Implementation Review

IMPLEMENTATION REVIEW OF
CONTROLS FOR GSA'S PRIVACY ACT DATA
REPORT NUMBER A020256/O/T/F03005
DATED JANUARY 6, 2003
ASSIGNMENT NUMBER A060045

January 18, 2006

Office of Inspector General
General Services Administration

Office of Audits

IMPLEMENTATION REVIEW OF CONTROLS FOR GSA'S PRIVACY ACT DATA REPORT NUMBER A020256/O/T/F03005 DATED JANUARY 6, 2003 ASSIGNMENT NUMBER A060045

January 18, 2006

U.S. GENERAL SERVICES ADMINISTRATION
Office of Inspector General

January 18, 2006

Reply to Attn of: Deputy Assistant Inspector General for Information Technology Audits (JA-T)

To: Gail T. Lovelace
Chief People Officer (C)

Michael W. Carleton
Chief Information Officer (I)

Subject: Implementation Review of Controls for GSA's Privacy Act Data
Report Number A020256/O/T/F03005
Dated January 6, 2003
Assignment Number A060045

The Office of Inspector General has completed an implementation review of the management actions taken on the three recommendations in the subject audit report. The audit report presented the results of our review of controls in place to ensure adequate protection for Privacy Act data maintained within the General Services Administration's (GSA) information technology (IT) systems. A formal action plan provided by the Office of the Chief People Officer (OCPO) on March 6, 2003 addressed our recommendations and identified specific steps to be completed, with the assistance of the Office of the Chief Information Officer (OCIO) and the Office of Acquisition Policy, to improve the controls and oversight of Privacy Act information. Attachment A contains a copy of the management action plan your office provided.

Background

Identity theft continues to be a rapidly growing category of crime facilitated by use of the Internet to obtain personal information without the consent of the individual. As such, additional controls for electronic files, including those that may contain sensitive personnel information, should be carefully considered to help manage increasing risks in this area. Recent management actions indicate 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. Our initial review, conducted between September and October 2002, assessed the management and adequacy of controls in place to protect Privacy Act data, including personally identifiable information. We focused on controls for files containing systems of records, processes for periodically reviewing these files, web server content management and training, and supervision of GSA associates and contractors with access to select Privacy Act data. Our report recommended steps to improve management, operational, and technical controls for the protection of sensitive data, including personally identifiable information.

Specifically, we recommended that the OCPO work together with the OCIO to improve the management of GSA's Privacy Act data by: (1) working 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. Your office concurred with these recommendations and has taken specific steps as delineated in the March 2003 time-phased action plan.

Scope and Methodology

This implementation review included discussions with information security and privacy personnel in the OCIO and the OCPO to determine if management's action plan has been implemented and whether conditions identified with the initial review have been resolved. We analyzed Privacy Act clauses recently added to the Federal Acquisition Regulation (FAR), including Parts 24 and 39. To sample the application of these Privacy Act requirements in IT support contracts, we reviewed contracts for the Comprehensive Human Resources Integrated System (CHRIS), the Payroll and Accounting and Reporting (PAR) system, and the GSAJobs system. We considered applicable statutes, regulations, policies, guidance, and operating procedures, including: the Privacy Act of 1974; Office of Management and Budget (OMB) Circular A-130, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals, and Appendix III, Security of Federal Automated Information Resources, November 28, 2000; OMB's Implementation Guidance for the E-Government Act of 2002, M-03-18, August 1, 2003; OMB's Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, M-03-22, September 26, 2003; the GSA Privacy Act Program, CPO 1878.1, October 27, 2003; and Conducting Privacy Impact Assessments (PIAs) in GSA, CPO 1878.2, May 28, 2004. We also reviewed memoranda issued by the OCIO regarding the Privacy Act, including the June 22, 2005 memo regarding GSA Privacy Act regulations and Systems of Records notices and the July 15, 2003 memo requesting that Heads of Services and Staff Offices and Regional Administrators provide input to update the Agency's Systems of Records list, and information disseminated via the Privacy Act Program website maintained by the OCPO. Fieldwork was completed between October and December 2005.

