FEDERAL ELECTION COMMISSION

OFFICE OF INSPECTOR GENERAL

FINAL REPORT

2007 Performance Audit of Privacy and Data Protection

December 2007

ASSIGNMENT No. OIG-07-02

FEDERAL ELECTION COMMISSION
WASHINGTON, D.C. 20463
Office of Inspector General

MEMORANDUM

TO: The Commission

FROM: Inspector General

SUBJECT: 2007 Performance Audit of Privacy and Data Protection

DATE: December 7, 2007

The Office of Inspector General (OIG) of the Federal Election Commission (FEC) contracted with Cotton & Company, LLP to conduct a performance audit of privacy and data protection policies and procedures and, specifically, to determine whether the FEC is complying with Section 522 of the Consolidated Appropriations Act, 2005 (42 U.S.C.A. § 2000ee-2). Section 522 requires an independent third-party review of the agency's use of personally identifiable information (PII)[1] and of its privacy and data protection policies and procedures at least every two years; this audit satisfies the required third-party review.

Audit Findings and Recommendations

The report contains recommendations to address weaknesses found by the auditors. The auditors reported seven separate findings and provided thirteen recommendations for improving privacy practices at the FEC. A table summarizing the findings and recommendations is included on page two of the report on the *2007 Performance Audit of Privacy and Data Protection* prepared by Cotton & Company. Management was provided a draft copy of the audit report for comment and generally concurred with the findings and recommendations. Management agreed with five findings but did not agree with the following two findings and the corresponding recommendations:

- Finding 4 - Privacy Roles and Responsibilities Are Not Adequately Documented (pages 15 through 17 of the audit report)

- Finding 6 - Privacy Impact Assessments Have Not Been Conducted (pages 19 – 20)

Management prepared a narrative response to all findings and recommendations presented in the report; the management response is included in Attachment 1 of the report, beginning on page 22. Based on management's response, Cotton & Company prepared additional responses for the two findings where management agreement was not reached; refer to pages 17 and 20 of the report.

The OIG agrees with all findings and recommendations presented by the auditors and the OIG believes the FEC's implementation of the independent auditor's recommendations will enable the FEC to reach an appropriate level of compliance with respect to privacy practices.

[1] See Attachment III of the audit report for a definition of personally identifiable information (PII) and other terminology contained in the audit report.

Audit Follow-up

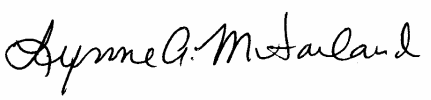
In accordance with Office of Management and Budget (OMB) Circular No. A-50, *Audit Follow-up*, revised, the FEC should develop a corrective action plan to set forth the specific action planned to implement the recommendations and the schedule for implementation. In addition, the OIG's *Internal Audit Process* specifies the corrective action plan, detailing planned implementation activities and dates, is due to the OIG within 30 days of receipt of this report. Lastly, FEC Directive 50, *Audit Follow-up*, states the Staff Director will recommend, and the Commission will approve, the audit follow-up official. Due to the Commission-wide implications of the audit recommendations, and the fact that management did not concur with all audit recommendations presented by Cotton & Company, the OIG recommends the Staff Director act as the audit follow-up official (AFO) for the audit.

As part of the OIG's audit contract with Cotton & Company, the agreement provides for a post-audit presentation with FEC officials to further expand on the findings and recommendations contained in the report. The presentation should be scheduled with the OIG and delivered prior to February 28, 2008. The AFO and/or Commissioners may wish to exercise this option in order to gain a further understanding of the findings and recommendations, in particular where management agreement was not reached. The post-audit meeting could be an opportunity to further the FEC's understanding of the audit findings, to include federal government privacy requirements, potential control frameworks, and tangible methods of improving privacy practices throughout the agency.

OIG Evaluation of Cotton & Company, LLP Audit Performance

In connection with the OIG's contract with Cotton & Company, we reviewed Cotton & Company's report and related documentation and inquired of its representatives. Cotton & Company is responsible for the attached auditor's report and the conclusions expressed in the report. The OIG's monitoring and review of Cotton & Company's work disclosed no instances where Cotton & Company did not comply, in all material respects, with generally accepted government auditing standards (GAGAS).

We appreciate the courtesies and cooperation extended to Cotton & Company and the OIG staff during the audit. If you should have any questions concerning the audit report, please contact my office on (202) 694-1015.



Lynne A. McFarland
Inspector General

Attachments

Cc: Staff Director
General Counsel
Associate General Counsel for Law and Advice
Chief Information Officer
Director of Human Resources

2007
PERFORMANCE AUDIT OF PRIVACY AND DATA PROTECTION

FEDERAL ELECTION COMMISSION

AUDIT REPORT NUMBER OIG-07-02

Cotton & Company LLP
Auditors · Advisors
635 Slaters Lane, 4th Floor
Alexandria, Virginia 22314
703.836.6701
www.cottoncpa.com

Cotton & Company LLP
635 Slaters Lane
4th Floor
Alexandria, VA 22314

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

December 7, 2007

Ms. Lynne A. McFarland
Inspector General
Federal Election Commission
999 E Street, NW
Washington, DC 20463

Subject: Report on the 2007 Performance Audit of the Federal Election Commission's Compliance with Section 522 of the Consolidated Appropriations Act, 2005 (42 U.S.C.A. § 2000ee-2)

Dear Ms. McFarland:

In accordance with terms of the subject task order, Cotton & Company LLP conducted a performance audit of privacy and data protection policies and procedures used by the Federal Election Commission (FEC). The audit included assessing compliance with applicable federal security and privacy laws and regulations as well as a review of the FEC's policies and procedures related to identifying and securing privacy-related data.

We interviewed key personnel involved in identifying and protecting personally identifiable information and reviewed documentation supporting the FEC's efforts to comply with federal privacy and security laws and regulations. We identified specific control weaknesses and deficiencies and developed recommendations designed to improve FEC compliance with federal privacy and security laws and regulations.

We conducted the performance audit in accordance with *Government Auditing Standards*. We were not engaged to and did not perform a financial statement audit, the purpose of which would be to express an opinion on specified elements, accounts, or items. This report is intended to meet the objectives described above and should not be used for other purposes.

We appreciate the opportunity to have worked with the FEC. Please call me if you have questions.

Very truly yours,

COTTON & COMPANY LLP

Loren F. Schwartz, CPA, CISA, CIPP
Partner

CONTENTS

Section	Page
Executive Summary	1
Background	4
Federal Election Commission	4
Federal Privacy Framework	6
Objectives, Scope and Methodology	8
Detailed Findings and Recommendations	10
1. A Comprehensive Inventory of Personally Identifiable Information Has Not Been Documented	10
2. Safeguards Over Sensitive Personally Identifiable Information Need Improvement	12
3. Privacy Policies and Procedures Have Not Been Approved and Implemented	14
4. Privacy Roles and Responsibilities Are Not Adequately Documented	15
5. Privacy Training Has Not Been Provided to FEC Employees and Contractors	17
6. Privacy Impact Assessments Have Not Been Conducted	19
7. Personnel Have Not Complied with FEC Computer Security Policy	21

Attachments	
1 Management's Response to Draft Report	22
2 Status of Prior-Year Privacy Findings and Recommendations	28
3 Definitions	31

2007
PERFORMANCE AUDIT OF
PRIVACY AND DATA PROTECTION

FEDERAL ELECTION COMMISSION

The Office of Inspector General (OIG) of the Federal Election Commission (FEC) contracted with Cotton & Company LLP to conduct a performance audit of privacy and data protection policies and procedures and, specifically, to determine if the FEC is complying with section 522 of the *Consolidated Appropriations Act, 2005*[1] (hereafter referred to as Section 522). This report is organized into the following sections:

- Executive Summary
- Background
- Objectives, Scope and Methodology
- Detailed Findings and Recommendations

EXECUTIVE SUMMARY

Section 522 requires certain agencies to assign a Chief Privacy Officer (CPO) who is responsible for identifying and safeguarding personally identifiable information (PII)[2]. Section 522 also requires an independent third-party review of agency use of PII and of its privacy and data protection policies and procedures at least every two years. This audit satisfies the required third-party review.

We provided a draft of this report to the FEC for comment. In addition, we met with FEC officials to discuss report findings and recommendations. The FEC's response is included as Attachment 1 to this report.

The FEC has made progress in addressing previously identified privacy weaknesses. Of the thirteen prior-year recommendations in the OIG's 2006 *Inspection Report on Personally Identifiable Information*, seven were closed as of our report date. The status of specific prior-year findings and recommendations is summarized in Attachment 2.

Our audit of the FEC's information privacy practices determined that, while progress has been made, significant additional work is still necessary to ensure that controls around PII in both paper and electronic form are implemented. Our findings and recommendations are summarized on the following page.

[1] 42 U.S.C.A. § 2000ee-2.
[2] See Attachment 3 for a definition of personally identifiable information (PII) and other terminology contained in this report.

