on a sample of GSA's major IT systems that collect and store PII revealed that software security patches have not been consistently and promptly applied, leaving these systems vulnerable to known security weaknesses. In response to evolving requirements aimed at improving the protection of PII, including remote access to and transportation and storage of PII, GSA has taken steps to better protect PII; however, further action is needed to ensure that shared goals for preventing, detecting, and/or recovering from a PII security breach are established and achieved to manage escalating risks in this area.

## **Recommendations**

To better manage risks of unauthorized or unintentional disclosure of personally identifiable information (PII), we recommend that the Chief Human Capital Officer:

- (1) Develop an implementation plan for the Privacy Act Program which identifies key roles, responsibilities, milestones, and management performance measures to achieve long-term improvement goals.
- (2) Work closely with the Chief Information Officer to establish collaborative agency-wide procedures to:
  - (a) Ensure that the Privacy Act Program is integrated with the Agency's security program and assesses risk with and identifies controls for all PII, including PII residing outside of major IT systems.
  - (b) Periodically assess the need for and potential uses of automated content management and data leakage tools or other procedures to assist in identifying and protecting PII within GSA's IT and system environment.

- (c) Confirm that required security hardening guides are being followed and that vulnerabilities are promptly recorded and mitigated for major IT systems that collect and store PII.
  - (d) Implement remaining privacy controls required by M-06-16, including encryption and two-factor authentication for systems maintaining PII.
  - (e) Develop a plan that includes the key activities, milestones, and performance measures necessary to guide GSA in discontinuing the collection and storage of social security numbers in IT systems where no longer required.
- (3) Work with the Office of the Chief Acquisition Officer to review contracts in support of major IT systems that collect and store PII to ensure that the appropriate privacy clauses have been included and that contractors supporting GSA's IT systems that collect and store PII are aware of and fulfill their roles and responsibilities for protecting GSA's PII.
- (4) Complete development and implementation of role-based training for GSA Associates and contractors who are responsible for protecting sensitive information, including PII.

### **Management Comments**

The CHCO and CIO provided consolidated management comments on March 28, 2008 on specific audit findings and recommendations in response to our draft report. The comments indicate a general concurrence with our audit findings and recommendations, and a copy of the comments is included as Appendix D. The CHCO and the CIO agreed with our recommendation to develop an implementation plan for the Privacy Act Program which identifies key roles, responsibilities, milestones, and management performance measures to achieve long-term improvement goals. Management also acknowledged the need to do more to protect PII and identified planned actions to meet audit recommendations. Management comments indicate that the CHCO will work closer with the OCIO to ensure that hardening guides are being appropriately applied and that the CHCO is working with the Office of Procurement Management Review, Office of Acquisition Integrity to randomly audit Privacy Act systems to ensure that the proper FAR clauses are included. In response to our recommendation to implement remaining privacy controls required by OMB Memorandum M-06-16, management comments provided additional information on the status of two of the three remaining requirements. The response also stated that GSA was unaware of a technical means to log all computer-readable data extracts from databases holding sensitive information and verify that each extract including sensitive data has been erased within 90 days or its use is still required. While management comments explained that some manual processes are being used in a limited capacity to support this requirement, we reaffirm the importance of determining an automated method to implement this control.

Management comments highlight activities recently completed and planned related to our recommendation to develop a plan that includes key activities, milestones, and performance measures necessary to guide GSA is discontinuing the collection and storage of SSNs in IT systems where no longer required. In response to our recommendation to complete development and implementation of role-based training for GSA Associates and contractors responsible for protecting sensitive information, including PII, management comments discuss goals to begin role-based training and highlight a 95% completion rate of the Privacy Awareness training over the past year. Management comments in response to our recommendation to assess the need for



and potential uses of automated content management and data leakage tools or other procedures to assist in identifying and protecting PII within GSA's IT and system environment explain that the OCIO is currently evaluating data leakage prevention tools to assist in identifying and protecting PII within GSA's IT and system environment. While evaluating automated content and data leakage tools is a first step toward better protecting PII stored outside of IT systems that maintain Privacy Act data, our audit found that the Privacy Act Program has not yet ensured that PII stored on laptops and servers or in databases or applications that are not considered part of a major IT system is identified and protected as needed. Over the past year we identified numerous instances where PII stored outside of major IT systems was placed at undue risk. Therefore, we reaffirm the need to better ensure that all PII in GSA's IT systems environment be identified and properly protected from unauthorized access, modification, and disclosure.

IMPROVEMENTS TO THE GSA PRIVACY ACT  
PROGRAM ARE NEEDED TO ENSURE THAT  
PERSONALLY IDENTIFIABLE INFORMATION  
(PII) IS ADEQUATELY PROTECTED  
REPORT NUMBER A060228/O/T/F08007

**INTRODUCTION**

The Office of Management and Budget (OMB) has defined personally identifiable information (PII) as “information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.” Information systems containing PII can be either electronic or manual. Various laws and regulations address the need to protect sensitive information held by government agencies, specifically the Privacy Act of 1974 (and revisions), the E-Government Act of 2002 [including the Federal Information Security Management Act (FISMA)], and related OMB circulars and memoranda.

In January 2003, the General Services Administration (GSA) Office of Inspector General (OIG) Information Technology (IT) Audit Office issued a report<sup>3</sup> on controls for the General Services Administration's (GSA) privacy data. At that time, we found that: (1) controls for GSA's sensitive data needed to be more robust to adequately address risks in an automated business environment; (2) roles and responsibilities for protecting Privacy Act data from unauthorized disclosure may not have been effectively communicated; (3) online security training required for GSA Associates and contractors in 2002 did not cover Privacy Act requirements or restrictions on unauthorized disclosures of personal information entrusted to those who work with sensitive files; (4) GSA IT service contracts did not state the need to protect Privacy Act data and failed to specify restrictions or penalties for unauthorized disclosures; (5) periodic review of web server content would strengthen controls to prevent improper disclosure of Privacy Act data on GSA web servers located outside the firewall, as well as those accessible within GSA; and (6) the list of Systems of Records was not up-to-date and comprehensive. We recommended that the Chief People Officer (CPO)<sup>4</sup> work closely with the Chief Information Officer (CIO) to improve the management of GSA's Privacy Act data by: (1) coordinating with the Office of Acquisition Policy to ensure that appropriate Privacy Act requirement clauses are included in IT support contracts utilized by GSA and that roles and responsibilities for the protection of sensitive data are made explicit for contractors entrusted with such data, (2) updating GSA's Systems of Records list, and (3) ensuring that accountability and responsibility is assigned for identifying and implementing specific controls for each of GSA's Systems of Records.

In January 2006<sup>5</sup>, we completed an implementation review of management actions taken on the three recommendations in the 2003 audit report. We found that management had taken actions in accordance with the time-phased action plan provided in response to our 2003 report;

---

<sup>3</sup> Review of Controls for GSA's Privacy Act Data, Report Number A020256/O/T/F03005, dated January 6, 2003.

<sup>4</sup> The GSA CPO was officially renamed the Chief Human Capital Officer (CHCO) in October 2006.

<sup>5</sup> Implementation Review of Controls for GSA's Privacy Act Data, Report Number A020256/O/T/F03005, dated January 6, 2003, Assignment Number A060045, dated January 18, 2006.

however, conditions raised in the initial report remained. Contracts for two of the three systems we reviewed did not include appropriate Federal Acquisition Regulation (FAR) clauses for Privacy Act systems, and GSA's list of Privacy Act systems, maintained by the Office of the Chief Human Capital Officer (OCHCO), was still not complete. Further, clear roles and responsibilities for GSA Associates and contractors were not yet established across GSA, and training had not been provided to ensure that responsible individuals were aware of requirements for protecting GSA Privacy Act data.

### **Objectives, Scope, and Methodology**

The objective of our review of the Agency's Privacy Act Program was to determine if GSA: (1) manages sensitive personal information pursuant to legal and regulatory requirements, including e-Government provisions for privacy controls; (2) has implemented technical, managerial, and operational privacy-related controls to effectively mitigate risks inherent to Privacy Act Systems of Records; and (3) has established procedures and automated mechanisms to verify control efficacy. If not, what additional measures are needed to improve protection of sensitive data? We gathered information related to actions that GSA has taken to protect PII prior to and in response to OMB Memorandum M-06-16 and considered recently developed Agency policy regarding the protection of sensitive information. We considered the Agency's mandatory on-line privacy training, information disseminated through the Privacy Act Program internal and external websites, and an Information Paper on the actions taken by GSA to meet the requirements of M-06-16. We also reviewed a GSA report responding to OMB Memorandum M-06-20 and Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005. We interviewed appropriate staff from GSA's OCHCO and OCIO with key responsibilities for ensuring the protection of PII. We also provided input based on the audit work completed during this review for the OIG response to privacy questions as part of its annual reporting on FISMA for fiscal year (FY) 2007<sup>6</sup>.

