FEDERAL ELECTION COMMISSION

OFFICE OF INSPECTOR GENERAL

FINAL REPORT

2010 Follow-up Audit of Privacy and Data Protection

March 2011

ASSIGNMENT No. OIG-10-03

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

MEMORANDUM

TO: The Commission

FROM: Inspector General

SUBJECT: Follow-up Audit of Privacy and Data Protection

DATE: March 31, 2011

This memorandum transmits the Federal Election Commission (FEC) Office of Inspector General's (OIG) final report of the *Follow-up Audit of Privacy and Data Protection* prepared by Cherry, Bekaert & Holland (CBH). The OIG contracted with CBH to perform a follow-up audit on the findings and recommendations identified in the *2006 Inspection Report on Personally Identifiable Information* and the *2007 Performance Audit of Privacy and Data Protection*. CBH's objective was to determine whether management implemented the agreed upon actions for each recommendation and whether each audit finding in the two prior reports have been fully resolved.

Audit Findings and Recommendations

CBH's review identified that management has made some improvements since the *2006 Inspection Report on Personally Identifiable Information* [PII] and *2007 Performance Audit of Privacy and Data Protection.* However, sixteen (16) of nineteen (19) previous recommendations are still open and new recommendations have been added. Thus, several existing and emerging risks to PII, and privacy and data protection have not been identified and addressed.

Significant issues within this report address the progress of the FEC's privacy and data protection program, and the protection of PII within the agency. The FEC's current governance structure over the privacy and data protection program consists of the Co-Chief Privacy Officers (CPOs) who share privacy and data protection responsibilities. This approach of shared responsibilities, along with the CPOs' other full-time responsibilities, prevents efficient and effective progress of the privacy and data protection program. Without one full-time person committed to ensuring: (1) proper handling of PII within the agency; (2) the FEC adheres to all required federal regulations; and (3) adequate oversight and monitoring of the privacy and data protection program, the FEC will continue to face greater challenges and continuous risk to the agency, which is reflected throughout the issues in this report.

The OIG's 2007 contracted audit firm, as well as CBH and my office, believe that the Commission should appoint a single Chief Privacy Officer, as intended by law. The

Chief Privacy Officer would continue to be supported by the FEC Privacy Team, both for technical and legal guidance. We acknowledge the current budget environment is challenging, and therefore if a full-time CPO position cannot be justified, that serious consideration be given to detailing an existing FEC staff person, with the knowledge and/or aptitude in privacy, to assume primary responsibility for FEC privacy.

Audit Follow-up

In accordance with FEC *Directive 50,* Audit Follow-up, the next step of the audit process will be for the Staff Director to recommend, and the Commission approve, the Audit Follow-up Official (AFO). The AFO is responsible for the development of management's corrective action plan (CAP) to address the findings and recommendations identified in the audit report. In addition, the AFO is responsible for finalizing the CAP to be provided to the Commission. Due to the number of issues identified in the report, the OIG is recommending an extended schedule to provide management sufficient time to finalize an effective CAP. The OIG recommends management develop a CAP within 45 days from the issuance of this report, or by May 16, 2011, and provide the CAP to the OIG for review and comment. The OIG will provide comments to management and the CAP should be finalized by management and transmitted to the Commission by May 31, 2011.

OIG Evaluation of Cherry, Bekaert & Holland (CBH) Audit Performance

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

We appreciate the courtesies and cooperation extended to Cherry, Bekaert & Holland and the OIG staff. If you should have any questions concerning this report, please contact my office on (202) 694-1015. Thank you.

Lynne A. McFarland
Inspector General

Attachment

2010 FOLLOW-UP AUDIT OF PRIVACY AND DATA PROTECTION

FEDERAL ELECTION COMMISSION

AUDIT REPORT NUMBER OIG-10-03

Cherry, Bekaert & Holland, L.L.P.
1834 Gallows Road – Suite 400
Vienna, VA 22182
www.cbh.com

Cherry, Bekaert & Holland, L.L.P.
The Firm of Choice.
www.cbh.com
1834 Old Gallows Road – Suite 400
Vienna, Virginia 22182
Phone 703.506.4440
Fax 703.506.8817

March 29, 2011

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

Subject: 2010 Follow-up Audit Report on Privacy and Data Protection

Dear Ms. McFarland:

In accordance with the terms of the task order, Cherry Bekaert & Holland LLP conducted a follow-up audit of the findings and recommendations included in the *2007 Performance Audit of Privacy and Data Protection,* and the *2006 Inspection Report on Personally Identifiable Information* for the purpose of determining the status of the corrective actions for the findings noted in these reports.

We interviewed key personnel involved in identifying and protecting personally identifiable information and reviewed documentation supporting the FEC's efforts to address the findings and recommendations contained in the reports referenced above. During the course of our review, we identified additional specific control weaknesses and deficiencies and developed recommendations designed to improve the FEC's privacy program and compliance with federal privacy and security laws and regulations.

We conducted this follow-up audit in accordance with *Government Auditing Standards*. This report is intended to meet the purpose described above and should not be used for other purposes.

We appreciate the opportunity to have served the FEC Office of Inspector General.

Very truly yours,

John Montoro
Partner

CONTENTS

Section		Page
Executive Summary		1
Background		9
Federal Election Commission		9
Federal Privacy Framework		10
Objectives, Scope and Methodology		12
Detailed Findings and Recommendations		14
1.	Privacy Roles and Accountability	14
2.	Privacy Impact Assessments Have Not Been Conducted	17
3.	Monitoring and Review of Regulatory Requirements	20
4.	A Current PII Inventory is Not Maintained	22
5.	Current Risk Assessments of Systems Containing PII Are Not Performed	26
6.	Mobile Computing Policy, Device Encryption and Controls	28
7.	Safeguards Over Sensitive Agency Information and PII Need Improvement	37
8.	Lack of Detailed Procedures and Periodic Review	45
9.	Logging	49
10.	Protections for Remote Access to PII	52
11.	Vendor Due Diligence	54
12.	System of Records Notice (SORN) Updates	57
13.	Training Workstations	61