Findings		Recommendations
1.	A Comprehensive Inventory of Personally Identifiable Information Has Not Been Documented	We recommend that the Chief Privacy Officer: 1a. Conduct a comprehensive review to identify and document all PII collected, processed, and stored within the FEC. 1b. Develop, document, and implement procedures for periodically updating the FEC's inventory of PII.
2.	Safeguards Over Sensitive Personally Identifiable Information Need Improvement	We recommend that the Chief Privacy Officer: 2a. Develop and implement a comprehensive data management framework to ensure that sensitive PII in both hard copy and electronic format is adequately identified (including its location within the FEC), secured, and properly disposed of when no longer needed. 2b. Develop a policy and procedures to ensure that the FEC's PII maintained or processed by third parties is adequately protected from unauthorized use or disclosure.
3.	Privacy Policies and Procedures Have Not Been Approved and Implemented	3. We recommend that the Chief Information Officer finalize, approve, and fully implement privacy policies, procedures, and directives in accordance with federal laws and regulations.
4.	Privacy Roles and Responsibilities Are Not Adequately Documented	We recommend that the FEC: 4a. Consider identifying one individual (position), such as the FEC Staff Director, as Chief Privacy Officer. 4b. Assign privacy roles and responsibilities to specific positions. In the event that the FEC continues with shared CPO and SAOP responsibilities, clearly delineate roles and responsibilities among individuals sharing these positions. 4c. Identify, document, and assign roles and responsibilities for monitoring compliance with federal and FEC privacy requirements.
5.	Privacy Training Has Not Been Provided to FEC Employees and Contractors	5. We recommend that the Chief Privacy Officer develop and implement privacy training for all FEC employees and contractors to ensure that personnel understand their privacy roles and responsibilities.
6.	Privacy Impact Assessments Have Not Been Conducted	We recommend that the FEC: 6a. Identify and implement a governance framework to ensure that controls within the FEC are appropriately identified, documented, and implemented. We recommend that the Chief Privacy Officer: 6b. Conduct privacy impact assessments in accordance with Section 522. 6c. Comply with OMB memorandums or, in the event of statutory exemption, document that sufficient controls exist to mitigate the need to comply. Where compliance is not adopted as the result of resource constraints, document the legal assessment, risk analysis, and cost-benefit to the FEC.
7.	Personnel Have Not Complied with the FEC Computer Security Policy	7. We recommend that the Chief Information Officer take necessary steps to ensure user compliance with FEC IT security policies and procedures.

The conditions represented by these findings appear to result from two primary causes:

- Lack of ownership over privacy within the FEC.
- Lack of an overall risk-based compliance and governance framework at the FEC.

First, without a single point of privacy ownership, there appears to be little urgency or accountability for moving forward with strong privacy practices. FEC privacy is co-owned by two individuals, and it is unclear who is responsible for specific management actions related to privacy. Best practice would assign a single member of management as owner for privacy and have that owner rely on other resources, as needed, to assist in legal or information technology matters.

Office of Management and Budget (OMB) Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*, states the following:

> *In furtherance of the Administration's commitment to protecting information privacy, OMB is today asking each executive Department and agency ("agency") to identify to OMB the senior official who has the overall agency-wide responsibility for information privacy issues. Consistent with the Paperwork Reduction Act, the agency's Chief Information Officer (CIO) may perform this role. Alternatively, if the CIO, for some reason, is not designated, the agency may have designated another senior official (at the Assistant Secretary or equivalent level) with agency-wide responsibility for information privacy issues. In any case, the senior agency official should have authority within the agency to consider information privacy policy issues at a national and agency-wide level.*
>
> *The senior agency official will have overall responsibility and accountability for ensuring the agency's implementation of information privacy protections, including the agency's full compliance with federal laws, regulations, and policies relating to information privacy, such as the Privacy Act. As is required by the Privacy Act, the Federal Information Security Management Act (FISMA), and other laws and policies, each agency must take appropriate steps necessary to protect personal information from unauthorized use, access, disclosure or sharing, and to protect associated information systems from unauthorized access, modification, disruption or destruction. Agencies are required to maintain appropriate documentation regarding their compliance with information privacy laws, regulations, and policies. And, agencies have the authority to conduct periodic reviews (e.g., as part of their annual FISMA reviews) to promptly identify deficiencies, weaknesses, or risks. When compliance issues are identified, agencies are obligated to take appropriate steps to remedy them.*

While OMB has suggested that the Chief Information Officer (CIO) may be designated as the Senior Agency Official for Privacy (SAOP), the FEC may be better served by having an individual in an operational senior management position (the FEC Staff Director for example) serving as the SAOP. The Staff Director position would have knowledge of operational issues within the FEC to make better risk-based decisions related to privacy and have authority to implement and enforce those decisions once they are made.

The lack of a risk-based compliance and governance framework at the FEC appears to be the second cause underlying the seven findings listed above, and a contributing cause for other internal control weaknesses previously reported by the FEC's Inspector General[3]. The FEC's Office of General Counsel (OGC) opined in September 2004 on the FEC's exemption from several important federal laws, regulations, and standards related to management controls and procedures for information technology (IT)

[3] *Federal Election Commission Performance and Accountability Report, Fiscal Year 2004, Inspector General Assessment of Major Performance and Management Challenges*, pages 111-115. http://www.fec.gov/pages/budget/fy2004/par_2004.pdf.

security. The basis for the exemption was primarily due to the FEC's exemption from the *Paperwork Reduction Act* (PRA), an act generally unrelated to IT security. Most federal IT security laws and regulations, such as the *Computer Security Act of 1987*, as amended, derive their authority from the PRA or other laws from which the FEC is exempt.

Specifically, the FEC's OGC concluded that the FEC was exempt from the *Computer Security Act of 1987*, a law that established minimum acceptable security practices for federal computer systems. In addition, the FEC was not required to follow Federal Information Processing Standards (FIPS) issued by the National Institute of Standards and Technology (NIST). FIPS are standards and guidelines pertaining to federal computer requirements. Finally, the FEC was exempt from the *Federal Information Security Management Act* (FISMA), a law followed by a majority of both small and large federal agencies and departments to provide information security for their operations and assets.

FEC decisions on whether to adhere to IT and privacy security federal government guidelines often appear to be made based on legal interpretations of laws and OMB memorandums, rather than on sound risk management. This is supported by evaluating the significant legal resources that management assigned to decision making compared with limited resources for risk management activities. A more specific example is management's decision not to perform privacy impact assessments. This decision was made based on an FEC OGC opinion that the FEC did not legally have to comply with this requirement, rather than on sound risk management.

Risk-based frameworks, such as those offered by the Committee of Sponsoring Organizations of the Treadway Commission (COSO, www.coso.org) and Control Objectives for Information and Related Technology (CobiT, www.isaca.org), present common definitions of internal controls, standards, and criteria against which companies and organizations can assess their control systems. Within the Executive Branch of the federal government, NIST has developed a thorough compliance framework based on risk.

The NIST framework encourages agencies to perform risk assessments and then make internal control decisions based on those risk assessments. NIST guidance is scalable for agencies both larger and smaller than the FEC. Adopting a framework, such as the one promulgated by NIST, would help to ensure that the FEC is adhering to best practice standards and maintaining, at a minimum, the same level of internal control as the Executive Branch of the federal government. Without a risk-based framework in place, management's ability to identify and measure the effectiveness of the FEC's internal control structure becomes more difficult.

Other federally appropriated organizations that are exempt from FISMA and NIST guidelines have formally adopted these requirements as a matter of best practice to help ensure that sound internal controls are established and followed. In summary, the FEC's legal exemption from FISMA and NIST guidance does not preclude the agency from formally adopting a FISMA-NIST based framework as a matter of best practice and good government.

BACKGROUND

Federal Election Commission

The FEC, an independent federal agency established by the Congress as a Commission, is responsible for administering and enforcing the *Federal Election Campaign Act* (FECA), 2 USC § 431. The FEC administers and enforces FECA through the three core programs of disclosure, compliance, and public financing.

- **Disclosure.** Disclosure involves receiving reports of campaign finance transactions by candidates and political committees involved in elections for federal office and promulgating them as part of the public record.

- **Compliance.** Compliance involves reviewing and assessing campaign finance transactions to ensure that filers abide by appropriate FECA limitations, prohibitions, and disclosure requirements. Compliance also involves oversight of individual contributors, corporations, labor unions, and "issue" groups that, although they may not fit within the universe of filers, can be involved in violations of FECA. The FEC has exclusive jurisdiction over civil enforcement of FECA and engages in civil enforcement proceedings to resolve instances of noncompliance.

- **Public Financing.** Public financing is the system for financing Presidential primaries, general elections, and national party conventions. Congress designed the program to correct campaign finance abuses perceived in the 1972 Presidential electoral process. The program combines public funding with limitations on contributions and expenditures. The program has three parts: (1) matching funds for primary candidates, (2) funds to sponsor political-party Presidential nominating conventions, and (3) funds for the general election campaigns of major party nominees and partial funding for qualified minor and new party candidates.

  Based on statutory criteria, the FEC determines which candidates and committees are eligible for public funds and funding amounts. The U.S. Treasury then makes the necessary payments. The FEC audits all committees that received public funds to ensure that committees used funds in accordance with the FECA, public funding statutes, and FEC regulations. Based on the FEC's audit findings, Presidential committees may be required to make repayments to the U.S. Treasury.