During audit survey, we reviewed security documentation for seven major IT systems that collect and store PII, including analyzing the security plans for GSAJobs, the Excluded Parties List System (EPLS), the System for Tracking and Administering Real-Property (STAR), and the EDS e-Travel System (EDS), and the risk assessments for the STAR, FedBizOps (FBO), the Carlson Wagonlit e-Travel System (CWGT), and the Northrup Grumman Mission System e-Travel System (NGMS) against the National Institute of Standards and Technology (NIST) Guide for Developing Security Plans for Information Technology Systems, Special Publication (SP) 800-18 and the NIST Risk Management Guide for Information Technology Systems SP 800-30, respectively. We also reviewed Privacy Impact Assessments for FBO, the Federal Procurement Data System – Next Generation (FPDS-NG) and STAR for adequacy. During audit fieldwork, we interviewed system security officials, examined system privacy and security documentation, and used commercially available tools and agreed upon procedures to complete network security scanning and examine database configuration for three of GSA's major IT systems that collect and store PII – STAR, FBO, and CWGT. Web application security scanning was also performed on FBO. Automated techniques were used to verify the degree of implementation of GSA's

---

<sup>6</sup> FY 2007 Office of Inspector General FISMA Review of GSA's Information Technology Security Program, Report Number A070108/O/T/F07015, dated September 17, 2007.

hardening guides, and we tested NIST SP 800-53 controls related to privacy, selecting a subset of controls from eight of the 17 control families.

To assess managerial, operational, and technical PII controls for the Privacy Act Program and for the three systems tested, we relied on applicable statutes, regulations, policies, and operating procedures, such as: the GSA Information Technology Security Policy, CIO P 2100.1D, June 2007; GSA Privacy Act Program, CPO 1878.1, October 2003; Conducting Privacy Impact Assessments (PIAs) in GSA, CPO 1878.2, May 2004; Safeguarding Personally Identifiable Information, CIO IL-06-02, August 2006; Federal Information Processing Standards Publication (FIPS PUB) 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004; FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006; NIST SP 800-53, Recommended Security Controls for Federal Information Systems, February 2005; NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categorization Levels, June 2004; Public Law 107-347, E-Government Act of 2002; OMB Circular A-130, Management of Federal Information Resources, November 2000; the Privacy Act of 1974; the Federal Information Security Management Act of 2002; and the GSA CIO's IT procedural guides on password generation and protection, managing enterprise risk, access control, media sanitization, and auditing and monitoring. We also referenced OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 23, 2006; OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 2003; OMB Memorandum M-03-18, Implementation Guidance for the E-Government Act of 2002, August 2003; OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, July 2006; and OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, May 2006.

We conducted this performance audit work in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The scope of our work did not assess the accuracy and integrity of the data within the three Privacy Act systems tested or consider controls for paper-based Systems of Records<sup>7</sup>.

---

<sup>7</sup> According to the Privacy Act of 1974, a "System of Record" is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

## **RESULTS OF AUDIT**

As the GSA Senior Agency Official for Privacy, the CHCO is responsible for establishing and overseeing the Agency's Privacy Act Program and for ensuring compliance with privacy laws, regulations and related Agency policy. With issuance of a benchmark report, the CHCO has highlighted GSA's use of information in an identifiable form, identified the Agency's privacy and data protection policies and procedures, and required the use of certain technical controls to protect PII. The OCHCO has worked with the GSA-CIO, who manages the Agency's IT Security Program, to issue a joint instructional letter which introduces Agency-specific policy and direction for protecting PII in GSA IT systems, including associated records of that information, such as printed paper documents or other storage media. GSA also recognizes the need to eliminate unnecessary use of social security numbers in IT systems. However, while improvements have been made to the GSA Privacy Act Program, key components are not yet in place to ensure that PII is adequately protected from inappropriate access or modification. The Privacy Act Program has not yet ensured that all required privacy controls are in place and operating effectively and that GSA Associates and contractors are fully aware of key roles, responsibilities, and accountability for protecting PII across GSA's IT infrastructure. Improved management controls are needed to guide GSA's Privacy Act Program, including a comprehensive assessment of the adequacy of existing controls. Additionally, GSA needs to ensure that all IT support contracts include the appropriate privacy related clauses to ensure that contractors are aware of restrictions on Privacy Act data and their responsibilities for protecting PII. While the OCHCO has provided basic privacy awareness training to the majority of GSA Associates and contractors, role-based privacy training is needed for GSA Associates and contractors who are responsible for the protection of PII. Further, vulnerability scans performed on a sample of major IT systems that collect and store PII revealed that software security patches have not been consistently and promptly applied, leaving these systems vulnerable to known security weaknesses. In response to evolving requirements aimed at improving the protection of PII and other sensitive information, including remote access to and transportation and storage of PII, GSA has taken steps to better protect PII; however, further action is needed to ensure that shared goals for preventing, detecting, and/or recovering from a PII security breach are established and achieved to manage escalating risks in this area.

### **GSA's Privacy Act Program Has Not Yet Established Needed Safeguards**

GSA's Privacy Act Program is intended to ensure that the Agency fulfills the requirements of the Privacy Act of 1974 and provides privacy and data protection procedures governing the collection, use, sharing, disclosure, transfer, storage, and security of information in an identifiable form relating to the Agency's employees and the public. However, improved management controls are needed to guide GSA's Privacy Act Program, including a comprehensive assessment of the adequacy of existing controls. Further, policies and procedures established with the Privacy Act Program have not fully considered PII that may be maintained across GSA's broader IT system environment, including PII stored outside of major IT systems that collect and store PII. Additionally, GSA needs to ensure that all IT support contracts include the appropriate privacy related clauses to ensure that contractors are aware of restrictions on Privacy Act data and their responsibilities for protecting PII. While basic privacy awareness training has been provided to all GSA Associates and contractors, role-based training for

specialized job functions that handle PII, such as Human Resource Specialists and Payroll Specialists, is needed. This training would help ensure that all individuals with significant responsibilities related to PII are informed of risks and that required controls for the protection of Privacy Act information are in place and operating as intended.

### Improved Management Controls Are Needed to Guide the Agency's Privacy Act Program

Within GSA, primary management control responsibilities for protecting sensitive information, including PII, are dispersed among several key officials. The CHCO is the Senior Agency Official for Privacy, the GSA official responsible for establishing and overseeing the Agency's Privacy Act Program and for ensuring GSA's compliance with privacy laws, regulations and GSA policy. GSA's CIO has overall responsibility for the Agency's IT Security Program and the IT Capital Planning Program. As such, the CIO develops and implements security controls for Privacy Act data by reviewing Privacy Impact Assessments (PIAs) that are prepared by GSA Service and Staff Offices for security considerations for IT systems. The CIO is also responsible for verifying that the development of PIAs is a part of GSA's IT Capital Planning and Investment Control Policy. System Authorizing Officials (AOs) also carry out key responsibilities for securing IT systems under their jurisdiction. Specifically, AOs are responsible for reviewing and approving PIAs for their organizations and for ensuring that identified Privacy Act systems that handle privacy data meet information privacy and security requirements. They also review existing and proposed IT Privacy Act systems in their organizations to assess the need to conduct a PIA, coordinate the preparation of the PIA with program and system managers, and approve the PIA for their organizations

Following OMB M-06-15, Safeguarding Personally Identifiable Information, issued May 2006, the OCHCO, as GSA's designated Senior Agency Official for Privacy, took steps to review the Agency's policies and processes, identify any deficiencies, and take corrective action as appropriate to ensure it has adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to PII. In August 2006, a joint instructional letter<sup>8</sup> from the GSA-CIO, who manages the Agency's IT Security Program, and the CHCO introduced Agency-specific policy and direction for protecting PII in GSA IT systems, including associated records of that information, such as printed paper documents or other storage media. This instructional letter established security requirements beyond those established with GSA's IT Security Program to specifically address risks with PII. Also, in August 2006, the OCHCO issued a benchmark report on GSA's Privacy Act Program in response to Section 522 requirements within the Appropriations Act of 2005. The benchmark report discusses GSA's use of information in an identifiable form, identifies the Agency's privacy and data protection policies and procedures, and requires the use of certain technical controls. This report was provided to OMB as part of the Agency's response to specific privacy control questions required with FISMA for FY 2006. Policies and procedures referenced in the report include controls established with GSA's IT Security Program. The Privacy Benchmark Report, however, did not: (1) comprehensively address the adequacy of the implementation of existing controls in GSA PII systems, including those established with the Agency IT Security Program; (2) identify deficiencies or improvement goals for the Privacy Act Program; or (3) develop a plan for improving the existing Privacy Act Program. A comprehensive agency-wide assessment, as required by M-06-15, is needed for

---

<sup>8</sup> Safeguarding Personally Identifiable Information, CIO IL-06-02, issued August 2006.

GSA to adequately ensure that required privacy controls have been implemented and that the controls are operating as intended for both manual and automated systems across GSA.