Observations

We found that management has taken actions in accordance with the time-phased action plan in response to our 2003 report; however, conditions raised in the previous report remain. Contracts for two of the three systems we reviewed did not include the appropriate FAR clauses for Privacy Act systems, and GSA's list of Privacy Act systems, maintained by the OCPO, is still not up-to-date. Further, roles and responsibilities for GSA associates and contractors are not yet well defined, and training has not been provided to ensure that responsible individuals are aware of requirements for protecting GSA Privacy Act data.

Recommendation # 1 - **Work 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**.

In 2003, we reported the need to specify restrictions or penalties for unauthorized disclosures and for GSA IT service contracts to state the need to protect Privacy Act data. Since then, the Office of Acquisition Policy has developed contract clauses covering Privacy Act information to be used in GSA's IT support contracts, and the OCPO has issued an Order mandating Privacy Act clauses to be used in GSA's IT support contracts. During this implementation review, we analyzed four IT support contracts for three Privacy Act Systems: (1) PAR, (2) GSAJobs, and (3) CHRIS. We found that two of the contracts did not include or reference the requisite FAR clauses. Further, we were unable to verify whether biennial reviews of a random sample of GSA's IT support contracts are being completed as required by OMB. These reviews are important in order to ensure that the wording of each contract makes the provisions of the Privacy Act binding on the contractor. Without appropriate contract provisions for protecting Privacy Act data, the Agency cannot be sure that contractors are aware of restrictions on Privacy Act data and the consequences of unauthorized disclosures.

Recommendation # 2 - **Update GSA's Systems of Record list**.

We also reported that the Agency's list of Privacy Act Systems of Records (SOR) needed to be updated. The Privacy Act of 1974 defines a System of Record as 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. The OCPO has issued memoranda to Heads of Services and Staff Offices and to Regional Administrators requesting an update of the Privacy Act SOR under their jurisdiction, and the SOR list, as identified on the official GSA Privacy Act Program website, has been updated to include a major system for managing human resource information. However, the SOR list is not yet current and complete. For example, the Federal Acquisition Institute (FAI) Online system, Federal Business Opportunities (FedBizOps), Federal Procurement Data System - Next Generation (FPDS-NG), System for Tracking and Administering Real Property (STAR), GSAJobs, and USA Services are not yet identified as a SOR on the Privacy Act Program website. With the exception of GSAJobs, which is covered under an OPM Privacy Act notice, these systems also do not have published Privacy Act notices. Privacy Act notices are required to be published in the Federal Register to report any new use or intended use of the information in the system and to provide an opportunity for interested persons to submit written data, views, or arguments to the Agency. Additionally, the list of SOR identified on GSA's Privacy Act Program website has not been updated to remove transferred and obsolete systems, including Classified Control Files; the Emergency Notification System; and Incident Reporting, Investigation, Contingency Planning/Analysis, and Security Case Files. Without a complete and accurate inventory of SOR, specific risks with these systems may not be adequately addressed.

Recommendation # 3 - **Ensure that accountability and responsibility is assigned for identifying and implementing specific controls for each of GSA's Systems of Records**.

The need to clarify key roles and responsibilities for protecting GSA's Privacy Act data from unauthorized disclosure was also reported as a matter requiring management attention. At that time, online security training for GSA Associates and contractors did not cover Privacy Act requirements or restrictions on unauthorized disclosures of personal information entrusted to those who work with sensitive files. Further, controls for protecting GSA's sensitive data were not robust enough to adequately address risks in the Agency's automated business environment. We also found that GSA web server files needed to be reviewed for sensitive data to strengthen controls to prevent improper disclosure of Privacy Act data on GSA web servers both behind and outside the firewall. With this implementation review, we found that the Agency has not yet developed a Privacy Act training program, increasing the risk of inappropriate disclosure of sensitive information. We also found that GSA has not assigned roles and responsibilities to verify the implementation of required privacy-related controls, including the incorporation of appropriate privacy-related clauses in IT support contracts. Consequently, it is unclear whether privacy-related controls required by the OCPO have been consistently implemented for all GSA Privacy Act systems. While technical controls for Privacy Act data, such as automated content management and data leakage technologies are readily available, the Agency does not have procedures in place to apply these beneficial tools. Moreover, general procedures are not yet in place to ensure that controls over sensitive Privacy Act data are in place and operating as expected.