The FEC is headed by six commissioners appointed by the President and confirmed by the Senate. Commissioners serve six-year terms, and no more than three Commissioners may represent the same political party. By statute, the Commissioner chairmanship rotates every year, and the designated chairman has limited authority to set the agency's agenda.

Under the Commissioners, the FEC's organizational structure is separated into four primary offices:

- **Office of the Staff Director (OSD).** OSD is headed by a statutory officer. Subordinate organizations to the Staff Director are in most cases called "offices" for staff support activities and "divisions" for line activities involved in one or more of the three core programs. Programmatic elements under OSD include the Disclosure Division, Information Technology, Information Division, Press Office, Reports Analysis Division, and Audit Division.

- **Office of the General Counsel (OGC).** OGC is headed by a statutory officer. Subordinate offices to OGC are titled Associate General Counsels, and each supports one or more of the three core FEC programs.

- **Office of Inspector General (OIG).** OIG is headed by a statutory officer, the Inspector General, who reports directly to the Commission.

- **Chief Financial Officer (CFO).** The Office of the CFO is headed by the CFO. Subordinate offices include finance, procurement, and budget.

The FEC's privacy structure consists of a Privacy Officer, Co-Chief Privacy Officers (CPOs), and Co-Senior Agency Officials for Privacy (SAOP). The Privacy Officer position is held by the Associate

General Counsel (GC) for General Law and Advice (GLA), while the CPO and SAOP positions are shared by the GC GLA and Chief Information Officer (CIO). Responsibilities for privacy are separated into two areas, legal and technical; GC GLA handles legal issues, and the CIO handles technical issues.

Federal Privacy Framework

Privacy in the federal government is rooted in passage of the *Privacy Act of 1974*. Congress enacted the Privacy Act based on its understanding that:

1. The privacy of an individual is directly affected by collection, maintenance, use, and dissemination of personal information by federal agencies.

2. The increasing use of computers and sophisticated information technology, while essential to efficient government operations, has greatly magnified the harm to individual privacy that can occur from any connection, maintenance, use, or dissemination of personal information.

3. Opportunities for any individual to secure employment, insurance, and credit have a right to due process, and other legal protections are endangered by misuse of certain information systems.

4. The right to privacy is a personal and fundamental right protected by the Constitution of the United States.

5. To protect the privacy of individuals identified in information systems maintained by federal agencies, it is necessary for Congress to regulate collection, maintenance, use, and dissemination of information by such agencies.

The purpose of the *Privacy Act of 1974* is to provide certain safeguards for an individual against an invasion of personal privacy by requiring federal agencies, except as otherwise provided by law, to:

1. Permit an individual to determine what records pertaining to him/her are collected, maintained, used, or disseminated by such agencies.

2. Permit an individual to prevent records pertaining to him/her obtained by such agencies for a particular purpose from being used or made available for another purpose without consent.

3. Permit an individual to gain access to information pertaining to him/her in federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records.

4. Collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information.

Section 6 of the *Privacy Act of 1974* directed OMB to develop guidelines for agencies to use in the Act's implementation. Driven by the Privacy Act and recent high-profile incidents surrounding actual or potential privacy breaches or loss of sensitive PII, OMB has released a number of memorandums for agencies to follow in protecting PII, including:

- OMB Circular A-130, *Management of Federal Information Resources*, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals

- OMB Memorandum M-03-18, *Implementation of E-Government Act of 2002*

- OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*
- OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*
- OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*
- OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to Breach of Personally Identifiable Information*
- OMB Memorandum M-07-18, *Ensuring New Acquisitions Include Common Security Configurations*
- OMB Memorandum M-07-19, *Reporting Instructions for Federal Information Security Management Act and Agency Privacy Management*

In addition to the Privacy Act and OMB memorandums, Congress passed and the President signed into law the *Consolidated Appropriations Act, 2005* (Public Law 108-447), on December 8, 2004. Section 522 of this Act mandates of certain agencies the designation of a senior privacy official, establishment of privacy and data protection procedures, a written report by the agency on the use of information in an identifiable form,[4] independent third-party review of the agency's use of information in an identifiable form, and a report by the Inspector General to the agency head on the independent review and resulting recommendations.

Section 522 (d)(3) requires the Inspector General to contract with an independent third-party privacy professional to evaluate the agency's use of information in an identifiable form and privacy and data protection procedures. The independent review is to include (a) an evaluation of the agency's use of information in identifiable form, (b) an evaluation of the agency's privacy and data protection procedures, and (c) recommendations on strategies and specific steps to improve privacy and data protection management. Section 522 requires an independent third-party review at least every two years and requires the Inspector General to submit a detailed report on the review to the agency head. The independent third-party report and related Inspector General report are to be made available to the public through the internet.

Additional laws, regulations, and criteria released by Congress, OMB, and NIST related to privacy include:

- *The E-Government Act of 2002*, Section 208, HR 2458
- Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*

[4] Identifiable form is any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Personally identifiable information (PII) has a similar meaning and will be the term used throughout this document.

- NIST Special Publication (SP) 800-60, Volume I: *Guide for Mapping Types of Information and Information Systems to Security Categories*

- NIST SP 800-60, Volume II: *Guide for Mapping Types of Information and Information Systems to Security Categories*

OBJECTIVES, SCOPE AND METHODLOGY

The FEC's OIG contracted with Cotton & Company to conduct a performance audit of the agency's privacy and data protection policies and procedures and compliance with Section 522. Specific audit objectives were to:

- Determine the FEC's compliance with privacy requirements outlined in Section 522.

- Evaluate the FEC's use of information in identifiable form to ensure that the FEC's description of this use is accurate and accounts for the agency's current technology and its processing of information in an identifiable form.

- Evaluate the FEC's protection procedures of information in identifiable form to ensure that all technologies used to collect, use, store, and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy policies and practices governing collection, use, and distribution of information.

- Recommend strategies and specific steps to improve privacy and data protection management.

- Review the FEC's technology, practices, and procedures for collecting, using, sharing, disclosing, transferring, and maintaining security over information in identifiable form relating to agency employees and the public.

- Review the FEC's stated privacy and data protection procedures for collecting, using, sharing, disclosing, transferring, and maintaining security over information in identifiable form relating to agency employees and the public.

- Conduct a detailed analysis of the FEC's intranet, network, and websites for privacy vulnerabilities, including:

    - Noncompliance with stated practices, procedures, and policies.

    - Risks for inadvertent release of information in identifiable form from the agency's website.

In addition, because the FEC has determined that certain federal privacy laws and regulations do not apply to the agency due to specific exemption under the *Paperwork Reduction Act* (*E-Government Act of 2002* and a number of OMB regulations), Cotton & Company reviewed the FEC's internal legal assessments of compliance requirements for privacy regulations, laws, and other federal guidance to determine if we agreed with the FEC's assessment of exemptions. Specific laws and regulations reviewed included:

- Title V, Section 522 of the *Consolidated Appropriations Act, 2005*
- *Privacy Act of 1974,* 5 USC § 552a
- OMB memorandums related to privacy
- *E-Government Act of 2002,* H.R. 2458

The audit included a detailed analysis of the FEC's intranet and websites for privacy vulnerabilities, including noncompliance with stated policies, practices, procedures, and risks for inadvertent release of information in an identifiable form from the FEC website. Finally, we conducted a follow-up review of findings identified in the FEC OIG's 2006 *Inspection Report on Personally Identifiable Information*.

During our audit, we noted that the FEC had not adopted a compliance framework for privacy. Therefore, Cotton & Company chose a framework we consider to be a best practice with which to audit against. We based our audit on federal best practices, including NIST Special Publications, FIPS, and OMB memorandums and circulars.

Cotton & Company conducted the audit through the use of detailed interviews, questionnaires, and evaluations of FEC privacy and security policies, procedures, and directives. We conducted interviews to obtain an understanding of the types of information, including PII, handled by FEC personnel and to determine if management had identified and adequately protected sensitive PII. We interviewed key personnel from senior management and staff from various offices including the Office of the CFO, Office of the CIO, and OGC.

We developed and administered a questionnaire to a subjective population of FEC employees inquiring about their use of PII as part of daily work activities. Based on questionnaire responses, we followed up with additional interviews or emails to obtain further clarification and information about employee use of PII. The follow-up interviews or emails were to determine specifically if: PII was being used, processed, stored, or handled by FEC personnel; what controls, if any, were in place over PII; and whether PII identified was included in the FEC's system of records (SOR).

In addition, where sensitive PII was identified, we determined if management was aware that agency personnel had access to sensitive PII and if the FEC implemented adequate controls over the PII.

We conducted our audit in accordance with *Government Auditing Standards*, as promulgated by the Comptroller General of the United States for performance audits. We conducted this audit from September to November 2007. We were not requested to, and we cannot, express an opinion as it relates to any financial information or information security controls related to the FEC.

Based on audit results, Cotton & Company developed findings and recommendations for management, which are in the following section.

DETAILED FINDINGS AND RECOMMENDATIONS

Finding 1: A Comprehensive Inventory of Personally Identifiable Information Has Not Been Documented

The Chief Privacy Officer(s) have not developed and documented a comprehensive inventory of PII collected, processed, and stored by the FEC. The FEC's efforts to date have primarily been aimed at identifying PII or systems of record for inclusion in the SOR (required under the Privacy Act). The SOR identifies only systems or PII that meet all of the following criteria:

1. Does the system contain PII?
2. Is the system operated by or for the FEC?
3. Is the information searchable by name or unique identifier?
4. Is the information accessed regularly?