In September 2007, when responding to specific privacy related FISMA questions raised by OMB, we completed a qualitative assessment of the Agency's (1) Privacy Impact Assessment (PIA) process, including adherence to existing policy, guidance, and standards, and (2) progress to date in implementing the provisions of M-06-15. As part of our assessment, we considered actions and activities undertaken since the Agency's 2006 self-review, including the Agency's policies and processes, and the administrative, technical, and physical means used to control and protect PII. With our annual 2007 FISMA audit report<sup>9</sup>, we discussed progress made to date, including GSA's appointment of a Senior Agency Official for Privacy, completion of the privacy benchmark report, updates to the IT Security Policy to reflect privacy requirements, and implementation of a PIA process. We also considered outstanding goals to develop and implement controls for encryption of PII stored on mobile devices or for accessing PII from personally owned computers. We concluded that a comprehensive agency-wide assessment of the adequacy of existing privacy controls for PII, including clarification of primary roles and responsibilities for verifying the implementation of those controls, is a necessary step in moving toward common goals and processes for the protection of PII. Our review of contracts for a sample of IT systems that collect and store PII also found that contracts for systems with PII do not yet consistently include privacy-related FAR clauses. Further, security related patches have not been consistently applied to automated systems, leaving some databases vulnerable to known security threats.

While improvements have been made to the GSA Privacy Act Program with increased controls for PII, GSA has not comprehensively assessed the adequacy of implementation for existing privacy controls in GSA PII systems and key roles and responsibilities for verifying the implementation of those controls have not been documented. To promote the establishment of improved policies and procedures to manage risk with PII, it is important that GSA clearly communicate its long-term goals and milestones to guide the Privacy Act Program. While responsibilities for protecting PII lie with various entities in GSA, a program implementation plan highlighting key milestones and performance goals and measures is not in place to guide the various players in implementing GSA's Privacy Act Program. Accountability is important for the success of GSA's Privacy Act Program and should guide a program implementation plan that will assist with managing and protecting GSA's PII. A program implementation plan would further guide coordination amongst key officials responsible for privacy data and ensure these officials accurately reflect agency-wide privacy policies and procedures. Such a plan would identify all key players involved in implementing the Privacy Act Program and identify necessary communication activities and information flows to protect PII. Improved management controls, including a program implementation plan to guide the Agency's Privacy Act Program, are needed to ensure successful coordination of privacy responsibilities at all levels within GSA.

---

<sup>9</sup> FY 2007 Office of Inspector General FISMA Review of GSA's Information Technology Security Program, Report Number A070108/O/T/F07015, dated September 17, 2007.

## Privacy Policies and Procedures Have Not Fully Considered PII Maintained Outside of Major IT Systems that Collect and Store PII

For the FY 2007 timeframe, GSA's Privacy Act Program identified 18 major IT systems that collect and store PII. Specific IT controls required for PII include policy stating that employees shall not remove PII from GSA facilities or access PII remotely unless approved in writing and that PII shall not be stored on or accessed from personally owned computers or personally owned mobile devices. GSA's IT Security Policy also states that PII shall be stored on network drives and/or in application databases with proper access controls and shall be made available only to those individuals with a valid need to know and that encryption is required when exchanging PII via e-mail or when stored on workstations or mobile devices. However, the Privacy Act Program has not yet ensured that PII stored on laptops and servers or in databases or applications that are not considered part of a major IT system is identified and protected. Specifically, over the past year we have identified numerous instances where PII stored outside of major IT systems was placed at undue risk. Controls for GSA's Privacy Act data could be more robust to better address known risks associated with all PII, including PII stored outside of major IT systems that collect and store PII. Technical controls, such as automated content management and data leakage technologies are readily available, and the use of such tools to facilitate the identification or storage of PII across GSA's entire system environment is currently being evaluated by the OCIO. Until such tools are provided to system officials responsible for privacy controls, compensating controls and mechanisms (manual or automated) should be considered to identify and protect PII stored outside of major IT systems throughout GSA's IT infrastructure.

Many of the recent OMB Memoranda, including OMB Memorandum M-06-16 and an OMB Memorandum titled the "Top 10 Risks Impeding the Adequate Protection of Government Information," stipulate specific actions that should be taken to protect sensitive information. While the joint instructional letter issued by the CHCO and the CIO initially was provided to establish additional policy and direction for protecting PII in IT systems and any associated record, the current CIO IT Security Policy with updated security requirements does not address privacy controls for PII that is stored outside of major IT systems. Such controls are needed to address the risk inherent with PII stored and transmitted across and outside the GSA IT infrastructure. In September 2007, we identified two privacy control vulnerabilities where we were able to access social security numbers (SSNs) for several Federal government employees and owners of sole proprietorship operated businesses on a website accessible through GSA's Intranet. Over the past few months, we also discovered that access controls were not adequately assessed to ensure the appropriate level of protection for databases that contain PII for two Privacy Act systems using the Business Objects reporting software<sup>10</sup>. In one instance, an authorized user from a client agency, while utilizing one of the Business Objects reporting tools, was able to produce a report that displayed over 40,000 employee records containing sensitive employee data for several agencies, including GSA. We also recently reported<sup>11</sup> to the GSA-CIO that Lotus Notes databases were developed and implemented without having appropriate access controls in place to prevent unauthorized access to PII, including date of birth, name, and

---

<sup>10</sup>The Business Objects utility is a commercial off the shelf product that is used to run queries and reports against databases.

<sup>11</sup> Alert Report on Security of GSA's Electronic Messaging Services (GEMS) and National Notes Infrastructure (GNND), Report Number A070180/O/T/W07001, dated September 12, 2007.



SSN. The OCIO has begun taking steps to remediate reported vulnerabilities for the Agency's Lotus Notes databases; however, these examples, together, demonstrate the need to ensure that effective controls are in place to better protect PII, including PII that is stored outside systems designated as major IT systems, from unauthorized disclosure and access and to preserve authorized access restrictions.

#### Appropriate Privacy-Related Clauses Are Needed in All IT Contracts

In 2003, we reported the need to place restrictions or penalties on unauthorized disclosures and for GSA IT service contracts to specifically state requirements to protect Privacy Act data. Since then, the Office of Acquisition Policy has developed contract clauses in the Federal Acquisition Regulations (FAR) to cover Privacy Act information. According to the FAR, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function, the contracting officer shall insert the following clauses in solicitations and contracts: (a) The clause at 52.224-1, Privacy Act Notification and (b) The clause at 52.224-2, Privacy Act. The GSA IT Security Policy, updated in June 2007, states that all GSA contracts and Request for Proposals (RFP) involving Privacy Act information must adhere to the FAR Privacy Act provisions and include the specified contract clauses, as appropriate, to ensure that personal information and the system data are protected as mandated, by contractors who work on GSA-owned IT systems. However, based on our analysis, IT support contracts for GSA systems with PII still do not consistently include the required privacy-related FAR clauses. During an implementation review of the recommendations from our previous report, we analyzed four IT support contracts for three major IT systems that collect and store PII – the Payroll Accounting and Reporting (PAR) system, GSAJobs, and the Comprehensive Human Resources Integrated System (CHRIS) - and found that two of the contracts did not include or reference the requisite FAR clauses. In 2007, we analyzed IT support contracts for three additional Privacy Act systems – STAR, CWGT, and FBO. Two of these three IT support contracts did not include or reference the appropriate FAR clauses related to privacy. We were informed that the Office of the Chief Acquisition Officer (OCAO) Office of Acquisition Integrity has agreed to work with the OCHCO Information Resources and Privacy Management Division during FY 2008 to review a sample of contracts for major IT systems that collect and store PII to verify whether or not the contracts include the appropriate privacy-related FAR clauses. Without the assurance of adequate contract provisions for protecting Privacy Act data required for these important systems, GSA cannot be sure that contractors are aware of restrictions on Privacy Act data and their responsibilities for protecting PII. Such provisions are also needed to adequately prepare for a potential PII security breach and to respond effectively as needed to manage the consequences of unauthorized access to PII, including the threat of identity theft.

#### Role-Based Training Is Necessary to Clarify Privacy Responsibilities

Tightened IT security and data privacy is intended to better protect sensitive information, including PII that can be easily transported outside Federal buildings. However, it is essential that GSA Associates and contractors, who are increasingly relied on and entrusted with access to Privacy Act data, fully understand the need to safeguard PII and that those with significant privacy responsibilities agree to protect such sensitive data. While GSA has provided basic privacy awareness training to the majority of GSA Associates and contractors, this training did

not address OMB Memorandum M-06-16 requirements regarding the protection of remote access, storage, and transportation of PII. Role-based privacy training, which would provide job-specific and comprehensive information privacy training for all GSA Associates and contractors directly involved in the administration of personal information, has not yet been provided. Initially, OCHCO planned to implement role-based privacy training in 2006; however, the training has been postponed. The OCHCO now plans to begin role-based privacy training in early 2008. This training is intended to provide best practices for handling and disseminating PII and will be made available to persons whose jobs require the handling and use of PII, such as Human Resource Specialists and Payroll Specialists. Without sufficient role-based privacy training for GSA Associates and contractors responsible for the protection of PII, this sensitive information may not be adequately protected from unauthorized or unintentional disclosure and/or modification.

### **System Vulnerability Tests Revealed Weaknesses in Configuration and Patch Management**

We applied commercially available tools, manual techniques, and agreed upon procedures to test controls for three of GSA's major IT systems that collect and store PII<sup>12</sup>. Testing included conducting network security scans, examining database configuration, and reviewing web application security. We found that improvements in system configuration settings and timely patch management are needed to secure these systems and protect PII. Specific vulnerabilities for the three major IT systems tested are included in Appendix C. Due to the sensitive nature of the information contained in this appendix, only reports provided to the Offices of the CHCO and CIO contain detailed scanning results.