Next Steps

It is essential that GSA associates and contractors who are increasingly relied on and entrusted with access to Privacy Act data understand the need to safeguard this information and agree to protect it. Since our previous review, the E-Government Act of 2002 emphasized the need to adequately protect personal information in Federal IT systems, and OMB now requires that Privacy Impact Assessments be conducted for IT systems that contain personal data on members of the general public, including Government employees and contractors. Agency responsibilities have also been expanded to fulfill Privacy Act requirements and improve the protection of sensitive data. Given new requirements for controls for Privacy Act systems, the conditions we observed with this implementation review, and related actions requiring additional management attention, we recommend that you reassess the Agency's policies and procedures for protecting Privacy Act data. Because of increasing risks in this area, we plan to continue monitoring controls for select SOR and Privacy Act data by conducting additional audits in fiscal year 2006.

We would like to express our appreciation to you and your staff for your assistance and cooperation during this implementation review. Should you have any comments or questions about this review, please contact me or Gwendolyn McGowan, Deputy Assistant Inspector General for Audits, Information Technology Audit Office, on (703) 308-1223.

Jennifer M. Klimes
Audit Manager (JA-T)
Information Technology Audit Office

Attachment A – Time-Phased Action Plan to Review of GSA's Privacy Act Data, Report Number A020256/O/T/F03005, Dated January 6, 2003

GSA

GSA Office of the Chief People Officer

March 6, 2003

MEMORANDUM FOR EUGENE WASZILY
ASSISTANT INSPECTOR GENERAL
FOR AUDITING (JA)

FROM: GAIL T. LOVELACE
GSA CHIEF PEOPLE OFFICER (C)

SUBJECT: REVIEW OF CONTROLS FOR
GSA'S PRIVACY ACT DATA
REPORT NUMBER A020256/O/T/F03005

I'm providing the response to the subject audit report dated January 6, 2003. Attached documents include the Management Decision Record and a time-phased Action Plan as required by GSA Order ADM P 2030.2B.

The Action Plan spells out the steps that my office, with the assistance of the Office of the Chief Information Officer (I) and the Office of Acquisition Policy (MV), will take to implement the proposed recommendations aimed at improving the controls and oversight of Privacy Act information.

If there are any questions, please contact Fred Alt on (202) 501-2518 or Jinaita Kanarchuk on (202)-501-1452.

Attachments (2)

cc: Gwendolyn A. McGowan (JA-T)
Ralph Boldt (BECA)
Michael W. Carleton (I)
David A Drabkin (MV)

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

ACTION PLAN

Designated Responding Official: **Gail T. Lovelace, Chief People Officer (CPO)**
Contact Person: **Fred Alt, CPO Chief Information Officer**
Telephone No.: **202-501-2518**

AUDIT REPORT NUMBER	RECOMMENDATION/ FINDING NUMBER	PROPOSED RECOMMENDATION/ FINDING COMPLETION DATE
A020256/O/T/F03005	1	**September 30, 2003**

RECOMMENDATION: That the Office of the Chief People Officer (C), with the assistance of the Office of the Chief Information Officer (I), work with the Office of Acquisition Policy (MV) 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.

Management Response:

The Chief People Officer concurs with the findings and the recommendation.