In addition to being limited to the four criteria above, the FEC's SOR does not describe PII collected, processed, or stored in sufficient detail to meet requirements of a PII inventory. A PII inventory should identify all PII and specifically document where the PII is being stored. The PII inventory description should include not only the PII office location, but precisely identify the locked room or cabinet in which PII is stored.

Finally, while the FEC's SOR does include general descriptions of how PII is being stored, such as in locked filing cabinets, on protected computer networks, or located in locked rooms, these descriptions do not identify which cabinets or rooms, and the descriptions were inaccurate in many cases, as shown by results of our after-hours walkthrough (see Finding 2).

Section 522 (a), Privacy Officer, states:

> *Each agency shall have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy, including – (7) ensuring that the Department protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.*

OMB Memorandum M-07-16, Section B.1, *Privacy Requirements - Review and Reduce the Volume of Personally Identifiable Information*, page 6, Review Current Holdings, states**:**

> *Agencies must now also review their current holdings of all personally identifiable information and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete, and reduce them to the minimum necessary for the proper performance of a documented agency function.*

OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*, page 1, states:

> *As is required by the Privacy Act, the Federal Information Security Management Act (FISMA), and other laws and policies, each agency must take appropriate steps necessary to protect personal information from unauthorized use, access, disclosure or sharing, and to protect associated information systems from unauthorized access, modification, disruption or destruction. Agencies are required to maintain appropriate documentation regarding their compliance with information privacy laws, regulations, and policies.*

Finally, the FEC's *Privacy Protection Policies and Procedures* (Draft), undated, Section VII, Security, states:

> *The FEC shall provide security protection for all records that contain personal information maintained in FEC's systems to ensure the accuracy, integrity and confidentiality of the records. The FEC's security protections for systems that store personal information shall include appropriate administrative, technical and physical safeguards such as:*
>
> *1. Physical security of both hard copy and electronic data;*
> *2. Personnel security for employee and contractor access to data;*
> *3. Network security for data in transit; and*
> *4. Secure and timely destruction of records.*
>
> *The security protection afforded each system shall be commensurate with the risk level and magnitude of harm the FEC and/or the record subject would face in the event of a security breach.*

Because management has focused its resources on updating the SOR, which is required under the Privacy Act, 5 USC § 552a, and has not focused on identifying all sensitive PII, regardless of whether it meets the four criteria identified by the FEC, we noted a significant amount of unprotected sensitive PII during our after-hours walkthrough. Without conducting a comprehensive review of all types of information received, processed, and stored by the FEC, management cannot ensure that all sensitive PII has been identified and adequate controls implemented to protect sensitive PII from unauthorized use, disclosure, or destruction. In addition, the likelihood of fraudulent activities is greater.

Recommendations

We recommend that the Chief Privacy Officer:

1a. Conduct a comprehensive review to identify and document all personally identifiable information collected, processed, and stored within the FEC. This inventory should be detailed enough to identify the information format (hard copy vs. electronic) and specifically identify where the information is maintained (cabinets, offices, storage rooms, etc).

1b. Develop, document, and implement procedures for periodically updating the FEC's inventory of PII.

Management Response

*Management **concurs** with this finding and stated they are in the process of finalizing their Plan to Review and Reduce Holdings of Personally Identifiable Information and Eliminate Unnecessary Use of Social Security Numbers. Prior to the development of this plan, the FEC distributed a survey to agency divisions to determine which divisions collect and use Social Security Numbers, the rationale for collection and use, necessity for this collection, and if alternate identifiers may be used. Initial survey results provided useful information and will assist FEC management in implementing the above-mentioned plan.*

Auditor Response: We look forward to following up with this matter in the future to ensure management's actions adequately address the weaknesses identified.

Finding 2: Safeguards Over Sensitive Personally Identifiable Information Need Improvement

Controls were not adequate to ensure that sensitive PII collected, processed, or stored by the FEC has been adequately safeguarded. We performed an after-hours walkthrough and identified instances in which PII was easily accessible to unauthorized personnel. Specific examples include:

- FEC employee timesheets, travel, and training records, including employee names, social security numbers, and birth dates, were stored in unsecured common-area desks and unlocked file cabinets.
- Candidate records and FEC audit work papers, containing names, addresses, phone numbers, canceled checks with bank account and routing numbers, and signatures were in unsecured common-area desks and cubicles.
- "Matter Under Review" (MUR) documentation, including banking information (checks and copies of checks showing routing and account numbers) were in unsecured areas, such as desks, unlocked common-area cabinets, and cardboard boxes in offices and common areas.
- Interoffice folders marked "confidential" containing possible PII regarding employees were in unsecured common-area mail slots and on common-area desks.
- CDs labeled "confidential" or marked with other information noting possible PII were in unlocked offices on desks.
- Outdated individual applications for FEC employment containing names, addresses, phone numbers, and social security numbers were retained in an unsecured office common area of a FEC program division.

In addition, the FEC has not adequately assessed controls over third-party systems housing FEC data for effectiveness. For example, the FEC has not performed a review to ensure that controls over the payroll system hosted by the National Finance Center (NFC) are in place and operating effectively.

The FEC's *Privacy Protection Policies and Procedures* (Draft), undated, Section VII, Security, states:

> *The FEC shall provide security protection for all records that contain personal information maintained in FEC's systems to ensure the accuracy, integrity and confidentiality of the records. The FEC's security protections for systems that store personal information shall include appropriate administrative, technical and physical safeguards such as:*
>
> *1. Physical security of both hard copy and electronic data;*
> *2. Personnel security for employee and contractor access to data;*
> *3. Network security for data in transit; and*
> *4. Secure and timely destruction of records.*
>
> *The security protection afforded each system shall be commensurate with the risk level and magnitude of harm the FEC and/or the record subject would face in the event of a security breach.*

Section 522, (a)(7), states:

> *Each agency shall have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy, including ensuring that the Department protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.*

OMB Memorandum M-05-08, page 1, states:

> *As is required by the Privacy Act, the Federal Information Security Management Act (FISMA), and other laws and policies, each agency must take appropriate steps necessary to protect personal information from unauthorized use, access, disclosure or sharing, and to protect associated information systems from unauthorized access, modification, disruption or destruction. Agencies are required to maintain appropriate documentation regarding their compliance with information privacy laws, regulations, and policies.*

The FEC does not have a comprehensive framework in place for effectively identifying, documenting, and protecting PII in both electronic and hard copy form. In addition, the CPO has not taken appropriate steps to identify where sensitive PII is used within the FEC and to ensure that business areas have effective policies, procedures, and practices in place to handle PII in their possession.

Section 522, (a)(1), states:

> *Each agency shall have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy, including assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of information in an identifiable form.*

Also, we concluded that FEC business areas (offices, divisions, and branches) have not clearly documented and implemented policies, procedures, and practices for handling the retention, storage, and destruction of sensitive PII. While management has identified PII for inclusion in the SOR and has implemented some high-level security controls (encryption and 2-factor authentication) over the FEC's computers, the CPO has not taken adequate steps to ensure that sensitive PII in both hard copy and electronic form within the FEC has been identified and adequately protected.

Without a comprehensive framework in place that ensures that sensitive PII has been identified and is being adequately protected, the risk of unauthorized access to sensitive PII increases. Unauthorized access to sensitive PII, such as social security numbers and banking information, could be used to commit identify theft or other fraudulent activities.

Recommendations

We recommend that the Chief Privacy Officer:

2a. Develop and implement a comprehensive data management framework to ensure that sensitive PII in both hard copy and electronic format is adequately identified (including its location within the FEC), secured, and properly disposed of when no longer needed.

2b. Develop a policy and procedures to ensure that FEC PII maintained or processed by third parties is adequately protected from unauthorized use or disclosure.

Management Response

*Management **concurs** with this finding and stated that they are reexamining their privacy program to ensure that policies, procedures, and guidelines to protect PII are at an acceptable level. In addition, representatives stated that they will again remind FEC employees of the importance of protecting PII and implement personalized training specific to the agency to assist each employee and contractor in understanding the critical importance of protecting PII.*

Auditor Response: We look forward to following up with this matter in the future to ensure management's actions adequately address the weaknesses identified.

Finding 3: Privacy Policies and Procedures Have Not Been Approved and Implemented

The FEC has not established and implemented comprehensive privacy and data protection policies and procedures governing the agency's collection, use, sharing, disclosure, transfer, storage, and security of information in identifiable form in accordance with Section 522.

The FEC's timeframe for complying with Section 522 requirements was delayed, in part, due to its effort to determine if the agency was subject to the Act. Management filed a privacy report with the OIG in compliance with Section 522 in February 2007. As of the completion of our audit, management was still in the process of developing draft policies, procedures, and directives, which, when finalized, must undergo Commission approval before being implemented.