#### **System Configuration Settings Improvements Are Needed**

Configuration management provides a structured methodology for applying technical and administrative changes and monitors the results of changes throughout the resource life cycle. Configuration management provides assurance that the IT resource in operation is the correct version (configuration) and changes to be made are reviewed for security implications prior to implementation. Configuration management helps ensure changes to IT systems take place in an identifiable and controlled environment and do not unintentionally harm any of the IT resource's properties, including its security. Changes to the IT resource have security implications because they may introduce or remove vulnerabilities and because changes require updating of IT Security documentation (e.g. contingency plan, risk assessment, etc.), and may impact accreditation. Configuration management weaknesses were found within the hardware, software, and database platforms for all three of the GSA major IT systems that collect and store PII selected for testing. On one of the systems tested, much of the hardware had reached its end-of-life (EOL) date and is no longer supported by the manufacturer. The operating system and the database management system (DBMS) could not be upgraded due to compatibility issues, and many of the latest software patches and security enhancements could not be installed, exposing the system to many known vulnerabilities. Operating system patches were also needed in another system to correct outdated and vulnerable mail service software. Unnecessary services were found on two systems, leaving potential entry points for unauthorized access.

---

<sup>12</sup> The systems tested during this review were the System for Tracking and Administering Real-Property (STAR), FedBizOps (FBO), and the Carlson Wagonlit e-Travel System (CWGT).

Configuration weaknesses were also found in one of the web-based applications tested. Two of these weaknesses provided information that could have assisted an unauthorized user in performing a malicious attack and allowed users to create weak passwords. Controls should be in place to ensure that GSA's systems are appropriately hardened to reduce risk of inadvertent or unauthorized access to PII.

#### Timely Patch Management Could Reduce Security Vulnerabilities

Technical scanning conducted on the same three systems indicated that the periodic cumulative DBMS patches have not been applied in a timely fashion, exposing these systems to numerous known vulnerabilities. For example, testing conducted on February 26, 2007 revealed that one of GSA's systems using a Sybase DBMS had not yet applied a cumulative patch released on April 14, 2006, 10 months after the patch was released. Tests performed on March 15, 2007 indicated that one of GSA's Oracle DBMS-based systems had not yet applied an Oracle critical update released in July 2005, approximately 20 months after the patch was released. Scans performed against another GSA Oracle DBMS-based system, performed on April 23, 2007, indicated that Oracle critical updates released in January 2007 had not been installed and were scheduled for installation on the production database in October 2007, 10 months after the patch was released<sup>13</sup>. Timely patch management is needed to mitigate the risk of exposure to known vulnerabilities and potential unauthorized access to PII in Agency major IT systems that collect and store PII.

#### Implementing Specific Controls for PII Requires Additional Actions

Over the past two years, OMB memoranda have highlighted the importance of privacy officers in Federal agencies, including specific actions intended to better protect PII. OMB memoranda addressed to heads of agencies and departments, include M-06-16, issued in June 2006, and M-07-16, issued in May 2007. M-06-16 requires that agencies assess their baseline of privacy activities and properly safeguard their assets while using information technology to compensate for the lack of physical security controls when information is removed from, or accessed from outside the agency location. Specifically, agencies are to review their privacy controls against a checklist for protection of remote information and implement four additional controls within 45 days of the issuance of the memorandum. M-07-16 requires that agencies develop and implement a breach notification policy to outline the framework within each agency for ensuring that the proper safeguards are in place to protect sensitive information within 120 days from the date of the memorandum. To address increased risk with PII, the use of social security numbers (SSNs) in agency systems and programs should be carefully reassessed to identify instances in which collection or use of the SSN is superfluous. OMB requires a plan to guide in the elimination of unnecessary collection and use of SSNs within 18 months. Although GSA has made progress toward implementing better safeguards for protecting PII and in meeting new privacy requirements, additional actions are needed to establish such important controls required to manage the escalating risks with PII.

OMB Memorandum M-06-16 directed all departments and agencies to take the following actions: (1) encrypt all data on mobile computers/devices which carry agency data unless the

---

<sup>13</sup> We confirmed that these updates were applied with a patch in October 2007, as intended.

data is determined to be non-sensitive, in writing, by the agency Deputy Secretary or an individual he/she may designate in writing; (2) allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access; (3) use a “time-out” function for remote access and mobile devices requiring user re-authentication after 30 minutes of inactivity; and (4) log all computer-readable data extracts from databases holding sensitive information and verify that each extract including sensitive data has been erased within 90 days or its use is still required. While the GSA-CIO IT Security Policy requires that all four requirements from M-06-16 be implemented in GSA’s IT systems, almost one and a half years after the controls were to be implemented, three of the four provisions have not been fully implemented. Specifically, GSA has not yet implemented an encryption solution to force users to encrypt PII stored on GSA user workstations or mobile devices. GSA is in the process of preparing a deployment schedule for an encryption solution called Credant. According to officials in the OCIO, the infrastructure is in place to deploy the solution, and GSA plans to complete a pilot of the technology before the full-scale deployment. The initial version of Credant that GSA planned to implement did not allow for automatic encryption of USB devices<sup>14</sup>, however, according to GSA CIO’s office, a new version has recently been released that has made USB encryption policies easier to implement. GSA plans to implement this version in the spring of 2008, along with the laptop rollout. Without enforcement of these controls, either automated or through other compensating measures, it is up to the individual user to ensure that PII is encrypted as required. In addition, two-factor authentication for electronic portable devices that contain PII, where one of the factors is provided by a device separate from the computer gaining access, has not yet been implemented. Rather than investing significant resources to develop and implement a solution for two-factor authentication that may not be in compliance with Homeland Security Presidential Directive (HSPD)-12, GSA plans to address this requirement with its HSPD-12 solution. GSA has tested a two-factor authentication solution and is working on the standard for readers on the desktops and laptops for a pilot, planned for approximately 50 users. Further, GSA has not implemented the control requiring that computer-readable data extracts from databases holding PII be logged and erased within 90 days unless its use is still required, as officials have stated that they are unaware of any immediate viable solution to implement this control.

In assessing the Agency’s adherence to the security checklist provided with OMB Memorandum M-06-16, we found that GSA has implemented controls for confirming the identification of PII protection needs. GSA has also partially implemented controls for verifying the adequacy of organizational policy and protecting the transportation and remote storage of and remote access to PII. However, these controls are being provided primarily at the policy and/or procedures level and have not been fully implemented with GSA’s PII systems and extended IT infrastructure. Agency-wide responsibility for ensuring that these controls have been implemented per privacy policy has not yet been established, and GSA has not yet implemented the following controls: (1) controls enforcing no remote storage/transportation of and no remote access to PII, when not permitted; (2) controls enforcing that remote transportation/storage of and remote access to PII be encrypted; and (3) controls enforcing allowed downloading of PII.

Further, OMB Memorandum M-07-16 identified additional controls required for PII and specifies that responsibility for safeguarding PII is shared by officials accountable for

---

<sup>14</sup> A USB device is a mobile storage device that could be used to store sensitive information.

administering operational and privacy and security programs, legal counsel, Agencies' Inspectors General and other law enforcement, and public and legislative affairs. The memorandum requires that agencies implement a breach notification policy and outlines a framework to ensure that the proper safeguards are in place to protect privacy information. It also requires that agencies reassess the need to collect and use SSNs within IT systems and develop a plan to eliminate the use and collection of SSNs where superfluous. The Agency has been working to meet the requirements of M-07-16 and has issued an Information Breach Notification Policy<sup>15</sup> via an instructional letter on September 21, 2007 to provide policy on what actions should be taken when it is determined that PII has been compromised. GSA has identified initial milestones for collecting information from system owners on whether their system collects SSNs and, if so, for what purpose. System owners were also asked what impact discontinued use of SSNs may have on their systems. By the end of December 2007, GSA was to make decisions as to which specific systems need to continue to collect/use SSNs. GSA recognizes the need to lessen the use of SSNs but also realizes that some systems will not be able to function without collecting this data element. While GSA has made initial efforts in determining how to reduce the collection and use of SSNs, a detailed plan that identifies key activities, milestones, and performance measures to remove use of SSNs, where superfluous, has not yet been developed. Although GSA has made progress toward implementing better safeguards for protecting PII and in meeting new privacy requirements, additional actions are needed to establish required privacy controls and manage the escalating risks with PII to ensure that PII is not put at risk of unauthorized or unintentional disclosure.