Attachments

1. Cover Memo To Management Responses to the Cherry, Bekaert & Holland LLP 2010 Follow-up of the 2007 Performance Audit of Privacy and Data Protection Report	63
2. Status of 2006 and 2007 Privacy Findings and Recommendations	65
3. Definitions	72
4. Executive Order 13556 Controlled Unclassified Information	73

2010
FOLLOW-UP AUDIT OF PRIVACY AND DATA PROTECTION

FEDERAL ELECTION COMMISSION

The Office of Inspector General (OIG) of the Federal Election Commission (FEC) contracted with Cherry Bekaert & Holland LLP to conduct a follow-up audit of the *2007 Performance Audit of Privacy and Data Protection*, and the *2006 Inspection Report on Personally Identifiable Information* and, specifically, to determine if the FEC has adequately implemented the agreed actions for each recommendation and whether each audit finding has been fully resolved. This report is organized into the following sections:

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

EXECUTIVE SUMMARY

The importance of data protection and privacy within the Federal government and commercial enterprises is constantly increasing and requires continuous attention. The challenges will be even greater in the future as the potential use of new technologies (e.g., cloud computing, more prolific use of wireless mobile computing devices) and changes to business processes and work arrangements (e.g., increased focus on telework) will create new risks to be managed. There is also a general increasing concern among individuals about the use and privacy of their personal information controlled by Federal agencies. For any entity handling personally identifiable information (PII), the effort to sustain an effective and defensible privacy program that meets the public's expectations and applicable legal requirements can be a substantial task.

Based on our observations during this follow-up audit, we do not believe that the current shared approach to privacy and data protection used by the FEC adequately addresses the current needs of the agency and there is no reason to believe it will meet future challenges if changes are not made. The FEC currently uses a team approach to privacy and data protection which is lead by two co-Chief Privacy Officers (CPOs) and supported by the Information Systems Security Officer (ISSO) and two members of the Office of General Counsel, collectively referred to as the "Privacy Team." All of the team members have privacy as a "collateral duty" to their main roles and responsibilities and can only spend a minimum amount of their time on privacy matters. While privacy and data protection is a multi-disciplinary subject that requires the input from various departments and subject matter experts, the lack of a single full-time CPO is unique when compared to other Federal agencies and commercial enterprises of similar size and was a finding in the previous audit in 2007.

It is our opinion, and the opinion of the prior auditors, that the current approach of having co-CPOs with privacy as a minimal collateral duty is fundamentally flawed. The model of shared responsibility has limited the FEC's privacy program progress and prohibits the FEC from maturing the privacy program beyond reacting to audit findings and legislative requirements. Despite the substantial budget constraints, we recommend that the FEC change the current approach and appoint one full-time CPO to lead the FEC's privacy and data protection program. The CPO should be the single accountable individual for privacy and data protection that can be supported by the subject matter expertise and experience of the existing Privacy Team members. In addition, a formal governance framework to identify, monitor and measure risk and program metrics is required to provide the appropriate structure and accountability. These two recommendations are consistent with those noted in the *2007 Performance*

Audit of Privacy and Data Protection, with which management disagreed and did not implement. This is the third independent review of the FEC's privacy and data protection program since 2006. The FEC also engaged consultants to assist in certain necessary privacy and data protection initiatives since 2007 and has spent approximately $875,000 on these audits and consultant efforts, yet many of the previous audit recommendations are not addressed. Sixteen (16) of nineteen (19) previous recommendations are still open and many new recommendations have been added.

During our review, we did note that there have been improvements since the *2007 Performance Audit of Privacy and Data Protection.* Specifically, important progress included: developing and approving policies; completing an inventory and risk assessment of internal PII repositories in May 2009; deploying security and privacy training in 2008; executing application vulnerability and penetration tests on an annual basis; and enhancing physical security measures within the FEC. However, fundamental activities such as updating and maintaining the inventory of PII and risk assessments have not occurred. In addition, the PII inventory and risk assessment report provided by the consultant in May 2009 included important recommendations that have not yet been addressed by the FEC. The PII inventories and associated recommendations for each division were not provided to division management, despite being completed almost two years ago, along with a request to validate the inventories, update and maintain listings, and respond to recommendations specific to the division. Thus, existing and emerging risks to PII have not been identified and addressed.

The table on the following pages summarizes the current findings and recommendations, and whether management concurred with those recommendations.

Summary of Findings, Recommendations and Management Concurrence

Findings		Recommendations		Management Concurrence
1.	Privacy Roles and Accountability (Repeat finding)	We recommend that the FEC:		
		1a.	Assign privacy roles and responsibilities to one individual CPO with high level sponsorship in the Commission. If the Commission decides to continue with two CPOs and SAOPs, roles and responsibilities under these titles should be clearly delineated between individuals sharing the positions.	1a. Management does not concur.
		1b.	Identify, document in position descriptions and performance plans, and assign specific roles and responsibilities for the monitoring and reporting of compliance with Federal and Commission privacy requirements.	1b. Management does not concur.
2.	Privacy Impact Assessments Have Not Been Conducted (Repeat finding)	We recommend that the FEC:		
		2a.	Conduct privacy impact assessments in accordance with Section 522, or create an alternative process for ensuring that privacy risks associated with PII are documented, assessed and remediated as necessary.	2a. Management concurs in part.
		2b.	Comply with OMB memoranda, or in the event of statutory exemption and a decision not to voluntary comply, document that sufficient controls exist to mitigate the need to comply. Where compliance is not adopted due to resource constraints or other reasons, document the legal assessment, risk analysis, and cost-benefit to the FEC.	2b. Management concurs in part.
		2c.	Identify and implement a governance framework (e.g., NIST, the AICPA's Generally Accepted Privacy Principles (GAPP)), to ensure that controls within the FEC to protect PII are appropriately identified, documented, and implemented.	2c. Management concurs in part.
3.	Monitoring and Review of Regulatory Requirements (Repeat finding)	We recommend that the FEC:		
		3a.	Develop a process and assign accountability for the proactive and timely identification of new OMB memoranda, Executive Orders, and other guidance to ensure that they are reviewed and referred for legal opinion on a timely basis.	3a. Management concurs.
		3b.	Complete legal reviews of OMB memoranda and other guidance on a more timely basis and consistently communicate the results to the affected stakeholders, with a copy to the co-Chief Privacy Officers.	3b. Management concurs in part.
4.	A Current PII Inventory is Not Maintained (Repeat finding)	We recommend that the FEC:		
		4a.	Update and maintain the inventory of all systems that contain PII for all the divisions. A potential approach is to use the templates created by Solutions Technology Systems, Inc. (STSI) and have each division update their current listing and implement business processes to continually update the inventory based on new or revised handling and storage of PII. A full review could be conducted by the divisions at least annually and will help support the biennial Privacy Act Systems of Records update process.	4a. Management concurs in part.