The following privacy policies, procedures, and directives were in **draft** stage during our testing period:

- *Privacy Protection Policies and Procedures*
- *FEC Plan to Review and Reduce Holdings of Personally Identifiable Information and Eliminate Unnecessary Use of Social Security Numbers*
- *Privacy Rules of Conduct*
- *Designation of Chief Privacy Officer and Senior Agency Official for Privacy*
- *Policy and Plan for Responding to Breaches of Personally Identifiable Information* (finalized after audit testing period)

Section 522, (b), Establishing Privacy and Data Protection Procedures and Policies, states:

> *In general.--Within 12 months of enactment of this Act, each agency shall establish and implement comprehensive privacy and data protection procedures governing the agency's collection, use, sharing, disclosure, transfer, storage and security of information in an identifiable form relating to the agency employees and the public. Such procedures shall be consistent with legal and regulatory guidance, including OMB regulations, the Privacy Act of 1974, and section 208 of the E-Government Act of 2002.*

In addition, Section 522 (1), In General, states:

> *Within 12 months of enactment of this Act, each agency shall establish and implement comprehensive privacy and data protection procedures governing the agency's collection, use, sharing, disclosure, transfer, storage, and security of information in identifiable form relating to the agency employees and the public.*

The FEC's *Privacy Protection Policies and Procedures* (Draft), undated, Section VII, Security, states:

> *The FEC shall provide security protection for all records that contain personal information maintained in FEC's systems to ensure the accuracy, integrity and confidentiality of the records. The FEC's security protections for systems that store personal information shall include appropriate administrative, technical and physical safeguards such as:*
>
> *1. Physical security of both hard copy and electronic data;*
> *2. Personnel security for employee and contractor access to data;*
> *3. Network security for data in transit; and*
> *4. Secure and timely destruction of records.*
>
> *The security protection afforded each system shall be commensurate with the risk level and magnitude of harm the FEC and/or the record subject would face in the event of a security breach.*

Without clearly documented privacy policies and procedures, management cannot ensure that is has adequate controls in place over the use and protection of sensitive PII. In addition, without documented privacy policies and procedures to disseminate to the user community, management cannot ensure that employees and contractors understand their responsibilities for collecting, using, sharing, disclosing, transferring, storing, and securing sensitive PII.

For example, we noted an instance in which the FEC inadequately documented a recent security breach response. Management insufficiently documented its conclusion that a breach of sensitive PII did not occur. Specifically, the available documentation did not contain a clear description of the compensating controls that were in place to mitigate a potential release of sensitive PII. If the FEC's documented *Policy and Plan for Responding to Breaches of Personally Identifiable Information* had been in place at the time of the FEC's identification of the potential breach, and management had sufficiently completed an Identity Theft Risk Analysis, more information would have been available for the OIG and others to reach the same conclusion as management.

Recommendation

3. We recommend the Chief Information Officer finalize, approve, and implement privacy policies, procedures, and directives in accordance with federal laws and regulations.

Management Response

*Management **concurs** with this finding and stated they are in the process of finalizing agency privacy policies, procedures, and directives and expects to circulate final documents for Commission approval within the next 30 days.*

Auditor Response: We look forward to following up with this matter in the future to ensure management's actions adequately address the weaknesses identified.

Finding 4: Privacy Roles and Responsibilities Are Not Adequately Documented

The FEC's privacy roles and responsibilities have not been clearly documented and assigned in accordance with Section 522. CPO, PO, and SAOP roles and responsibilities have been documented in draft privacy policies and directives, but these have not been finalized and implemented.

In addition, the CPO and SAOP positions are being shared by the GC GLA and the CIO, although documented roles and responsibilities for the CPO and SAOP have not been specifically assigned. In

addition, while draft CPO roles and responsibilities do include responsibility for ensuring compliance with laws and regulations, draft policies and directives do not identify how compliance will be monitored or identify specific privacy monitoring activities for each of the CPOs. Based on interviews with each CPO, it was unclear who is ultimately responsible for ensuring compliance with privacy policies and procedures at the agency level.

Section 522, (a), Privacy Officer, states:

> *Each agency shall have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy, including –*
>
> 1. *assuring that the use of technologies sustain and do not erode, privacy protections relating to use, collection, and disclosure of information in an identifiable form;*
>
> 2. *assuring that technologies used to collect, use, store, and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use and distribution of information in the operation of the program;*
>
> 3. *assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as defined in the Privacy Act of 1974;*
>
> 4. *evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;*
>
> 5. *conducting a privacy impact assessment of proposed rules of the Department on the privacy of information in identifiable form, including the type of personally identifiable information collected and the number of people affected;*
>
> 6. *preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of section 552a of title 5, 11 United States Code, internal controls, and other relevant matters;*
>
> 7. *ensuring that the Department protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction;*
>
> 8. *training and educating employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies; and*
>
> 9. *ensuring compliance with the Departments established privacy and data protection policies.*

Section 522 (b), Establishing Privacy and Data Protection Procedures and Policies, states:

> *In general.--Within 12 months of enactment of this Act, each agency shall establish and implement comprehensive privacy and data protection procedures governing the agency's collection, use, sharing, disclosure, transfer, storage and security of information in an identifiable form relating to the agency employees and the public. Such procedures shall be consistent with legal and regulatory guidance, including OMB regulations, the Privacy Act of 1974, and section 208 of the E-Government Act of 2002.*

Without clear assignment of privacy roles and responsibilities to specific individuals, management's ability to hold individuals accountable to identify and protect PII is reduced. In addition, the lack of clearly defined responsibilities increases the risk that individuals will not take adequate measures to protect sensitive PII, because they are unaware it is their responsibility or they believe it was being performed by others.

Recommendations

We recommend that the FEC:

4a. Consider identifying one individual (position), such as the FEC Staff Director, as Chief Privacy Officer.

4b. Assign privacy roles and responsibilities to specific positions. In the event that the FEC continues with shared CPO and SAOP responsibilities, clearly delineate roles and responsibilities among individuals sharing these positions.

4c. Identify, document, and assign roles and responsibilities for monitoring compliance with federal and FEC privacy requirements.

Management Response

*Management **does not concur** with this finding. The FEC has given careful consideration in assigning shared CPO and SAOP responsibility and believes that no one person at the FEC could effectively handle this task. Management believes there are specific areas of expertise required on the legal side, as well as the IT side, that lend themselves to share duties by staff that have expertise in these areas. To the extent this finding is about the specificity of the assignment of other responsibilities in the draft document, the FEC will, of course, carefully consider the recommendations.*

Auditor Response: While management does not concur with our recommendation of assigning one Chief Privacy Officer, we do want to reiterate our belief that the effective management of privacy within the agency is best achieved when overall responsibility and accountability lies with one individual. Proceeding with Co-CPOs and Co-SAOPs will inherently increase the risk of specific activities related to the identification and protection of PII being inadequately addressed by management. With that being said, management should ensure privacy roles and responsibilities which do not easily fall under the legal or IT umbrella have been identified, documented in their privacy policies and clearly assigned to one of the Co-CPOs. Our audit clearly showed that responsibility for protection of hard copy PII which does not fall under the legal or IT umbrella had not been identified and assigned to either of the CPOs, and as a result, we found numerous instances where sensitive PII was unprotected and susceptible to theft.

Finding 5: Privacy Training Has Not Been Provided to FEC Employees and Contractors

The FEC has not adequately trained employees on privacy policies and procedures to promote awareness of and compliance with established privacy policies. Management has not completed development and delivery of privacy-specific training to FEC employees and contractors. The FEC has included limited privacy information in its annual security awareness training; this information was not, however, provided in adequate detail to address all appropriate privacy-related issues.

Section 522, (a)(8), Privacy Officer, states:

> *Each agency shall have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy, including training and educating employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies.*

In addition, the FEC's *Privacy Protection Policies and Procedures* (Draft), Section IX, Training, states:

> *It is essential that all FEC employees and contractors who come in contact with personally identifiable information and the systems that contain that information be aware of statutory and regulatory privacy requirements and FEC privacy policies and procedures. Training will be provided to all employees that come in contact with personally identifiable information or develop, manage, or maintain information systems that process and store personally identifiable information. Training will include the following:*
>
> 1. *The purpose and scope of the Privacy Act;*
> 2. *FEC Privacy Protection Policies and Procedures, including 11 C.F.R. Part 1 and the Breach Notification Policy and Plan;*
> 3. *Appropriate use and disclosure of records under the Privacy Act;*
> 4. *Security requirements for off-site computing;*
> 5. *Privacy Rules of Conduct, including the consequences for failure to follow the rules and available corrective actions; and*
> 6. *The possible criminal and civil penalties for violating the Privacy Act.*

While management is in the process of developing privacy specific training to deliver to FEC employees and contractors, the current lack of training increases the risk of sensitive PII being handled inappropriately.

In addition, without effective privacy training in place, employees may be unaware of FEC privacy policies and procedures, such as what constitutes sensitive PII, how to protect sensitive PII, and how to report potential breaches of sensitive PII. For example, of 69 individuals who responded to our privacy questionnaire, 30 (43 percent) did not recall receiving privacy training. Also, 41 respondents (59 percent) were unable to identify the individuals who hold the CPO position. Specifically,

- 22 did not correctly identify either of the CPOs (32 percent)
- 19 correctly identified only one of the two CPOs (27 percent)

Recommendation

5. We recommend that the Chief Privacy Officer develop and implement privacy training for all FEC employees and contractors to ensure that personnel understand their privacy roles and responsibilities. Privacy training topics should include identifying and protecting sensitive PII, and responding or reporting potential breaches of sensitive PII. Finally, privacy training should address the various practices and business needs within the FEC.