## **Conclusion**

Within GSA, the CIO and CHCO share responsibility and accountability for developing, implementing and administering the Agency's controls for protecting PII. Additionally, the Office of Acquisition Policy within the OCAO is responsible for developing, coordinating, and obtaining the required public comments and clearance on FAR clauses related to privacy and the protection of sensitive personal information. GSA has taken steps toward improving the protection of PII, including revisions to the GSA IT Security Policy to provide additional safeguards for PII and the implementation of a Privacy Act Program that identifies roles and responsibilities for protecting PII. GSA has also established a minimum level of controls required for Privacy Act systems which address specific PII challenges, including the potential of unauthorized or unintentional disclosure of privacy information. However, improvements to the GSA Privacy Act Program are needed to ensure that PII is consistently protected and that risk of unauthorized or unintentional disclosure to such sensitive information is further reduced. Employing effective controls to protect PII data across the Agency's system environment, whether the information is stored within an information system or on network or removable storage devices, is necessary to ensure that GSA Associates and contractors have a clear understanding of both the technical and human aspects of securing privacy information as well as acknowledging the need to address not only what is required by law but also what is expected by Agency policy. An effective Privacy Act Program would also verify that required controls have been implemented and ensure that GSA Associates and contractors have received both basic privacy awareness training as well as specialized role-based or job-specific training to ensure

---

<sup>15</sup> For this review, we verified that the Breach Notification Policy has been developed for GSA, but we did not assess the adequacy of or adherence to the policy.

that those responsible for protecting PII are aware of their responsibilities and the consequences of not adequately protecting such sensitive information. Further, improvements to ensure compliance with Agency patch management and system configuration policies and procedures would better ensure that system database and web application servers that store PII are not vulnerable to known exploits. Given their shared responsibility for developing and implementing controls for the protection of PII, clarification of roles and responsibilities between the CIO and CHCO regarding verification of the implementation of privacy-related controls would assist the two offices with managing and monitoring their respective security and privacy programs and ensure that key components necessary for an effective Privacy Act Program have been identified, developed, and implemented.

### **Recommendations**

To better manage risks of unauthorized or unintentional disclosure of personally identifiable information (PII), we recommend that the Chief Human Capital Officer:

- (1) Develop an implementation plan for the Privacy Act Program which identifies key roles, responsibilities, milestones, and management performance measures to achieve long-term improvement goals.
- (2) Work closely with the Chief Information Officer to establish collaborative agency-wide procedures to:
  - (a) Ensure that the Privacy Act Program is integrated with the Agency's security program and assesses risk with and identifies controls for all PII, including PII residing outside of major IT systems.
  - (b) Periodically assess the need for and potential uses of automated content management and data leakage tools or other procedures to assist in identifying and protecting PII within GSA's IT and system environment.
  - (c) Confirm that required security hardening guides are being appropriately followed and that identified vulnerabilities are promptly recorded and mitigated for major IT systems that collect and store PII.
  - (d) Implement remaining privacy controls required by M-06-16, including encryption and two-factor authentication for systems maintaining PII.
  - (e) Develop a plan that includes the key activities, milestones, and performance measures necessary to guide GSA in discontinuing the collection and storage of SSNs in IT systems where no longer required.
- (3) Work with the Office of the Chief Acquisition Officer to review contracts in support of major IT systems that collect and store PII to ensure that the appropriate privacy clauses have been included and that contractors supporting Privacy Act Systems of Records are aware of and fulfill their roles and responsibilities for protecting GSA's PII.
- (4) Complete development and implementation of role-based training for GSA Associates and contractors who are responsible for protecting sensitive information, including PII.

### **Management Comments**

The CHCO and CIO provided consolidated management comments on March 28, 2008 on specific audit findings and recommendations in response to our draft report. The comments indicate a general concurrence with our audit findings and recommendations, and a copy of the

comments is included as Appendix D. The CHCO and the CIO agreed with our recommendation to develop an implementation plan for the Privacy Act Program which identifies key roles, responsibilities, milestones, and management performance measures to achieve long-term improvement goals. Management also acknowledged the need to do more to protect PII and identified planned actions to meet audit recommendations. Management comments indicate that the CHCO will work closer with the OCIO to ensure that hardening guides are being appropriately applied and that the CHCO is working with the Office of Procurement Management Review, Office of Acquisition Integrity to randomly audit Privacy Act systems to ensure that the proper FAR clauses are included. In response to our recommendation to implement remaining privacy controls required by OMB Memorandum M-06-16, management comments provided additional information on the status of two of the three remaining requirements. The response also stated that GSA was unaware of a technical means to log all computer-readable data extracts from databases holding sensitive information and verify that each extract including sensitive data has been erased within 90 days or its use is still required. While management comments explained that some manual processes are being used in a limited capacity to support this requirement, we reaffirm the importance of determining an automated method to implement this control.

Management comments highlight activities recently completed and planned related to our recommendation to develop a plan that includes key activities, milestones, and performance measures necessary to guide GSA in discontinuing the collection and storage of SSNs in IT systems where no longer required. In response to our recommendation to complete development and implementation of role-based training for GSA Associates and contractors responsible for protecting sensitive information, including PII, management comments discuss goals to begin role-based training and highlight a 95% completion rate of the Privacy Awareness training over the past year. Management comments in response to our recommendation to assess the need for and potential uses of automated content management and data leakage tools or other procedures to assist in identifying and protecting PII within GSA's IT and system environment explain that the OCIO is currently evaluating data leakage prevention tools to assist in identifying and protecting PII within GSA's IT and system environment. While evaluating automated content and data leakage tools is a first step toward better protecting PII stored outside of IT systems that maintain Privacy Act data, our audit found that the Privacy Act Program has not yet ensured that PII stored on laptops and servers or in databases or applications that are not considered part of a major IT system is identified and protected as needed. Over the past year we identified numerous instances where PII stored outside of major IT systems was placed at undue risk. Therefore, we reaffirm the need to better ensure that all PII in GSA's IT systems environment be identified and properly protected from unauthorized access, modification, and disclosure.

### **Internal Controls**

As part of our review, we assessed the effectiveness of the Agency's Privacy Act Program and the implementation of controls for the protection of Privacy Act data. This audit included a review of selected management, operational, and technical controls relating to privacy for three of GSA's major IT systems that collect and store PII – FBO, STAR, and CWGT. This report states in detail the need to strengthen specific controls in order to strengthen the Privacy Act Program and better implement controls to protect PII.

IMPROVEMENTS TO THE GSA PRIVACY ACT  
PROGRAM ARE NEEDED TO ENSURE THAT  
PERSONALLY IDENTIFIABLE INFORMATION  
(PII) IS ADEQUATELY PROTECTED  
REPORT NUMBER A060228/O/T/F08007

**Appendix A – GSA 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.

**PLEASE PROVIDE YOUR RESPONSES USING THE DROP DOWN MENU IN GRAY**



**Section One**

<b>Security Controls and Assessment Procedures</b>		
<b>Security Checklist For Personally Identifiable Information That Is To Be Transported and/ or Stored Offsite, Or That Is To Be Accessed Remotely</b>		
	<b>REQUIRED RESPONSE</b>	<b>OPTIONAL RESPONSE</b>
<i>Procedure</i>	<i>Yes</i> <i>No</i> <i>Partial</i> <i>Not Applicable</i>	<i>Controls Not Yet in Place</i> <i>Policy</i> <i>Procedures</i> <i>Implemented</i> <i>Monitor &amp; Tested</i> <i>Integrated</i>
<b>STEP 1: Has the Agency confirmed identification of personally identifiable information protection needs? If so, to what level?</b>	<i>Yes</i>	<i>Procedures</i>
<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>	<i>Yes</i>	
<i>Comments: GSA has verified information categorization to ensure identification of PII requiring protection when accessed remotely or physically removed. GSA uses FIPS PUB 199 as guidance for assigning security categorization level within PII systems and has an automated system to help with and provide rigor to the process. Annually, the CPO requires PIAs be developed for (1) existing PII systems that have undergone a significant change since last year (such as changes in the collection or flow of data, new uses or disclosure of information, or incorporation of additional data items); (2) new systems containing personal information about members of the general public that have been developed since last year's PIA submissions; and (3) all systems with personal information about Federal government employees. The CPO provides a template for use in completing PIAs for GSA's PII systems.</i>		
<i>Action Item 1.2: Has the Agency verified existing risk assessments?</i>	<i>Yes</i>	

*Comments: GSA has verified existing risk assessments. For 5 of GSA's 18 PII systems, risk assessments have not yet been updated to address remote access and physical removal of PII data; however, most of these systems are undergoing certification and accreditation.*

**OVERALL STEP 1 COMMENTS:** GSA has defined PII as “any personal information that is associated with a unique identifier and can be accessed through that identifier. A personal identifier usually is a name plus another piece of information such as a Social Security Number (SSN), but can be any designation that is unique to a particular person. Personal information, for Federal government purposes, is any information that is protected by the Privacy Act. This includes personal information collected about public individuals. It also includes information collected about Federal personnel, with some exceptions for work-related information. In addition to name and SSN, some PII examples are a name plus home street and e-mail addresses, home and emergency telephone numbers, date of birth, marital status, race, sex, national origin, qualifications, medical history, private sector employment history, financial and credit records, grievances and appeals, legal and arrest records, and information about some (but not all) personnel actions.” GSA has identified 18 PII systems and designated each PII system as a moderate impact system. GSA has verified information categorization to ensure identification of PII requiring protection when accessed remotely or physically removed and verified existing risk assessments.