Summary of Findings, Recommendations and Management Concurrence

Findings		Recommendations		Management Concurrence
		4b.	Finalize the evaluation of the draft STSI recommendations and develop, document and implement a corrective action plan as necessary. Progress against the corrective action plan should be formally and periodically reported to management.	4b. Management concurs.
		4c.	Provide the Privacy Team's SSN Reduction Plan Phase 1 report to the applicable division heads, and work with those offices to prepare action plans to address the findings in the report.	4c. Management concurs.
		4.d	Complete Phase 2 and Phase 3 of the "FEC's Plan to Review and Reduce Holdings of Personally Identifiable Information and Eliminate Unnecessary Use of Social Security Numbers In Response to OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information" as soon as practical. This can be accomplished by providing the STSI results to the divisions and requesting a response on the ability to reduce or eliminate the questionable uses of social security numbers already identified by the contractor.	4d. Management concurs in part.
5.	Current Risk Assessments of Systems Containing PII Are Not Performed (Modified repeat finding)	We recommend that the FEC:		
		5a.	Perform a risk assessment annually for all existing and new applications that collect, process, transmit or store PII. If privacy impact assessments (PIAs) were performed, a risk assessment component could be built into that process to accomplish both the PIA and risk assessment recommendations.	5a. Management concurs in part.
		5b.	Prepare a documented corrective action plan for any deficiency noted for each risk assessment performed and report progress periodically until all corrective actions are implemented. The corrective action plan should be approved by management.	5b. Management concurs in part.
		5c.	Include all systems containing PII that are being retired in the risk assessments and develop action plans to ensure the proper transfer of PII to a new system or the secure destruction of the PII in the retired system.	5c. Management concurs in part.
6.	Mobile Computing Policy, Device Encryption and Controls (Repeat finding)	We recommend that the FEC:		
		6a.	Modify the *Federal Election Commission Mobile Computing Security Policy*, Policy Number 58-4 to require all mobile devices, including Blackberrys, be encrypted.	6a. Management concurs in part.
		6b.	Revise the Policy Number 58-4 to specify when exceptions to policy may occur, who may approve the exception, the risks to PII if an exception is granted and any compensating controls, and the level of documentation required to support the exception.	6b. Management concurs in part.
		6c.	Record all mobile computing devices in inventory when received after purchase instead of when issued.	6c. Management does not concur.

Summary of Findings, Recommendations and Management Concurrence

Findings		Recommendations		Management Concurrence
		6d.	Perform a review of the process and systems used to maintain the inventory of mobile devices to ensure that they are appropriately designed to maintain a complete and accurate inventory. A complete physical inventory of all mobile devices ***purchased*** less those ***disposed*** should be performed and reconciled to the existing mobile device inventory listing.	6d. Management does not concur.
		6e.	Include a record in the inventory of whether the device is encrypted or not.	6e. Management does not concur.
		6f.	Implement a process and form requiring employees and contractors to sign when they receive a mobile device acknowledging their receipt of the asset and maintain a record of these sign-offs.	6f. Management does not concur.
		6g.	Implement an alternative to assigning a generic laptop encryption passphrase to contractors so that every contractor has a unique self selected passphrase, while maintaining the ability to decrypt the stored data in the event of an unexpected departure. The ability to recover unencrypted data of an employee should also be in place.	6g. Management concurs.
7.	Safeguards Over Sensitive Agency Information and PII Need Improvement (Repeat finding)	We recommend that the FEC:		
		7a.	ISSO, Physical Security Officer, and/or division management should conduct regular FEC office walkthroughs to ensure that agency staff comply with privacy and information security standards.	7a. Management concurs.
		7b.	Should emphasize document labeling requirements for documents with PII or sensitive information with all staff and standard document templates with labels be created and the use monitored.	7b. Management does not concur.
		7c.	Should develop a plan to implement Executive Order 13556, *Controlled Unclassified Information*, and comply with future directives issued by NARA.	7c. Management concurs in part.
		7d.	Division managers should work with the Physical Security Officer and the Records Officer to assess records management and secure storage needs and address failures to adequately secure sensitive information noted during the walkthrough.	7d. Management concurs.
		7e.	Contracting Officer and COTRs should enforce the requirement for contractors to certify secure destruction or return of FEC information in both paper and electronic format.	7e. Management concurs.
		7f.	Should establish a policy and procedures requiring COTRs to inspect the physical space occupied by contractors when the contractor departs to ensure paper and electronic records are securely disposed of or filed.	7f. Management concurs.
		7g.	Should implement the plan to develop and deploy privacy training specific to the individual divisions.	7g. Management concurs.