Management Response

*Management **concurs** with this finding. While they believe they have addressed protection of sensitive PII in security awareness training, issued guidelines for protecting PII, and followed up with emails and newsletters, management concurs that room for improvement exists regarding educating staff and contractors on their responsibilities for privacy. Management is developing a separate privacy education course outlining components necessary to ensure that all staff and contractors who have privacy responsibilities and access to PII are aware of their roles and responsibilities related to privacy and the need to protect PII during its entire lifecycle.*

Auditor Response: We look forward to following up with this matter in the future to ensure management's actions adequately address the weaknesses identified.

Finding 6: Privacy Impact Assessments Have Not Been Conducted

The FEC has not conducted privacy impact assessments in accordance with Section 522, Section (a)(5) as follows:

> *Each agency shall have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy, including conducting a privacy impact assessment of proposed rules of the Department on the privacy of information in an identifiable form, including the type of personally identifiable information collected and the number of people affected.*

The FEC conducted a legal review of this standard (privacy impact assessment) and concluded that this portion of the Consolidated Appropriations Act was grounded in FISMA, which the FEC has legally determined it is not required to follow.

While we are not disagreeing with that legal interpretation, management has not adopted a framework of compliance and governance related to privacy and information technology controls and instead is selective (generally based on legal decisions) with respect to which controls the FEC decides to implement.

FEC management has determined that since privacy impact assessments derive from the *E-Government Act of 2002*, (which the FEC is not subject to), it is not required to perform privacy impact assessments. We agree with this legal opinion. However, it is evident from management's approach to determining what privacy controls to implement, that management is concerned more with what it is legally required (hence the significant legal input into decisions), rather than what is the best course of action to take based on risk to the FEC.

Before determining if OMB-directed or -recommended activities are necessary to improve its privacy practices, the FEC's practice is to first assess whether the agency is legally required to comply by reviewing statutory authority under which the guidance is based. Where a decision is made that only partial compliance is required, we determined the legal assessments do not clearly define which activities will and will not be undertaken. Further, where a legal opinion is reached that compliance is not required (based on an assessment that a requirement is grounded in FISMA or another law), the FEC does not document whether existing privacy practices and controls mitigate the need to formally adopt the OMB requirements. Rather, the FEC relies on the legal opinion as to whether to direct resources toward those privacy activities.

The FEC's legal assessments have determined that the agency is not legally required to comply with any of the eight OMB privacy-related memorandums released since 2005 in their entirety. The FEC has decided, however, to adopt portions of six of the memorandums, either based on best practice or other

legal requirements. Of the remaining two, the FEC has determined exemption from one, and a final determination on compliance with the other, as a best practice, has yet to be finalized.

The *E-Government Act of 2002*, OMB memorandums, and other portions of the Executive Branch compliance framework are clear best practices in the government environment. While the FEC may be directly excluded from complying with FISMA and NIST guidance, other compliance frameworks exist that would meet organizational needs. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) model is a compliance and controls best practice framework in the corporate world. In addition, the Control Objectives for Information and Related Technology (CobiT) is an information technology governance process and often supports the COSO model. Both are internationally recognized and accepted frameworks for governance and control. By failure to adopt a framework, management is not able to make risk-based decisions regarding appropriate controls to implement.

Without a governance framework, management may be taking on more risk than it would otherwise want to accept or may be inefficient in the application of controls. Specifically, without a privacy impact assessment, the FEC cannot accurately assess where privacy-related risks exist. Sensitive PII may be compromised by exploiting these unprotected risks.

Recommendations

We recommend that the FEC:

6a. Identify and implement a governance framework to ensure that controls within the FEC are appropriately identified, documented, and implemented.

6b. Conduct privacy impact assessments in accordance with Section 522.

6c. Comply with OMB memorandums or, in the event of statutory exemption, document that sufficient controls exist to mitigate the need to comply. Where compliance is not adopted due to resource constraints, document the legal assessment, risk analysis, and cost-benefit to the FEC.

Management Response

*Management **does not concur** with this finding, stating that the recommendations in this finding will require careful consideration and may not ultimately be adopted precisely as set forth in the finding. In addition, management states that it does not perform privacy impact assessments due to limited resources, not based on legal opinion that the E-Government Act is not applicable to the FEC.*

Auditor Response: While management may be exempt from specific laws and regulations which outline security best practices, we believe management's fiduciary responsibility is to ensure adequate controls are in place to protect the FEC's information and information systems confidentiality, integrity, and availability. A security framework does not distinguish between what types of data it is protecting, but rather guides management in identifying, implementing, and monitoring the effectiveness of controls over information the agency determines to be important or sensitive. Examples of sensitive information can include not only privacy data, such as social security numbers and banking information, but also agency or company trade secrets and confidential business information. For this reason, we believe the best way to identify and protect PII, which was the focus of our audit, is to have a comprehensive security management framework in place.

Finding 7: Personnel Have Not Complied with FEC Computer Security Policy

The FEC's computer security policies were not being followed by FEC personnel. During an after-hours walkthrough of the FEC building, we identified the following:

- Employees left usernames and passwords written on notes within proximity to their computers.
- Employees left USB 2-factor privacy encryption authentication tokens unsecured in their laptops.

Federal Election Commission *Rules of Behavior and Acceptable Use Standards for Federal Election Commission Information and Systems Resources*, undated, Section 8.d, states:

> *Protect your password from disclosure. Specifically, do not post your password in your area.*

Section 18 states**:**

> *Protect FEC computing resources from theft or loss; take particular care to protect any portable devices and media entrusted to you, such as laptops, cell phones, palm-top computers, disks, CDs, and other portable electronic storage media.*

The FEC's *Mobile Computing Security Policy Number 58-4.3*, dated August 24, 2006, Section 2.a., states:

> *Portable computing devices and associated peripherals issued by the FEC should be viewed as government property that must be adequately protected from theft.*

Section 522, (a)(1), states:

> *Each agency shall have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy, including assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of information in an identifiable form.*

Passwords left on desks and USB tokens left in laptop computers in unsecured offices increase the likelihood that an individual with physical access may conduct unauthorized access of the laptop or other resources. As a result, unauthorized individuals may obtain sensitive PII and use the information for activities such as identity theft or fraud.

Recommendation

7. We recommend that the Chief Information Officer take necessary steps to ensure that users are complying with FEC IT security policies and procedures.

Management Response

*Management **concurs** with this finding and intends to address these physical security issues through an email to be sent to all staff the week of November 26, strong emphasis on privacy training now under development and in continued information systems security training; and other means and methods to be developed by the co-CPOs in conjunction with the FEC's physical security officer and other management officials.*

Auditor Response: We look forward to following up with this matter in the future to ensure management's actions adequately address the weaknesses identified.

ATTACHMENT 1
MANAGEMENT RESPONSES

Management Response to the Cotton & Company, LLP "2007 Report on Privacy and Data Protection"

We appreciate the opportunity to respond to the "2007 Report on Privacy and Data Protection," conducted pursuant to section 522 of the Consolidated Appropriations Act, 2005. We consider privacy to be a matter of great importance and have undertaken significant efforts to ensure compliance.

The FEC has always taken very seriously the need to protect the security and privacy of information in its possession. We are constantly aware that we possess sensitive information about individuals' involvement in activities that lie at the heart of the First Amendment. Our statute commands us, for example, not to make public information concerning ongoing enforcement matters, and our record of complying with this mandate over the past three decades is excellent. In the area of information systems security, we have taken many steps in the last four years to improve the security of sensitive and other electronic data, including 15 separate technical improvements such as two-factor authentication for employee laptops, upgrades to the majority of our server network operating systems, and installation of intrusion detection software; more extensive, and automated, user training in information security; and a continuous monitoring program that tests nine critical aspects of security or security response either annually or biannually.

We recognize that in the Internet age, special attention has to be devoted to specific concerns related to the privacy of information about individuals – both for the First Amendment-related reasons with which the Commission has always been concerned, and because of the potential for problems such as identity theft. We are at the beginning of our agency's privacy program, and we believe we have already accomplished a good deal given the limitations on our budgetary and human resources that we face as a small agency of fewer than 400 employees. Specific examples of what we have done and plan to do in the privacy areas are found in our responses to the specific audit findings.

We particularly welcome this audit, which we have always viewed as an opportunity to obtain a baseline that will assist management in working with the IG and with other stakeholders to improve the agency's privacy and data protection management. The importance we attach to privacy issues is reflected in this fact: in the entry conference for this audit, in October 2007, we were informed that so far as IG staff could determine, fewer than 10 agencies at that time had undertaken and made public the results of their section 522 audits. We believe that undergoing the audit process and publicizing its findings at this early stage of our privacy efforts underscores, particularly in comparison with other agencies, the FEC's commitment to enhance privacy protections within the bounds of our statutory mandate and the resources available to us.