	REQUIRED RESPONSE	OPTIONAL RESPONSE
<i>Procedure</i>	<p><i>Yes</i></p> <p><i>No</i></p> <p><i>Partial</i></p> <p><i>Not Applicable</i></p>	<p><i>Controls Not Yet in Place</i></p> <p><i>Policy</i></p> <p><i>Procedures</i></p> <p><i>Implemented</i></p> <p><i>Monitor &amp; Tested</i></p> <p><i>Integrated</i></p>
<b>STEP 2: Has the Agency verified the adequacy of organizational policy? If so, to what level?</b>	<i>Partial</i>	<i>Policy</i>
<i>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?</i>	<i>Yes</i>	

*Comments: GSA has verified the adequacy of organizational policy. Recent joint policy from the CIO and CPO establishes requirements for remote access to and physical removal of PII; however, there is no enforcement of these controls.*

<p><i>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?</i></p>	<p><i>Partial</i></p>	
<p><i>1. For Personally Identifiable Information physically removed:</i></p>		
<p><i>a. Does the policy explicitly identify the rules for determining whether physical removal is allowed?</i></p>	<p><i>Yes</i></p>	
<p><i>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?</i></p>	<p><i>Partial</i></p>	
<p><i>2. For Personally Identifiable Information accessed remotely:</i></p>		
<p><i>a. Does the policy explicitly identify the rules for determining whether remote access is allowed?</i></p>	<p><i>Partial</i></p>	
<p><i>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?</i></p>	<p><i>No</i></p>	

<p>c. When remote access is allowed, does the policy identify the rules for</p>	<p>Yes</p>	
<p>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.)</p>		
<p><i>Comments: Policy states that an employee shall not remove PII from GSA facilities (including GSA managed programs housed at contractor facilities under contract), or accessed remotely, without written permission from the employee's supervisor, the data owner, and the IT system authorizing official. This applies to electronic media (e.g. laptops, Blackberries, USB drives), paper, and any other media (e.g., CDs/DVDs) that may contain PII. Policy states that if it is a business requirement to store PII on GSA user workstations or mobile devices including, but not limited to notebook computers, USB drives, CD-ROMs/DVDs, personal digital assistants and Blackberries, PII must be encrypted using an approved NIST algorithm, i.e., 3DES or AES. Certified encryption modules must be used to the greatest extent possible in accordance with FIPS PUB 140-2. Recommended methods of file encryption are also provided. Policy requires PII e-mailed within the GSA network or transmitted over the Internet to be encrypted. Basic privacy training has been provided to almost 80% of GSA Associates and contractors; however, this training does not instruct employees and contractors on how to implement or use encryption technologies during remote access or physical removal of data on mobile devices. Policy states that the Authorizing Official or their designee must grant remote access (i.e. external to GSA's network) privileges only to those GSA Associates and contractors with a legitimate need for such access as approved; however, there is no clear criteria for determination of remote access authorization. GSA has implemented a VPN solution for remote access but utilizes user name and password for authentication rather than an agency-issued certificate or a hardware token. Policy requires sensitive data on mobile storage devices that are removed from GSA premises be password protected or encrypted. While policy addresses the requirements for remote access to and physical removal of PII data, controls are not enforced to ensure compliance with established policy.</i></p>		
<p>Action Item 2.3: Has the organizational policy been revised or developed as needed, including steps 3 and 4?</p>	<p>Yes</p>	
<p><i>Comments:</i></p>		
<p><b>OVERALL STEP 2 COMMENTS:</b> GSA has verified the adequacy of organizational policy and updated policy as needed; however, GSA does not perform any checks to ensure that policies and procedures established for the protection of PII are consistently implemented. There is no clear criteria stated for determination of remote access authorization, and the Privacy Act training currently deployed by GSA does not instruct employees and contractors on how to implement or use encryption technologies during remote access or physical removal of data on mobile devices. GSA uses a VPN for remote access but does not use an agency-issued certificate or hardware token for authentication.</p>		

	REQUIRED RESPONSE	OPTIONAL RESPONSE
<i>Procedure</i>	<p><i>Yes</i></p> <p><i>No</i></p> <p><i>Partial</i></p> <p><i>Not Applicable</i></p>	<p><i>Controls Not Yet in Place</i></p> <p><i>Policy</i></p> <p><i>Procedures</i></p> <p><i>Implemented</i></p> <p><i>Monitor &amp; Tested</i></p> <p><i>Integrated</i></p>
<b>STEP 3: Has the Agency implemented protections for personally identifiable information being transported and/or stored offsite? If so, to what level?</b>	<i>Partial</i>	Policy
<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>	<i>Partial</i>	
<i>* Evaluation could include an assessment of tools used to transport PII for use of encryption.</i>		
<i>Comments: Policy states that an employee shall not remove PII from GSA facilities (including GSA managed programs housed at contractor facilities under contract), or accessed remotely, without written permission from the employee's supervisor, the data owner, and the IT system authorizing official. This applies to electronic media (e.g. laptops, Blackberries, USB drives), paper, and any other media (e.g., CDs/DVDs) that may contain PII. Policy states that if it is a business requirement to store PII on GSA user workstations or mobile devices including, but not limited to notebook computers, USB drives, CD-ROMs/DVDs, personal digital assistants and Blackberries, PII must be encrypted using an approved NIST algorithm, i.e., 3DES or AES. Certified encryption modules must be used to the greatest extent possible in accordance with FIPS PUB 140-2. Recommended methods of file encryption are also provided. Policy requires PII e-mailed within the GSA network or transmitted over the Internet to be encrypted. While policy addresses the requirements for transportation of PII data, controls for encryption of transportation of GSA PII are not enforced to ensure compliance with established policy.</i>		
<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>	<i>Partial</i>	
<i>* Evaluation could include a review of remote site facilities and operations.</i>		

*Comments: Policy states that an employee shall not remove PII from GSA facilities (including GSA managed programs housed at contractor facilities under contract), or accessed remotely, without written permission from the employee's supervisor, the data owner, and the IT system authorizing official. This applies to electronic media (e.g. laptops, Blackberries, USB drives), paper, and any other media (e.g., CDs/DVDs) that may contain PII. Policy states that if it is a business requirement to store PII on GSA user workstations or mobile devices including, but not limited to notebook computers, USB drives, CD-ROMs/DVDs, personal digital assistants and Blackberries, PII must be encrypted using an approved NIST algorithm, i.e., 3DES or AES. Certified encryption modules must be used to the greatest extent possible in accordance with FIPS PUB 140-2. Recommended methods of file encryption are also provided. Policy requires PII e-mailed within the GSA network or transmitted over the Internet to be encrypted. While policy addresses the requirements for storage of PII data, controls for encryption of remote storage of GSA PII are not enforced to ensure compliance with established policy.*

**OVERALL STEP 3 COMMENTS:** While policy addresses the requirements for transportation and remote storage of PII data, controls for encryption of transportation of GSA PII are not enforced to ensure compliance with established policy.

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

	<b>REQUIRED RESPONSE</b>	<b>OPTIONAL RESPONSE</b>
<i>Procedure</i>	<p style="text-align: center;"> <i>Yes</i>  <i>No</i>  <i>Partial</i>  <i>Not Applicable</i> </p>	<p style="text-align: center;"> <i>Controls Not Yet in Place</i>  <i>Policy</i>  <i>Procedures</i>  <i>Implemented</i>  <i>Monitor &amp; Tested</i>  <i>Integrated</i> </p>
<b>STEP 4: Has the Agency implemented protections for remote access to personally identifiable information? If so, to what level?</b>	<i>Partial</i>	<i>Policy</i>
<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>	<i>Yes</i>	
* Evaluation could include a review of the configuration of VPN application(s).		
<i>Comments: GSA has implemented a VPN solution for remote access utilizing user name and password for authentication.</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?	No	
* Evaluation could include a review of controls for downloading PII.		
Comments: Policy was recently updated to require that creation of computer-readable data extracts that include PII shall be maintained in an official log including creator, date, type of information, and user. However, this control has not been implemented and is not enforced. GSA has not yet established a plan to verify each extract including sensitive data has been erased within 90 days or its use is still required. Officials stated that they are unaware of any immediate viable solution to implement this control across GSA's PII systems.		
<b>If remote storage of personally identifiable information is to be permitted follow Action Item 4.3, otherwise follow Action Item 4.4.</b>		
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?	No	
Comments: Policy requires that (1) PII shall not be stored on or accessed from personally owned computers or personally owned mobile devices; (2) PII shall only be accessed from government furnished equipment (GFE) or contractor maintained computers configured in accordance with GSA IT security policy and technical security standards; and (3) if it is a business requirement to store PII on GSA user workstations or mobile devices including, but not limited to notebook computers, USB drives, CD-ROMs/DVDs, personal digital assistants and Blackberries, PII must be encrypted using an approved NIST algorithm, i.e., 3DES or AES. Without automated enforcement of this policy, verification and enforcement of this control is not possible.		
Action Item 4.4: Has the Agency enforced NIST Special Publication 800-53 security controls enforcing no remote storage of personally identifiable information?	No	
Comments: GSA has no mechanism in place that can monitor or control the storage and encryption of PII data when remote storage is permitted.		
<b>OVERALL STEP 4 COMMENTS:</b> GSA has implemented a VPN solution for remote access utilizing user name and password for authentication. While policy addresses the requirements for transportation and remote storage of PII data, controls for encryption of transportation of GSA PII are not enforced to ensure compliance with established policy. GSA has not implemented controls enforcing allowed downloading of PII or enforcing and encryption of remote storage of PII. GSA has also not implemented controls enforcing no remote storage of PII when not permitted.		