Summary of Findings, Recommendations and Management Concurrence

Findings		Recommendations		Management Concurrence
8.	Lack of Detailed Procedures and Periodic Review (Modified repeat finding)	We recommend that the FEC:		
		8a.	Should develop, implement and communicate detailed procedures to all employees for each security and privacy related policy. This may need to occur at the division or department level with the Privacy Team serving as subject matter experts. Detailed procedures will also be helpful for agency staff tasked with monitoring, enforcing and reporting on compliance with the requirements in the associated policies.	8a. Management concurs in part.
		8b.	Should directly link detailed procedures to the source policies and house them in a central, easily accessible location, such as the FEC Intranet.	8b. Management concurs.
		8c.	Should follow a standard template for all policies and supporting documents that includes an adoption and last revision date.	8c. Management concurs in part.
		8d.	Should review on a regular basis all of the privacy and data security policies, procedures, standards and guidelines on a defined timeframe (e.g., annually), and they should be dated, and updated as necessary and include a point of contact if employees have questions.	8d. Management concurs in part.
9.	Logging (Repeat finding)	We recommend that the FEC:		
		9.	Implement logging for all computer-readable data extracts from databases holding personally identifiable information (PII).	9. Management does not concur.
10.	Protections for Remote Access to PII (Repeat finding)	We recommend that the FEC:		
		10a.	Should change Policy 58-4.5 *Virtual Private Network (VPN)* and Directive 58, *Electronic Records, Software and Computer Usage,* to state that work related data must be saved to the network and not downloaded and saved on local devices. Exceptions to the policy should be clearly documented and approved by management, and, where possible, compensating controls put in place.	10a. Management concurs in part.
		10b.	Should further re-enforce the key elements in this and other security policies and also design and implement a formal communications plan to re-enforce key privacy and security principles contained in the policies and training. This communication plan should include scheduled periodic reminders to employees and contractors on key principles that can be delivered through such means as emails, log-in banners, newsletter articles, posters or other existing communication vehicles currently used to communicate with employees. The most effective messaging is typically brief and focused on a single topic. For example, an email message such as: REMINDER: Save all your work on the network and do not download to your computer.	10b. Management concurs.
		10c.	Modify the Intranet to contain a page with Privacy and data protection policies, procedures and updates. This would ensure that all FEC employees are aware of the policies with regard to PII and privacy and data protection.	10c. Management concurs.

Summary of Findings, Recommendations and Management Concurrence

Findings		Recommendations		Management Concurrence
11.	Vendor Due Diligence (Repeat finding)	We recommend that the FEC:		
		11a.	Should develop and maintain a comprehensive list of all vendors that handle PII.	11a. Management concurs.
		11b.	Should develop a policy and supporting procedures to assess and approve vendors with access to FEC PII to reasonably ensure that the vendor has adequate controls in place to protect the information before any PII is provided to the vendor.	11b. Management concurs in part.
		11c.	Should formally document the process used to review the FEC's vendors that are entrusted with PII and the results should be retained to evidence the review procedures performed. In addition, there should be documented management approval from the appropriate department head and either of the co-Chief Privacy Officers before the vendor is provided access to FEC PII. There may be more than one department head that should review and approve a specific vendor if the PII affected pertains to more than one department.	11c. Management concurs in part.
12.	System of Records Notice (SORN) Updates (Repeat finding)	We recommend the FEC Privacy Officer:		
		12a.	Develop a standardized template to allow system managers to accurately document SORs independently of the Privacy Team.	12a. Management concurs in part.
		12b.	Enhance existing guidelines and procedures to include timelines and deadlines that promote regular review and timely updates to SORs.	12b. Management concurs.
		12c.	Work with ITD management to incorporate SORs assessment processes into systems under development and IT lifecycle management processes.	12c. Management concurs.
		12d.	Work with the Physical Security Officer, the FEC Records Officer, and FEC management to incorporate SORs assessment processes into electronic and paper records management processes.	12d. Management concurs.
		12e.	Develop and implement policies and procedures that define monitoring and reporting processes to ensure SORs are updated and amendments published in accordance with Federal regulations by: • providing regular training to FEC managers and SOR system owners/managers; • Establish deadlines, based on the legal requirements of OMB A-130, for documenting the new SORs, revisions to existing SORs, and publish the updated SORN; • providing legal assessment of potential changes in SORs and quality assuring the SORs produced by system owners/managers; • including performance standards in employee performance plans that are linked to successful compliance with Federal regulations; and • requiring regular reporting of compliance with the timelines to the Commission.	12e. Management concurs in part.

Summary of Findings, Recommendations and Management Concurrence

Findings		Recommendations	Management Concurrence
13.	Training Workstations (New)	We recommend that the FEC: 13. Restrict the training workstations to only be able to access training materials.	13. Management concurs.

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 Division, 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 and Congress.

- **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 (AGC) for General Law and Advice (GLA), while the CPO and SAOP positions are shared by the AGC GLA and Chief Information Officer (CIO). Responsibilities for privacy are separated into two areas, legal and technical; AGC GLA handles legal issues, and the CIO handles technical issues. The Information Systems Security Officer (ISSO), and two attorneys from OGC GLA, along with the Co-CPOs comprise the FEC "Privacy Team."

Federal Privacy Framework

Privacy in the Federal government is rooted in passage of the *Privacy Act of 1974* and subsequent amendment. 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*, as amended, 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*, as amended, directed the Office of Management and Budget (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*
- OMB Memorandum M-08-23, *Securing the Federal Government's Domain Name System Infrastructure*
- OMB Memorandum M-09-02, *Information Technology Management Structure and Governance Framework*
- OMB Memorandum M-10-23,*Guidance for Agency Use of Third-Party Websites and Applications*
- OMB Memorandum M-11-02, *Sharing Data While Protecting Privacy*

In addition to the Privacy Act and OMB memoranda, 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,[1] 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.

[1] 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.

Section 522 (d)(3) previously required 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 required an independent third-party review at least every two years and required the Inspector General to submit a detailed report on the review to the agency head. Under section 522 of the Consolidated Appropriations Act 2008, the review may now be performed by the Office of Inspector General or by an independent third party. The review is no longer required every two years but allows the OIG the flexibility to perform it "periodically" as required. The report is to be made available to the public through the internet.

Additional laws, regulations, and criteria released by Congress, OMB, and the National Institute of Standards and Technology (NIST) related to privacy include[2]:

- *The E-Government Act of 2002*, Section 208
- *Federal Information Processi*ng 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*
- NIST Special Publication (SP) 800-60, Volume I, Revision 1: *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-60, Volume II, Revision 1: Appendices to *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*

The following Executive Order signed by President Obama dated November 4, 2010 addresses information classification within Federal government agencies:

- Executive Order #13556: *Controlling Unclassified Information*

OBJECTIVES, SCOPE AND METHODOLOGY

FEC Management prepared a corrective action plan (CAP) to address the findings and recommendations included in the Office of Inspector General's (OIG) *2007 Performance Audit of Privacy and Data Protection*. The objective of this audit follow-up was to determine whether management implemented the agreed actions for each recommendation and whether each audit finding in the 2007 report has been fully resolved. The audit follow-up was conducted in accordance with Government Auditing Standards. The FEC OIG engaged Cherry Bekaert & Holland LLP to perform this audit follow-up.