We read the audit's seven findings as identifying four immediate and concrete, as opposed to conceptual, issues to be tackled: the development of an inventory of personally identifiable information (PII); the physical security of hard copies and portable electronic media containing PII; the finalization of privacy policies and procedures; and staff training. As of this writing, two of these issues should be addressed in very short order: all draft policies and procedures have now been forwarded to the Commission for its consideration, and privacy training for all employees is under development and calendared for the first quarter of 2008. As for the other two issues, we have already sent a Commission-wide message reporting the results of the auditors' walkthrough and reminding employees of their obligations concerning the physical security of their work areas, and, as set forth in our response to Finding 1, we believe we have made a strong start towards the development of a PII inventory.

We also believe that the co-CPO structure described in the report, and differed with by the auditors, is in large part responsible for our making as much progress as we have – both for the expertise-related reasons described in our response to Finding 4, and for the simple reason that the involvement of two teams has made more people (though still very few) available to work on privacy-related tasks than otherwise might have been available.

We look forward to giving careful consideration to all of the recommendations in the report, and implementing many of them. Our specific responses to the audit's findings follow.

Finding 1: A Comprehensive Inventory of Personally Identifiable Information Has Not Been Documented

Management concur - Yes

Management Response: We believe that the process of completing the SORNs provided a very good start to our PII inventory. In connection with that process, the FEC reviewed its holdings of agency records. The review revealed that the agency's most sensitive PII is covered by either a proposed FEC SORN or a government-wide SORN. In fact, the auditors have informed us that based on their survey of a sample of agency employees about PII; it appeared that all of the agency's most sensitive PII was covered by a SORN. Management knows with a fairly high degree of confidence which business units within the Commission collect and retain what kinds of PII and for what purposes. The PII identified during the after hours walkthrough, noted in "Effect" above, is not as much related to the issue of having an inventory, but rather, related to the issue of security, training, and implementation. Also, in compliance with OMB Memorandum 07-16 and additional implementation guidance from OMB staff, the FEC has already published, on the agency website, a schedule to periodically review agency holdings of PII. The PII review will cover all agency PII and not just the most sensitive agency PII contained in the SORNs. Moreover, the FEC is in the process of finalizing its Plan to Review and Reduce Holdings of Personally Identifiable Information and Eliminate Unnecessary Use of Social Security Numbers. Prior to the development of this plan, the FEC sent out a survey to agency divisions to determine which ones collect and use social security numbers, the rationale for collection and use, whether the collection is necessary, and whether alternate identifiers may be used. The initial survey results provided useful information and will assist us in implementing the above mentioned plan.

We anticipate that our efforts to inventory PII will also be assisted by the audit results, and by collateral benefits from contractor support now underway to enable the Commission to prepare for compliance with electronic discovery amendments to the Federal Rules of Civil Procedure.

However, a truly comprehensive inventory of all PII retained within the Commission may require contractor support when adequate financial resources become available.

Auditor Response: We look forward to following up with this matter in the future to ensure management's actions adequately address the weaknesses identified.

Finding 2: Safeguards Over Sensitive Personally Identifiable Information Need Improvement

Management concur - Yes

Management Response: Although FEC Management believes it does have controls in place to sufficiently protect PII it concurs that there is always room for improvement. With this in mind, the FEC is reexamining its Privacy Program to ensure that its policies, procedures, and guidelines to protect PII are at an acceptable level. In addition to this reevaluation, Management will again remind FEC employees of

the importance of protecting PII, and implement personalized training specific to the agency to assist each employee and contractor in understanding the critical importance of protecting PII.

In particular, we understand this Finding, and the results of the walkthrough, as raising a specific issue regarding the physical security of hard copy documents containing the most sensitive PII, as well as of electronic documents stored on portable media. Management plans to address this issue through an email that has already been sent to all staff about the walkthrough and its results; through particular emphasis in the privacy training now under development; and through consultation with the Commission's Administrative Officer, who is also the Commission's physical security officer, about other means and methods.

As mentioned in response to Finding 1, we anticipate that our efforts to conduct a more comprehensive inventory of PII will be assisted by the receipt of the audit results and by collateral benefits from contractor support now underway to enable the Commission to prepare for compliance with electronic discovery amendments to the Federal Rules of Civil Procedure. However, a truly comprehensive inventory of all PII retained within the Commission may require contractor support when adequate financial resources become available.

Auditor Response: We look forward to following up with this matter in the future to ensure management's actions adequately address the weaknesses identified.

Finding 3: Privacy Policies and Procedures Have Not Been Approved and Implemented

Management concur - Yes

Management Response: We are in the process of finalizing agency privacy policies, procedures and directives. The final documents have been circulated for Commission approval.

Auditor Response: We look forward to following up with this matter in the future to ensure management's actions adequately address the weaknesses identified.

Finding 4: Privacy Roles and Responsibilities Are Not Adequately Documented

Management concur - No

Management Response: The FEC has given careful consideration in making the decision to have Co-CPO's/SAOPs. We believe that no one person at the FEC could effectively handle this task. There are specific areas of expertise required on the legal side as well as the IT area that lends itself to share duties by staff that has expertise in these areas. In other words, the synergy currently in place makes the sum of the parts greater than the whole or just having one CPO/SAOP. The two skill sets provide for complimentary efforts that allows for collaboration of people with organizational and technical skills to get the job done. In fact, the partnership between the two positions (Associate General Counsel for General Law and Advice and the Chief Information Officer) allows for the perfect balance of expertise to ensure all aspects of privacy requirements are addressed.

The two individuals that hold these positions and their respective staff are working well together on privacy matters; each office brings vital expertise to the task of privacy protection that the other does not have; the structure is consistent with the organization of the agency itself, in which the General Counsel and Staff Director each report directly to the Commission; and in practical terms, designation of any official as a single Chief Privacy Officer/Senior Agency Official for Privacy will not remove from either OGC or ITD any of the privacy duties either office now performs. In essence this structure allows for

more people to be involved with shared ownership and accountability ensuring maximum effort is spent to address the critical tasks of protecting PII.

Obviously, some privacy duties will by their nature involve primarily legal issues, and those will be principally in the purview of the Associate General Counsel for General Law and Advice. Some will by their nature involve primarily issues of information technology or information systems security, and those will be principally in the purview of the Chief Information Officer. We note that in our draft privacy policy documents, duties regarding compliance with the Privacy Act of 1974 are assigned solely to the "FEC Privacy Officer," a position distinct from the CPO or SAOP that will be held solely by the Associate General Counsel for General Law and Advice. Certain other duties related to the acquisition and management of information technology and information resources, the development of a sound, secure and integrated IT architecture, and promotion of effective and efficient design and operation of all major information resources management processes are specified in the draft as assigned solely to the Chief Information Officer. To the extent this Finding is about the specificity of the assignment of other responsibilities in the draft document, we will, of course, carefully consider the recommendations.

Auditor Response: While management does not concur with our recommendation of assigning one Chief Privacy Officer, we do want to reiterate our belief that the effective management of privacy within the agency is best achieved when overall responsibility and accountability lies with one individual. Proceeding with Co-CPOs and Co-SAOPs will inherently increase the risk of specific activities related to the identification and protection of PII being inadequately addressed by management. With that being said, management should ensure privacy roles and responsibilities which do not easily fall under the legal or IT umbrella have been identified, documented in their privacy policies and clearly assigned to one of the Co-CPOs. Our audit clearly showed that responsibility for protection of hard copy PII which does not fall under the legal or IT umbrella had not been identified and assigned to either of the CPOs and as a result we found numerous instances where sensitive PII was unprotected and susceptible to theft.

Finding 5: Privacy Training Has Not Been Provided to FEC Employees and Contractors

Management concur - Yes

Management Response: The FEC has addressed the protection of sensitive information (PII) in its very extensive training on information systems security; issued guidelines for protecting sensitive information; and followed up with emails and newsletters. Nevertheless, the FEC concurs that there is room for improvement regarding educating staff and contractors on their responsibilities as it relates to privacy. To this end, the FEC is developing a separate privacy education course outlining the components necessary to ensure that all staff and contractors who have privacy responsibilities and access to PII are aware of their roles and responsibilities related to privacy and the need to protect PII during its entire lifecycle. This privacy education course not only incorporates strategies necessary to address the issues presented in this Finding but also ensures that the FEC has a documented mechanism in place to address future changes in the privacy landscape.

Auditor Response: We look forward to following up with this matter in the future to ensure management's actions adequately address the weaknesses identified.

Finding 6: Privacy Impact Assessments Have Not Been Conducted

Management concur - No

Management Response: Management does not concur simply by way of underlining that the recommendations in this Finding will require careful consideration, and may not ultimately be adopted precisely as set forth in the Finding.

The audit has found that we have not conducted privacy impact assessments, and this is correct. Privacy impact assessments are required by the E-Gov Act, from which the Commission is exempt. There is a similar requirement in Section 522 of the Consolidated Appropriations Act, 2005. As this particular portion of Section 522 appears to be largely duplicative of the E-Gov Act, the Commission has determined that it is also exempt from this provision of Section 522 (which otherwise generally applies to it). To conclude otherwise would be to defeat the purpose of the Commission's exemption from the E-Gov Act.