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

**Section Two**

<b>Additional Agency Actions Required by OMB M-06-16</b>	
	<i>Yes</i>
	<i>No</i>
<i>Procedure</i>	<i>Partial</i>
	<i>Not Applicable</i>
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?	<i>Partial</i>
<p><i>Comments: Policy regarding encryption of data on mobile computers/devices has been limited to only address PII. Policy states that PII shall not be stored on or accessed from personally owned computers or personally owned mobile devices, and PII shall only be accessed from government furnished equipment or contractor maintained computers configured in accordance with GSA IT security policy and technical security standards. Policy also states that PII shall be stored on network drives and/or in application databases with proper access controls (i.e., user ID/password) and shall be made available only to those individuals with a valid need to know. Policy states that if it is a business requirement to store PII on GSA user workstations or mobile devices including, but not limited to notebook computers, USB drives, CD-ROMs/DVDs, personal digital assistants and Blackberries, PII must be encrypted using an approved NIST algorithm, i.e., 3DES or AES. Certified encryption modules must be used to the greatest extent possible in accordance with FIPS PUB 140-2, Security Requirements for Cryptographic Modules. Recommended methods of encryption are also provided. This policy was just implemented. Without automated enforcement of this policy, it is up to the individual user to comply. The Agency is beginning a pilot of full disk encryption and plans to begin phased implementation of encrypting all data on laptops in the first quarter of FY07 with complete implementation by the first quarter of FY08. Once full disk encryption is implemented, users will be forced to comply with established policy.</i></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?	<i>No</i>
<p><i>Comments: GSA has not implemented two-factor authentication, where one of the factors is provided by a device separate from the computer gaining access. Rather than investing significant resources to develop and implement a solution for two-factor authentication that will not be in compliance with Homeland Security Presidential Directive (HSPD)-12, GSA plans to address this requirement with its HSPD-12 solution next year.</i></p>	
3. Does the Agency use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity?	<i>Partial</i>
<p><i>Comments: Policy requires that all remote access connections and mobile devices shall automatically lock-out within 30 minutes of inactivity. However, a test of this control found that this control was not implemented consistently. We tested four of GSA's 18 PII systems and found that users were only timed out with two of the systems.</i></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?

No

*Comments: Policy was recently updated to require that creation of computer-readable data extracts that include PII shall be maintained in an official log including creator, date, type of information, and user. However, this control has not been implemented and is not enforced. GSA has not yet established a plan to verify each extract including sensitive data has been erased within 90 days or its use is still required. Officials stated that they are unaware of any immediate viable solution to implement this control across GSA's PII systems.*

<b>Section Three</b>		
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:		
<b>Type of work completed (i.e., assessment, evaluation, review, inspection, or audit).</b>		<b>Assessment</b>
<p><b>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.)</b></p>	<p>During this assessment, we used the President’s Council on Integrity and Efficiency (PCIE)/Executive Council on Integrity and Efficiency (ECIE) review guide and data collection instrument to direct our work. We interviewed appropriate staff from GSA’s Offices of the Chief People Officer (CPO) and Chief Information Officer (CIO) with key responsibilities for ensuring the protection of Agency sensitive information. We gathered information related to actions GSA has taken to protect personally identifiable information (PII) prior to and in response to the Office of Management and Budget (OMB) Memorandum M-06-16 and considered recently developed Agency policy regarding the protection of sensitive information. We considered the Agency’s mandatory on-line training, information disseminated through the privacy program website, and the Agency report on the activities taken to meet the requirements of M-06-16. We also reviewed a GSA report responding to OMB Memorandum M-06-20 and Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005. We tested select controls for a sample of PII systems to determine whether the 30-minute timeout requirement had been implemented. We reviewed select security and privacy documentation developed for seven PII systems. We also followed up on previously issued audit work by reviewing the list of Systems of Records for accuracy and completeness and developing a timeline documenting major steps and milestones directed at implementing controls for sensitive information.</p> <p>We met with the Chief Privacy Officer and the Chief Information Officer on September 21, 2006, who generally concurred with the results of our assessment and responses to the PCIE/ECIE data collection instrument.</p>	

**Assessment Methodologies Used to complete the DCI Sections**

<b>Mark All That Apply</b>					
	<b>Section One</b>				<b>Section Two</b>
	<b>Step 1</b>	<b>Step 2</b>	<b>Step 3</b>	<b>Step 4</b>	
<b>Interviews (G/F/C)</b>	C	C	C	C	C
<b>Examinations (G/F/C)</b>	F	F	F	F	F
<b>Tests (independently verified - Y/N)</b>	N	N	N	N	Y
<i>Assessment Method Descriptions consistent with NIST SP 800-53A - Appendix D pages 34 - 36.</i>					
<i>G = Generalized. F = Focused. C = Comprehensive.                      Y = Yes. N = No.</i>					

<p><b>Overall Summary Statement. (Please refer to page five of the review guide for sample language for summary statements.)</b></p>	<p>GSA has recently defined personally identifiable information (PII) for Agency systems and taken steps toward improving the protection of PII. The Agency's Chief Privacy Officer (CPO) and Chief Information Officer (CIO) have recently issued a joint instruction letter establishing policy regarding requirements for safeguarding PII. Basic privacy training has also provided the majority of Associates and contractors. System Owners for 18 systems that store or process PII have reported on compliance with the security checklist included with OMB Memorandum M-06-16 to the CIO. Systems within GSA containing PII have been designated with moderate level risk. However, all of the requirements of Office of Management and Budget (OMB) Memorandum M-06-16 have not been satisfied.</p> <p>The privacy guidance issued by the CPO and CIO covers two of the four recommendations in OMB Memorandum M-06-16. Specifically, since officials are unaware of any immediate viable solution to implement controls to verify each extraction of sensitive data has been erased within 90 days or its use is still required, GSA could not implement this recommendation. Additionally, rather than investing significant resources to implement a two-factor authentication solution that would be replaced by a Homeland Security Presidential Directive (HSPD)-12 compliant solution planned for implementation early next year, GSA decided not to meet the recommendation for implementing two-factor authentication for remote access at this time but with its HSPD-12 solution. Within GSA, the joint policy establishes requirements for encrypting PII on removable media and GSA workstations, but without automated enforcement of this policy, verification of this control is not yet possible. The Agency also plans to begin phased implementation of full disk encryption for GSA workstations and laptops next year. The recent policy also requires all remote access connections and mobile devices to be automatically locked out within 30 minutes of inactivity; however, tests of PII systems found that only two of the four systems had implemented this control.</p> <p>In assessing the Agency's implementation of the security checklist, we found that GSA has implemented controls for confirming the identification of PII protection needs. GSA has also partially implemented controls for verifying the adequacy of organizational policy and protecting the transportation and remote storage of and remote access to PII. However, these controls are being provided primarily at the policy and/or procedures level and have not been fully implemented with GSA's PII systems. Agency-wide responsibility for ensuring that these controls have been implemented per privacy policy has not yet been established, and GSA has not yet implemented the following controls: (1) controls enforcing no remote storage/transportation of and no remote access to PII, when not permitted; (2) controls enforcing that remote transportation/storage of and remote access to PII be encrypted; (3) controls enforcing allowed downloading of PII.</p> <p>Our assessment indicates that the Agency needs to improve policies and procedures for the protection of sensitive information in the following areas: (1) establish and communicate accountability and responsibility for specific privacy controls, including the implementation of technologies used to collect, use, store, and disclose information in identifiable form to allow for continuous auditing of compliance with established privacy policies, (2) improve privacy training to address OMB Memorandum M-06-16 requirements regarding the protection of remote access, storage, and transportation of PII; (3) obtain input from all Service and Staff Offices to ensure the Agency's definition of PII is comprehensive and that Associates and contractors fully recognize what information is considered PII, and (4) improve reporting for security weaknesses for PII systems and within the GSA privacy program.</p>
--	--

IMPROVEMENTS TO THE GSA PRIVACY ACT  
PROGRAM ARE NEEDED TO ENSURE THAT  
PERSONALLY IDENTIFIABLE INFORMATION  
(PII) IS ADEQUATELY PROTECTED  
REPORT NUMBER A060228/O/T/F08007

**Appendix B – Timeline of GSA Activities Related to Privacy Controls**

Date	Event
December 2002	E-Government Act of 2002 signed.
May 2003	CPO issues GSA guidance on ensuring security and privacy of personal information.
October 2003	GSA Privacy Act Program Order issued.
May 2004	GSA CPO Issues Guidelines on Conducting PIAs.
December 2004	Public Law 108-447 – Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005 identifies Agency and IG requirements for Privacy Reviews.
June 2005	CPO Memo issued on GSA Privacy Act regulations and Systems Of Records (SOR) notices.
August 2005	Submitted Privacy portion of the FY05 FISMA report to OCIO.
December 2005	GSA PIAs posted on gsa.gov.
May 2006	CPO Memo reminds employees of their responsibilities for safeguarding personally identifiable information.
	OMB M-06-15 on Safeguarding Personally Identifiable Information issued.
June 2006	Privacy Training 101 Available on GSA Online University.
	OMB M-06-16 on Protection of Sensitive Agency Information requires specific privacy controls.
July 2006	OMB M-06-19 on Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments issued.
	OMB M-06-20 FY06 Reporting Instructions for FISMA and Agency Privacy Management issued.