In addition to the seven findings and thirteen recommendations included in the *2007 Performance Audit of Privacy and Data Protection*, Cherry Bekaert & Holland LLP was required to determine whether controls are adequate to ensure the FEC System of Records (SOR) is updated and published in accordance with the Privacy Act of 1974 and the Office of Management and Budget (OMB) Circular A-130 Appendix I. Cherry Bekaert & Holland LLP also reviewed and is reporting on the six outstanding recommendations from the OIG's *2006 Inspection Report on Personally Identifiable Information.*

Cherry Bekaert & Holland LLP conducted this review through the use of the following: detailed interviews; review and evaluation of relevant documents such as FEC privacy and security policies,

[2] FEC legal analysis concluded that the FEC is exempt from these requirements.

procedures, directives, training materials, mobile device asset listings, system settings; and auditor observation. We conducted interviews to obtain an understanding of the corrective actions implemented since the *2007 Performance Audit of Privacy and Data Protection* and to understand management's approach and strategy for identifying, assessing risk, protecting PII and complying with applicable legal requirements. We interviewed key personnel from senior management and staff from various offices including the members of the FEC Privacy Team.

Based on results of our review, Cherry Bakaert & Holland LLP developed findings and recommendations for management, which are in the following section.

DETAILED FINDINGS AND RECOMMENDATIONS

Management's responses to the detailed findings were provided in a memorandum dated March 16, 2011 from Mr. Alec Palmer, Acting Staff Director, Chief Information Officer and Co-Chief Privacy Officer and Mr. Lawrence L. Calvert, Associate General Counsel for General Law and Advice and Co-Chief Privacy Officer to Ms. Lynne McFarland, Inspector General and Mr. Jonathan Hatfield, Deputy Inspector General. Management's responses are included verbatim below. Attachment 1 contains the cover memo to management's responses.

Finding 1: Privacy Roles and Accountability

The Chief Privacy Officer (CPO), Privacy Officer (PO), and Senior Agency Official for Privacy (SAOP) roles and responsibilities are documented in privacy policies and directives. The CPO and SAOP positions are currently being shared by the Associate General Counsel (AGC) for General Law and Advice (GLA) and the Chief Information Officer (CIO). Review of the documented roles and responsibilities for the CPO and SAOP showed they have not been specifically assigned to either the AGC for GLA or the CIO. In addition, while CPO roles and responsibilities do include responsibility for ensuring compliance with laws and regulations, the policies and directives do not identify how compliance will be monitored or identify which CPO will perform specific monitoring activities. To the best of our knowledge, we are not aware of any other Federal government agency or private sector organization that has co-CPOs.

Based on interviews with the co-CPOs, we determined that it was unclear which individual is specifically responsible for ensuring compliance with privacy policies and procedures at the agency level.

Consolidated Appropriations Act, 2005, 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 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. *training and educating employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies; and*
> 8. *ensuring compliance with the Departments established privacy and data protection policies.*

Section 522 (b) states that:

> *"Establishing Privacy and Data Protection Procedures and Policies. 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."*
>
> The FEC has not assigned responsibility for compliance with privacy regulations to a single individual. Instead the agency has chosen to share the responsibilities between two individuals but has not adequately defined the respective roles and responsibilities of either in job descriptions.
>
> Consolidated Appropriations Act, 2005, Section 522 (a) describes the responsibilities of a "Chief Privacy Officer" and does not prohibit co-Chief Privacy Officers. However, without clearly assigning accountability for privacy leadership to a specific individual, it has limited the progress of the privacy program made by the FEC and prohibits the FEC from maturing the privacy program beyond reacting to audit findings and legislative requirements. In addition, the Commission's ability to hold specific individuals accountable for failures to develop, implement, and monitor a privacy framework is reduced. Without a strong privacy framework, the risk of sensitive or personally identifiable information being obtained and used for unauthorized purposes increases.

Recommendations

We recommend that the FEC:

1a. Assign privacy roles and responsibilities to one individual CPO with high level sponsorship in the Commission. If the Commission decides to continue with two CPOs and SAOPs, roles and responsibilities under these titles should be clearly delineated between individuals sharing the positions.

1b. Identify, document in position descriptions and performance plans, and assign specific roles and responsibilities for the monitoring and reporting of compliance with Federal and Commission privacy requirements.

Management Response to 1a:

Management does not concur: The report provides that "[b]ased on interviews with the co-CPOs, we determined that it was unclear who was specifically responsible for ensuring compliance with privacy policies and procedures at the agency level." To clarify we believe that the roles and responsibilities of the Co-CPOs are clearly defined in Directive 65, and that there should not be one individual CPO. Directive 65, "Designation of Chief Privacy Officer and Senior Agency Official for Privacy" explicitly describes the duties of the Co-CPOs. The Directive indicates that the "Chief Information Officer [CIO] and the FEC Associate General Counsel for General Law and Advice [AGC] shall serve jointly as the Chief Privacy Officer as well as the Senior Agency Official for Privacy." It also provides that while the CIO and AGC will share the CPO duties, the CIO will address "technological safeguards and processes" and the AGC will address "issues of statutory and regulatory interpretation." Thus the Directive is clear as to the roles and responsibilities of the Co-CPOs.

Additionally, we disagree that an individual CPO is necessary. One of the benefits of having two CPOs (as well as having members of the team from OGC and OCIO) is that it affords us the opportunity to share unique perspectives and judgments that are possible only because of our differing expertise and backgrounds. Using a multidisciplinary team to address privacy issues enables us to consider technology and legal issues simultaneously. This would not be possible if there were only one CPO.

We acknowledge that there would be some benefits to having a single CPO. However, we believe most of these benefits would be realized only if the position of CPO was a full-time position, rather than a collateral duty. Such an official would likely be able to move projects forward more efficiently, and accountability would be simpler. However we believe that at this time, in the Commission's circumstance, those benefits are outweighed by the benefits of having a joint working group (i.e. less stove piping and more synergy; and the advantage of having two agency officials with the clout to receive buy-in for privacy projects from the Commission and senior managers). While we agree that privacy is of the utmost importance, and it is unfortunate that we have been unable to move forward with some privacy projects at a faster pace because of conflicting priorities, we still find that the progress that has been made is significant in comparison to what has been done in the past (e.g., it took approximately 13 years for the 2008 SORNs to be published, whereas there will only be a 3-year gap when the 2011 SORNs are published). Moreover, given that the greatest benefits of a single CPO would accrue from having a full-time CPO, we have to acknowledge that the ability to create such a position is highly unlikely in the budgetary environment the Commission is likely to face over the next several years. For these reasons, we respectfully decline to adopt a single CPO model.