Responsible Organizations:

ACTION TO BE TAKEN STEP BY STEP	SUPPORTING DOCUMENTATION TO BE SENT TO AUDIT RESOLUTION AND INTERNAL CONTROLS DIVISION		DOCUMENTATION WILL BE SENT BY LAST DAY OF
1. Develop and issue Instructional Memorandum addressing basic Privacy Act, Acquisition Policy, and IT Security issues in GSA.	C, with assist-ance of MV & I	Copy of Instructional Memorandum	April 30, 2003
2. Develop contract clauses covering Privacy Act information to be used in GSA's IT support contracts.	C, with assist-ance of MV & I	Copy of Contract Clauses covering Privacy Act information	August 31, 2003

ACTION TO BE TAKEN STEP BY STEP	SUPPORTING DOCUMENTATION TO BE SENT TO AUDIT RESOLUTION AND INTERNAL CONTROLS DIVISION		DOCUMENTATION WILL BE SENT BY LAST DAY OF
3. Issue GSA Order mandating the Privacy Act clauses to be used in GSA's IT support contracts, along with policy and guidance on roles and responsibilities for safeguarding sensitive information by contractors and GSA employees.	C, with assist-ance of I	Copy of GSA Order	September 30, 2003

ACTION PLAN

Designated Responding Official: **Gail T. Lovelace, Chief People Officer (CPO)**
Contact Person: **Fred Alt, CPO Chief Information Officer**
Telephone No.: **202-501-2518**

AUDIT REPORT NUMBER	RECOMMENDATION/ FINDING NUMBER	PROPOSED RECOMMENDATION/ FINDING COMPLETION DATE
A020256/O/T/F03005	2	**August 31, 2003**

RECOMMENDATION: That the CPO, with the assistance of the CIO, update GSA's Systems of Records List.

Management Response:

The CPO concurs with this recommendation.

ACTION TO BE TAKEN STEP BY STEP	SUPPORTING DOCUMENTATION TO BE SENT TO AUDIT RESOLUTION AND INTERNAL CONTROLS DIVISION		DOCUMENTATION WILL BE SENT BY LAST DAY OF
1. Memorandum to HSSOs and RAs requesting an update of Privacy Act systems of records under their jurisdiction.	C	Copy of memorandum	June 30, 2003
2. Update of Privacy Act systems of records on Privacy Act website on InSite.	C	Notification of updated Privacy Act systems of Records on Privacy Act website	August 31, 2003

ACTION PLAN

Designated Responding Official: **Gail T. Lovelace, Chief People Officer (CPO)**
Contact Person: **Fred Alt, CPO Chief Information Officer**
Telephone No.: **202-501-2518**

AUDIT REPORT NUMBER	RECOMMENDATION/ FINDING NUMBER	PROPOSED RECOMMENDATION/ FINDING COMPLETION DATE
A020256/O/T/F03005	3	**September 30, 2003**

RECOMMENDATION: That the CPO, with the assistance of the CIO, ensure that accountability and responsibility is assigned for identifying and implementing specific controls for each of GSA's Systems of Records.

Management Response:

The CPO concurs with this recommendation and will work with the CIO to include the assignment of accountability and responsibility for implementing controls for each of GSA's systems of records in the GSA Order that will be issued in response to Recommendation 1. The process and due dates will be the same as for Recommendation 1.

ACTION TO BE TAKEN STEP BY STEP	SUPPORTING DOCUMENTATION TO BE SENT TO AUDIT RESOLUTION AND INTERNAL CONTROLS DIVISION		DOCUMENTATION WILL BE SENT BY LAST DAY OF
1. Issue GSA Order mandating the Privacy Act clauses to be used in GSA's IT support contracts, along with policy and guidance on roles and responsibilities for safeguarding sensitive information by contractors and GSA employees.	C, with assist-ance of MV & I	Copy of GSA Order	September 30, 2003

IMPLEMENTATION REVIEW OF
CONTROLS FOR GSA'S PRIVACY ACT DATA
REPORT NUMBER A020256/O/T/F03005
DATED JANUARY 6, 2003
ASSIGNMENT NUMBER A060045

REPORT DISTRIBUTION

	Copies
Office of the Chief People Officer (C)	3
Office of the Chief Information Officer (I)	3
Office of Acquisition Policy (MV)	1
Counsel to the Inspector General (JC)	1
Regional Inspector General for Auditing (JA-W)	1
Assistant Inspector General for Auditing (JA and JAO)	2
Assistant Inspector General for Investigations (JI)	1
Audit Follow-up and Evaluation Branch (BECA)	1
Administration and Data System Staff (JAS)	1