Nevertheless, this legal conclusion -- with which the audit report explicitly does not disagree -- is not the *reason* we do not conduct privacy impact assessments. Our concern, instead, is one of resources. Examples of other agencies' privacy impact assessments (PIA) that we have reviewed appear to be rather resource-intensive to produce. For instance, the Justice Department's instructions alone for completing PIAs run 21 single-spaced pages. We are a small agency, and do not have the resources to devote any employees to privacy duties on a full-time basis. Currently, all employees assigned privacy duties perform them as collateral duties. We concluded that the opportunity costs of delay in non-privacy projects on which staff would otherwise be working would outweigh whatever benefits we would receive from doing them. We will of course, however, carefully consider the recommendation regarding PIAs.

From the specific criticism of failure to conduct PIAs, the Finding expands its conclusion to a broader point, which is also addressed in the Executive Summary. As we understand it, the auditors recommend that to the extent the Commission chooses not to follow National Institutes of Standards and Technology guidance issued pursuant to the Federal Information Security Management Act (from which the Commission is also exempt), it should adopt what the Finding refers to as a formal "governance framework." Under such a framework, again as we understand it, privacy decisions (at a minimum) or all management decisions in the agency (ideally) would be assessed under, and be to some degree driven by, a formal risk assessment process. As an example of such a process, the Finding refers specifically to the "COSO" model ("Committee of Sponsoring Organizations of the Treadway Commission,") which we are informed is one such model adopted by many private sector entities in the wake of the Sarbanes-Oxley Act.

This is an area on which management will need to obtain more information. While we certainly understand the relevance of risk management concepts and processes to the potential danger of a loss of sensitive PII, we believe that recommendations about how the Commission assesses risk or makes management decisions in general are certainly at the edge of this audit's scope, and will require careful and deliberate consideration by the Commission itself and the agency's most senior management prior to any decision to implement the recommendation here.

It should be noted that the FEC has taken an industry best practice approach and adopted a risk based Information System Security Program. This risk based approach is outlined in 58A Information System Security Program Policy and specifically in 58-2.1 Risk Management Policy (both of which were provided to the auditors). In concert with its risk based approach and in accordance with industry best practice the FEC has developed a comprehensive certification and accreditation process which provides senior management with an accurate view of vulnerabilities and threats, risk evaluation and prioritization, risk mitigation strategies and any associated residual risk. Evidence of our adherence to a risk-based approach is indicated by contracting with an unbiased third party to conduct a series of formal risk assessments. These risk assessments are currently ongoing. The information obtained from these risk assessments will be utilized to develop, modify and implement any new policies, procedures and standards to improve the Commission’s protection of all sensitive information, including PII. The FEC’s risk-based model is based upon standard industry best practices and facilitates a cost effective methodology for senior management to evaluate security strategies to protect information commensurate with the information’s level of sensitivity.

Additionally, it should be noted that we have created and implemented 28 security policies and 14 security standards which we believe demonstrates that the agency is truly following best practices. With the current staffing and financial limitations we believe these safeguards provide an acceptable level of risk.

Auditor Response: While management may be exempt from specific laws and regulations which outline security best practices, we believe management's fiduciary responsibility is to ensure adequate controls are in place to protect the FEC's information and information systems confidentiality, integrity, and availability. A security framework does not distinguish between what types of data it is protecting but rather guides management in identifying, implementing, and monitoring the effectiveness of controls over information the agency determines to be important or sensitive. Examples of sensitive information can include not only privacy data, such as social security numbers and banking information, but also agency or company trade secrets and confidential business information. For this reason, we believe the best way to identify and protect PII, which was the focus of our audit, is to have a comprehensive security management framework in place.

Finding 7: Personnel Are Not Complying with FEC Computer Security Policy

Management concur - Yes

Management Response: This Finding raises issues similar to those raised by Finding 2 in that both involve the physical security of work stations and common areas. As stated in response to that Finding, management intends to address these physical security issues through an e-mail that has already been sent to all staff; through strong emphasis in the privacy training now under development and in continued information systems security training; and through other means and methods to be developed by the co-Chief Privacy Officers in conjunction with the Commission's physical security officer and other management officials.

Auditor Response: We look forward to following up with this matter in the future to ensure management's actions adequately address the weaknesses identified.

ATTACHMENT 2
STATUS OF PRIOR-YEAR PRIVACY FINDINGS AND RECOMMENDATIONS

Finding	Recommendation	Status
Confirm identification of personally identifiable information protection needs	Perform a risk assessment to examine the threats and vulnerabilities associated with remote access to Federal Election Commission (Commission) resources and physical removal of PII.	Open Management will perform risk assessments for major applications and the general support system (GSS) in the near future. An examination of threats and vulnerabilities associated with remote access to FEC resources and physical removal of PII will be included in the GSS risk assessment.
	Perform a complete inventory of Commission assets clearly identifying which employees have custody over these assets with emphasis on removable portable devices; the make, build and configuration of these portable devices and which devices have been encrypted and/or password-protected.	Closed Management provided the audit team with a comprehensive inventory of all laptops and Blackberry devices including whom it was issued to, model, serial, and barcode numbers, and if the device is password protected, encrypted, and has 2-factor authentication.
	Implement technical and/or policy controls to prevent access to the Commission's resources for non-encrypted laptops either locally or remotely.	Open Management is in the process of implementing a network access control device that will deny or restrict access to the FEC's network for devices not in compliance with the FEC's policies and minimum settings. This device will not, however, be implemented until calendar year 2008.
	Implement password protection for personal digital assistants (PDAs) that have access to Commission email and other sources of sensitive information.	Closed
Verify adequacy of organizational policy	Update the Mobile Computing Security Policy to more accurately reflect which systems will be encrypted and which ones will be password protected in order to remove any ambiguities in the policy. Management should incorporate explicit rules for determining if remote access is allowed, user training and accountability measures in place to ensure that remote use of PII does not result in bypassing management controls.	Open Management did not change the *Mobile Computing Security Policy* to clarify which systems will be password protected and which will be encrypted. The policy states that "all mobile computing devices including Blackberries and Palm Pilots must be encrypted and/or password protected." The FEC stated that laptops must be encrypted and password protected while other devices, such as Blackberries and Palm Pilots, only need to be password protected. This is still, however, unclear in the policy.

Finding	Recommendation	Status
Implement protection for personally identifiable information being transported and/or stored offsite	Implement a review process to ensure FEC users have effectively downloaded and installed the encryption software and measures are in place to prevent possible circumvention of these safety precautions.	Closed
	Test and document results of all pre-deployment testing performed by the Information Technology Division to ensure the selected encryption software is compatible for FEC use.	Closed
Implement protections for remote access to personally identifiable information	Complete the implementation of the USB two-factor authentication devices.	Closed
	Update Commission mobile computing security policies to include procedures for downloading and remote storage of data.	Open Management did not change the *Mobile Computing Security Policy* to include procedures for downloading and remote storage of data. Users are periodically reminded to save files to the network through emails and newsletters. The policy has not, however, changed.
Additional Agency Requirements	Implement encryption technology on identified portable devices.	Closed Encryption technology has been installed on FEC laptops. Management provided the audit team with a comprehensive inventory of all laptops and Blackberry devices including whom it was issued to, model, serial, and barcode numbers, and if the device is password protected, encrypted, and has 2-factor authentication. We noted that there are several Apple laptops in use which do not have PGP encryption installed. However, the FEC stated that "no sensitive data is saved or accessed on the Apple laptops." Further, FEC also stated that "Apple users were not issued property passes," thereby restricting removal of the laptops from the FEC premises. OMB Memorandum M-06-16 allows this written permission. We verbally informed management that this approval should be in writing.
	Implement password protection on peripheral portable devices (Palm Pilots, Blackberries, etc)	Closed

Finding	Recommendation	Status
	Implemented a timeout feature for laptops/desktops which will timeout after 30 minutes of inactivity. [No timeout feature is in place for other peripheral devices.]	Open We reviewed the Blackberry server settings and noted that the timeout is set at 60 minutes instead of 30 minutes. In addition, users have the ability to change the timeout setting.
	Log all computer-readable data extracts, as comprehensive implementation of encryption on all portable computers will ensure PII is adequately protected	Open Management considers logging all computer readable data extracts as neither feasible nor reasonable and therefore does not intend to complete this recommendation.

ATTACHMENT 3
DEFINITIONS

Individual: A citizen of the United States or an alien lawfully admitted for permanent residence.

Information in Identifiable Form: Information in an IT system or online collection (a) that directly identifies an individual (name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (b) by which an agency intends to identify specific individuals in conjunction with other data elements (indirect identification). These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.

Personally Identifiable Information (PII): Any piece of information that can potentially be used to uniquely identify, contact, or locate a single person. Information such as social security numbers and banking information are generally considered sensitive.

Privacy Impact Assessment (PIA): Analysis of how information is handled (a) to ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (b) to determine risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy Policy in Standardized Machine-Readable Format: A statement about site privacy practices written in a standard computer language (not English text) that can be read automatically by a web browser.

System of Records (SOR): 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.

System of Records Notice (SORN): 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 that is required to be published in the federal register in accordance with the 1974 Privacy Act.