Auditor Response:

We acknowledge that progress has been made over the past couple of years and that the Privacy Team members have other significant job responsibilities. However, significant work remains. We continue to believe the Commission should appoint a single individual to the position of Chief Privacy Officer. We acknowledge that the current budgetary environment is very challenging and adding a new CPO position seems in conflict to budgetary constraints. However, it appears that management acknowledges the benefits of a full-time CPO. We believe that a discussion with the Commissioners by management regarding a full-time CPO position is warranted to create the position, or serious consideration is made to detail an existing FEC staff person with the knowledge and/or aptitude in privacy to assume primary responsibility for FEC privacy.

Management Response to 1b:

Management does not concur: The roles and responsibilities outlined in Directive 65, and the FEC Privacy Policies and Procedures provide sufficient accountability for the Co-CPOs with respect to agency-wide privacy compliance. If the goal is to hold someone accountable for privacy these directives accomplish that goal. The Co-CPOs in turn hold the rest of the Privacy team responsible and accountable for privacy duties.

Auditor Response:

Accountability should be strengthened through more detailed metrics that are included in the performance plans of Privacy Team members.

Finding 2: Privacy Impact Assessments Have Not Been Conducted

The original findings from the 2007 report regarding the lack of privacy impact assessments (PIAs)[3] and selective compliance with OMB memoranda without documented analysis and justification have not been addressed. While there are various security review procedures periodically executed by Information Technology Division (ITD) staff or contractors, the procedures compliment but do not replace the need for PIAs on new and existing systems. Also, rather than implementing information security controls described in OMB memorandums as a matter of best practice, the agency continues to rely on legal justifications and exemptions to support not adopting OMB standards. Noting the FEC's exemption from Financial Information Security Management Act (FISMA) and NIST under the E-Government Act, the longstanding practice of legal assessment, rather than risk assessment, lacks adequate due diligence because the potential impact of the agency's failure to implement specific information system security controls is not fully considered. For instance, OMB memoranda, M-08-23, released August 22, 2008, required agencies to deploy "Domain Name System Security (DNSSEC) to all Federal information systems by December 2009. DNSSEC provides cryptographic protections for DNS communication exchanges, thereby removing threats of DNS-based attacks and improving overall integrity and authenticity of information processed over the internet." It is noted that OMB memoranda are largely based on FISMA and NIST requirements, The FEC Office of General Counsel (OGC) provided a legal assessment of OMB M-08-23 on March 10, 2010 and opined that:

> *"The memo is derived from security recommendations made in NIST Special Publication 800-81; the security controls are intended to remove threats of attacks to the agency's domain name system (DNS). According to the memo, the controls are to be initiated on "FISMA high and moderate impact information systems" and will be tracked on future FISMA reports. The FEC is exempt from FISMA, since the Act only applies to agencies subject to the Paperwork Reduction Act (44 USC 3502), from which the FEC is explicitly exempt. The FEC is not required to follow NIST guidance under 15 U.S.C. § 278g-3(a). Moreover, because NIST guidance stems from FISMA, it follows that we are exempt from its recommendations. For these reasons, the FEC is not required to follow OMB M-08-23, although it may decide to do so only as a best practice."*

We note that the legal opinion stated the agency "may decide to do so only as best practice ," however the agency has not yet performed or documented a risk assessment and cost benefit analysis on implementing or failing to implement the security standard. The legal assessment was performed more than 18 months after release by OMB and after the date for submission of draft agency plans by September 5, 2008 and the effective date of December 2009. The assessment did not address mandatory language in the memorandum that expanded the scope of existing policy and applied it to "all United States Government "USG" information systems."

A documented risk assessment would include addressing questions such as:

- Is the subject matter in the OMB memorandum applicable to FEC operations?
- What are the risks or "what could go wrong" scenarios if the guidance in the OMB memorandum is not implemented?
- Considering current controls in place, what is the likelihood that the risks identified will materialize?

[3] *Privacy Impact Assessment (PIA)* - is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. Source: OMB 03-22.

- What is the cost to mitigate the risk?
- What is the level of complexity to mitigate the risk?
- Are the means to mitigate the risk primarily dependent on technology, process or personnel changes?
- What are the benefits to mitigate the risk?
- What is the estimated timeframe to mitigate the risk?
- What are the human resource requirements to mitigate the risk?
- If the risks identified will be accepted, the rationale, and management approval for that decision should be documented.

As interpreted and applied by the FEC, exception under the E-Government Act overrides the fact that the FEC does have high or moderate impact information systems and risk associated with potential unauthorized use, compromise, and loss of the fec.gov domain space. There is no documented acceptance of risk and no accountability if the agency's failure to apply the security standard results in the possibility of the FEC website being defaced with false or offensive information (e.g., pornography), disabled so that the website is not accessible to the public or is infected with malicious software that could harm a website visitor's computer.

Section 522, Section (a)(5) of the Consolidated Appropriations Act of 2005 states 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.*

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.*

The FEC has conducted a legal review and determined the agency is exempt from the requirement to complete PIAs. In addition, some Privacy Team members believe the PIA process is too onerous and there is not sufficient staff to execute PIAs. Neither of the co-Chief Privacy Officers has been assigned responsibility or accountability for performing alternate risk assessment processes.

A comprehensive approach to identifying, assessing, mitigating, monitoring and reporting risks, which would include a PIA or equivalent process, has not been mandated and thus has not been implemented. Without such a framework, management may be taking on more risk than they would otherwise want to accept, or the current process may be inefficient in the application of necessary controls. In addition, without a privacy impact assessment, the FEC cannot accurately assess where privacy related risks exist. Sensitive PII may be compromised by an unauthorized user if they exploit these unprotected risks.

Recommendations

We recommend that the FEC:

2a. Conduct privacy impact assessments in accordance with Section 522, or create an alternative process for ensuring that privacy risks associated with PII are documented, assessed and remediated as necessary.