Date	Event
August 2006	CIO issued IL-06-02, <u>Safeguarding Personally Identifiable Information (PII)</u> , regarding safeguarding PII in GSA IT systems and any associated record of that information.
	GSA Privacy Act Program website launched on gsa.gov.
	GSA Privacy Act Benchmark report in response to Public Law 108-447, Section 522.
October 2006	Agency submitted FY 06 FISMA report, which included questions related to privacy, to OMB.
May 2007	OMB M-07-16 on Safeguarding Against and Responding to the Breach of Personally Identifiable Information issued.
June 2007	GSA IT Security Policy revised to include Privacy requirements. This policy canceled CIO Instructional Letter 06-02, <u>Safeguarding Personally Identifiable Information (PII)</u> .
September 2007	Agency submitted to OMB the FY 07 FISMA report, including a response to specific questions related to privacy.

IMPROVEMENTS TO THE GSA PRIVACY ACT  
PROGRAM ARE NEEDED TO ENSURE THAT  
PERSONALLY IDENTIFIABLE INFORMATION  
(PII) IS ADEQUATELY PROTECTED  
REPORT NUMBER A060228/O/T/F08007

**Appendix C –Vulnerability Scanning Results**

Due to the sensitive nature of information contained in this appendix, only reports provided to system security officials and the GSA Senior Agency Information Security Officer contain detailed vulnerability scanning results for the three Privacy Act Systems of Records tested during this review. Requests for the details of technical vulnerability scanning results should be referred to Jennifer Klimes, Audit Manager, or Gwendolyn McGowan, Deputy Assistant Inspector General for IT Audits.

IMPROVEMENTS TO THE GSA PRIVACY ACT  
PROGRAM ARE NEEDED TO ENSURE THAT  
PERSONALLY IDENTIFIABLE INFORMATION  
(PII) IS ADEQUATELY PROTECTED  
REPORT NUMBER A060228/O/T/F08007


**Appendix D – CHCO/CIO Consolidated Response to Draft Report**




GSA Office of the Chief Human Capital Officer

MAR 28 2008

MEMORANDUM FOR GWENDOLYN A. MCGOWAN  
DEPUTY ASSISTANT INSPECTOR GENERAL FOR  
INFORMATION TECHNOLOGY AUDITS (JA-T)

FROM: GAIL T. LOVELACE   
CHIEF HUMAN CAPITAL OFFICER (C)

 CASEY COLEMAN  
CHIEF INFORMATION OFFICER (I)

SUBJECT: IMPROVEMENTS TO THE GSA PRIVACY ACT PROGRAM  
ARE NEEDED TO ENSURE THAT PII IS ADEQUATELY  
PROTECTED  
REPORT NUMBER A060228

Thank you very much for the opportunity to comment on your review of the GSA Privacy Act Program. We have worked diligently during 2007 to strengthen the program and increase protection of Personally Identifiable Information (PII). With existing and new regulations always on the forefront we feel it's important to work with your office. The Chief Human Capital Officer and the Chief Information Officer will continue to work closely together to ensure the Privacy Act program implements the appropriate security requirements.

If you have any questions, please contact Kurt Garbars, Senior Agency Information Security Officer, on (202) 208-7485 or Kim Mott, Privacy Act Officer, on (202) 208-1317.

Attachment

U.S. General Services Administration  
1800 F Street, NW  
Washington DC 20405-0002  
www.gsa.gov



**Improvements to the GSA Privacy Act Program are Needed to Ensure that PII is Adequately Protected  
Report #A060228**

Recommendations

1) Develop an implementation plan for the Privacy Act Program which identifies key role, responsibilities, milestone, and management performance measures to achieve long-term improvement goals.

CHCO concurs with this recommendation and is taking steps to accomplish this.

2) Work closely with the Chief Information Officer to establish collaborative agency-wide procedures to:

a) Ensure that the Privacy Act program is integrated with the Agency's security program and assesses risk with and identifies controls for all PII, including PII residing outside of major IT systems.

CHCO works with the OCIO on a continuing basis. We collaborated on CIO IL-06-2 (Safeguarding Personally Identifiable Information) which was recently incorporated into the GSA Information Technology Security Policy (CIO 2100.1D). We collaborated on Security Awareness and Privacy Training 101. Plus, we coordinate on POA&M Quarterly Reports, FISMA Yearly Reports, Exhibit 300 Yearly Reports, and all other reports and requests for information that come to GSA.

b) Periodically assess the need for and potential uses of automated content management and data leakage tools or other procedures to assist identifying and protecting PII within GSA's IT and system environment.

The OCIO is currently evaluating data leakage prevention tools.

c) Confirm that required security hardening guides are being appropriately mitigated for major IT systems that collect and store PII.

CHCO will work closer with the OCIO to ensure hardening guides are being properly mitigated for all systems that collect and store PII. The OCIO will inform system owners and scan for compliance.

d) Implement remaining privacy controls required by M-06-16, including encryption and two-factor authentication for systems maintaining PII.

Two-factor authentication is expected to be completed by 9/30/09. GSA has begun lab testing of two-factor authentication for remote access using HSPD-12 cards. Completion of this task is dependent on complete rollout of HSPD-12 cards and implementation of PKI infrastructure to support this. GSA employs a 30 minute or less

---

inactivity timeout on all remote access and mobile devices. GSA does not know of a technical means to enforce log and verify. Some manual processes have been used to support this in a limited way. The expected completion is to be determined. Encryption is currently implemented on all Blackberries and is currently being rolled out to all laptops and desktops. A joint message will be sent from the Office of the Chief Human Capital Officer (CHCO) and the Office of the Chief Information Officer (CIO) reminding people of the risk of storing sensitive or Personally Identifiable Information on their laptops and Blackberries until encryption is widely available. The message will instruct employees and contractors to use alternate encryption methods to protect PII that is being transmitted.

e) Develop a plan that includes the key activities, milestones, and performance measures necessary to guide GSA in discontinuing the collection and storage of SSNs in IT systems where no longer required.

GSA has developed a plan to reduce collection and use of SSNs at GSA. CHCO has collected information from system owners and has reviewed the data with OCIO. Based on data collected, recommendations will be made to a few system owners to halt SSN collection and use. GSA's plan will include milestones and performance measures. While CHCO will make every effort to reduce SSN collection and use we understand that certain software configurations make it impossible to eliminate its collection entirely.

3) Work with the Office of the Chief Acquisition Officer to review contracts in support of major IT systems that collect and store PII to ensure that the appropriate privacy clauses have been included and that contractors supporting Privacy Act Systems of Records are aware of and fulfill their roles and responsibilities for protecting GSA's PII.

CHCO is working with the Office of Procurement Management Review, Office of Acquisition Integrity to randomly audit of Privacy Act Systems of Records contracts to ensure the proper FAR clauses are included. The review is in the initial stage. On InSite, Privacy Program, GSA Contracting page it states that the Privacy Act applies to contractors who operate systems of records containing personal information, that contractors and its employees are considered employees of the agency and are subject to the same requirements for safeguarding information as Federal employees, contractors and their employees are subject to civil and criminal sanctions for any violation that may occur due to oversight or negligence.

4) Complete development and implementation of role-based training for GSA Associates and contractors who are responsible for protecting sensitive information, including PII.

CHCO has developed content for role-based training and it is expected to be deployed in the 3<sup>rd</sup> Quarter. CHCO worked with the HSPD-12 Training Office to ensure that HSPD-12 role-based training includes privacy information. During the last training cycle Privacy Training 101 had a 95% completion rate for employees and contractors.

IMPROVEMENTS TO THE GSA PRIVACY ACT  
PROGRAM ARE NEEDED TO ENSURE THAT  
PERSONALLY IDENTIFIABLE INFORMATION  
(PII) IS ADEQUATELY PROTECTED  
REPORT NUMBER A060228/O/T/F08007

**APPENDIX E – REPORT DISTRIBUTION**

	<u>Copies</u>
<b><u>With Appendix C</u></b>	
Office of the Chief Human Capital Officer (C)	3
Office of the Chief Information Officer (I)	3
Office of the Senior Agency Information Security Officer (IS)	1
Office of Acquisition Policy (MV)	1
Authorizing Official for STAR	1
Authorizing Official for FBO	1
Authorizing Official for CWGT	1
Information Systems Security Manager for STAR	1
Information Systems Security Manager for FBO	1
Information Systems Security Manager for CWGT	1
Information Systems Security Officer for STAR	1
Information Systems Security Officer for FBO	1
Information Systems Security Officer for CWGT	1
<b><u>Without Appendix C</u></b>	
Counsel to the Inspector General (JC)	1
Assistant Inspector General for Auditing (JA and JAO)	2
Deputy Assistant Inspector General for Finance and Administrative Audits (JA-F)	1

Assistant Inspector General for Investigations (JI)	1
Internal Control and Audit Division (BEI)	1
Administration and Data System Staff (JAS)	1