2b. Comply with OMB memoranda, or in the event of statutory exemption and a decision not to voluntary comply, 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.

2c. Identify and implement a governance framework (e.g., NIST, the AICPA's Generally Accepted Privacy Principles (GAPP)), to ensure that controls within the FEC to protect PII are appropriately identified, documented, and implemented.

Management Response to 2a:

Management concurs in part: At the outset, it must be noted that the agency has flexibility as to whether it should conduct privacy impact assessments (PIAs) as this is a requirement under the E-Government Act, from which the agency is exempt. Thus, as noted by the auditors, the agency is not mandated by law to conduct PIAs or any similar process that would be required by the E-Government Act. However, we may consider implementing a modified, or alternative, template document that would provide the benefits of a PIA without the strain on the Commission's staffing resources.

Auditor Response:

While PIAs are not a legal requirement for the FEC, PIAs, or an equivalent, are an invaluable tool to reasonably ensure that privacy risks are identified and addressed. We look forward to reviewing the details in the corrective action plan of when a modified or alternative template will be implemented or further explanation of why it will not be implemented.

Management Response to 2b:

Management concurs in part: The auditors noted that "rather than implementing information security controls described in OMB memorandums as a matter of best practice, the agency continues to rely on legal justifications and exemptions to support not adopting OMB standards." This is not entirely true. While legal exemptions may be one factor in determining whether to adopt a OMB standard, they are not the only factor. The agency relies on various factors to determine whether a standard should be implemented despite the exemption, most notably cost and resources.

Nevertheless, we agree that in certain cases it may be appropriate for the agency to conduct an informal risk assessment and cost-benefit analysis of an OMB requirement if there is a statutory exemption. These limited circumstances are: 1) where the requirements are feasible to implement from a budgetary, resource, and agency-mission perspective; and 2) where the costs or benefits of implementing those requirements are unclear or require additional investigation. While we do not agree that a formal documented risk assessment is necessary to explain why management decided to opt out of an OMB requirement that the agency is exempt from, we can agree to conduct a documented informal analysis that explains the costs of implementing the guidance, and how the costs outweigh the benefits of compliance.

Auditor Response:

While we acknowledge that an informal documented risk assessment would be an improvement over the current state, the agency's position why OMB guidance was or was not adopted should be a formal process with the conclusions approved by management.

Management Response to 2c:

Management concurs in part: We appreciate the auditors calling our attention to the GAPP framework. On first review, the principles of GAPP, although developed for private entities, appear to be closely aligned with the requirements of the Privacy Act (which applies to the FEC) and with the agency's privacy policies. While we cannot commit to adopting GAPP in its entirety at this time, we can commit to a careful review of GAPP.

Auditor Response:

We agree that a careful review of GAPP should be performed and a documented summary of the results be prepared and provided to management. We look forward to reviewing the details and milestones for the review in the corrective action plan.

Finding 3: Monitoring and Review of Regulatory Requirements

There is no defined process or assigned accountability by which the Commission identifies new OMB memoranda or Executive Orders and ensures that they are reviewed for legal applicability. In addition, if the memoranda or Executive Orders do not legally apply, a risk assessment to evaluate if it is prudent to adopt the directive is not performed. During this follow-up review, we identified several OMB memoranda related to information security or privacy issues that were issued since December 2007, when the prior audit report was released, including:

1. M-08-23, August 22, 2008, "Securing the Federal Government's Domain Name System Infrastructure (Submission of Draft Agency Plans Due by September 5, 2008)."

   FEC legal opinion rendered on March 10, 2010.

2. M-09-02, October 21, 2008, "Information Technology Management Structure and Governance Framework."

   FEC legal opinion rendered on June 16, 2009.

3. M-10-23, June 25, 2010, "Guidance for Agency Use of Third-Party Websites and Applications."

   FEC legal review in progress.

4. M-11-02, November 2, 2010, "Sharing Data While Protecting Privacy."

   FEC legal opinion rendered on December 6, 2010.

As is evident from the above, legal reviews are not always conducted on a timely basis. The reason is that unless a division or department requests a legal review of new OMB memoranda or Executive Order, the Office of General Counsel does not perform a review. In some cases, the delayed timing for performing a legal review is due to legal resources having higher priorities. As a result of untimely review of the OMB memoranda or Executive Orders, any applicable legal requirement or high risk item in the documents may

not be addressed on a timely basis if the affected division or department does take necessary action before requesting or receiving a legal opinion.

Recommendations

We recommend that the FEC:

3a. Develop a process and assign accountability for the proactive and timely identification of new OMB memoranda and Executive Orders to ensure that they are reviewed and referred for legal opinion on a timely basis.

3b. Complete legal reviews of OMB memoranda on a more timely basis and consistently communicate the results to the affected stakeholders, with a copy to the co-Chief Privacy Officers.

Management's General Response to Finding 3:

It is true that the Office of General Counsel General Law & Advice Division, Administrative Law Team provides advice most often upon request, as we are not always made aware of OMB memoranda when they are issued. However, there is one notable exception to this rule. Every year in connection with the Financial Statements Audit, the Administrative Law Team conducts a review of all information technology guidance, laws, and Government-wide rules and regulations passed within the last year. This documented legal review often includes a review of privacy-related OMB memoranda, since they often relate to information technology. As a result, yearly reviews are conducted on many privacy-related guidance.

Additionally, it cannot be assumed that the timing of a legal review will delay the agency's compliance. A division/office may determine to move forward with the enforcement of OMB guidance without seeking legal advice. Finally, as indicated in management's response to the 2007 audit, management does not solely base its decision to follow, or not follow, OMB guidance on legal exemptions. Even if the agency is exempt from following a certain OMB requirement, management may decide to implement it as a best practice. The decision to implement the requirement is often based on budgetary or resources concerns, not legality.

Auditor Response:

We acknowledge the annual review process. Our observation and concern is that the FEC as an agency does not have a formal process to identify, review and address all applicable legal requirements on a continuous basis regardless of whether the OGC is asked for an analysis. While the agency could take actions to comply with any particular legal requirement without legal review, we believe a process to identify and review all applicable requirements will result in greater assurance that the agency is aware of and ensures actions on those requirements to achieve compliance.

Management Response to 3a:

Management concurs: Management agrees to work with the Office of the Chief Information Officer (OCIO) and other stakeholders to develop a process for monitoring and/or processing privacy-related OMB memoranda and Executive Orders for legal review, when necessary.

Auditor Response:

The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation.

Management Response to 3b:

Management concurs in part: We agree that legal review of privacy-related OMB memoranda should take place in a timelier manner, and will look for ways to streamline this process. We note that, with respect to OMB M-08-23, we did not receive a legal review request from OCIO until February 23, 2010, and thus the legal review was promptly rendered on March 10, 2010. For OMB M-09-02, legal review was not sought by any of our clients. As a result, Administrative Law was not aware of the memorandum until it conducted its applicable laws legal review in connection with the Financial Statements Audit. Additionally, while an initial legal assessment was conducted for OMB M-10-23, on July 8, 2010 (one day after it was requested), it was determined to be a lower priority to the agency as the Commission is not extensively involved in third party social media sites such as YouTube or Facebook. The Commission has recently established a Twitter account. We will reevaluate the memo to determine its applicability and requirements with respect to the Commission's Twitter account.

It is important to also note that some OMB guidance that is about IT matters may have privacy implications, but may not on its face indicate that it is about privacy. Accordingly, in some instances guidance may be provided relatively soon after a client requests it but some time after it is promulgated.

Auditor Response:

The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation. We look forward to reviewing the detailed plan on how to streamline the review process in the corrective action plan.

Finding 4: A Current PII Inventory is Not Maintained

An inventory of FEC systems that contain personally identifiable information (PII) was conducted by Solutions Technology Systems, Inc. (STSI) and documented in a report dated May 20, 2009. The report contained many recommendations to enhance the protection of PII in both paper and electronic form. A process has not been developed, documented and implemented to periodically update the FEC's inventory of PII. Since the report was released more than 18 months ago, the FEC Privacy Team recently prepared a draft report evaluating the recommendations to determine which will be implemented.

The FEC Privacy Team created a document titled "FEC Plan to Review and Reduce Holdings of Personally Identifiable Information and Eliminate Unnecessary Use of Social Security Numbers In Response to OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information." This document contains a three phase approach to addressing the OMB requirements. The first phase, to identify uses of social security numbers in the agency, was completed by STSI as noted above. Phase 2 of the plan, to explore alternatives to the collection and use of social security numbers, was to be completed by May 2008. Phase 3, implement actions to reduce the use of social security numbers, where feasible, was scheduled to be completed in November 2008. To date, neither phase 2 nor phase 3 have been completed and the plan has not been updated to reflect revised implementation dates. In the Annual Privacy Management Report of the Federal Election Commission submitted to OMB on November 15, 2010, the Co-Senior Agency Officials for Privacy reported:

> *"The Co-Chief Privacy Officers intend to move forward with Phases 2 and 3 of the PII Plan, which includes reviewing the proposed recommendations from the Privacy Team, working with*

agency offices to discuss the alternatives to SSN use discussed in the Phase 1 Report, and implementing those alternatives if approved. The Privacy Team will also monitor the impact of those alternatives on work processes to determine their effectiveness."

The STSI report identified questionable or unnecessary use of social security numbers by form or document type, and division. The Privacy Team has not provided the information to the divisions with a request to explain, support or cease questionable use of social security numbers.

Consolidated Appropriations Act of 2005, 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 M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated May 22, 2007, section B.1, *Privacy Requirements -Review and Reduce the Volume of Personally Identifiable Information*, states:

"Review Current Holdings. 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 M-05-08, *Designation of Senior Agency Officials for Privacy*, dated February 11, 2005, 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."

FEC *Privacy Policies and Procedures*, 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."

There is no requirement to periodically update the inventory of PII that is part of the FEC's security and privacy governance approach. Completion of the review of the STSI recommendations and execution of the "FEC's Plan to Review and Reduce Holdings of Personally Identifiable Information and Eliminate

Unnecessary Use of Social Security Numbers In Response to OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information" was not completed due to other priorities, and the fact that Privacy Team members spend only a small portion of their time on privacy matters.

The lack of an updated current PII inventory prevents the Commission from effectively evaluating and ensuring the appropriate protection and disposal of PII. Delays in evaluating and implementing recommendations in the STSI report result in continued security risks to PII held by the Commission. The delay in implementing the plan to reduce the use of SSNs, where feasible, results in unnecessary risk of PII disclosure and increased effort to identify, protect and securely dispose of the information.

Recommendations

We recommend that the FEC:

4a. Update and maintain the inventory of all systems that contain PII for all the divisions. A potential approach is to use the templates created by STSI and have each division update their current listing and implement business processes to continually update the inventory based on new or revised handling and storage of PII. A full review could be conducted by the divisions at least annually and would help support the biennial Privacy Act Systems of Records update process.

4b. Finalize the evaluation of the STSI recommendations and develop, document and implement a corrective action plan as necessary. Progress against the corrective action plan should be formally and periodically reported to management.

4c. Provide the Privacy Team's SSN Reduction Plan Phase 1 report to the applicable division heads, and work with those offices to prepare action plans to address the findings in the report.

4d. Complete Phase 2 and Phase 3 of the "FEC's Plan to Review and Reduce Holdings of Personally Identifiable Information and Eliminate Unnecessary Use of Social Security Numbers In Response to OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information" as soon as practical. This can be accomplished by providing the STSI results to the divisions and requesting a response on the ability to reduce or eliminate the questionable uses of social security numbers already identified by the contractor.

Management Response to 4a:

Management concurs in part: While management concurs in part with this recommendation, we wish to correct a statement made in the report. The auditors found that "[t]here is no requirement to periodically update the inventory of PII that is part of the FEC's security and privacy governance approach." This is not true. The "FEC Plan to Review and Reduce Holdings of Personally Identifiable Information and Eliminate Unnecessary Use of Social Security Numbers In Response to OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information" provides for a biennial review of the agency's PII holdings as well as its SSN holdings and SORNs. Additionally, as part of the statement of work for the 2009 PII review, STSI created a proposed procedure for updating the PII inventory. Thus the agency has incorporated inventory updates into its overall privacy program. Accordingly, we agree that the PII inventory should be updated but only on a biennial basis (i.e. the next update would be conducted this year).

With respect to the recommendation that we devolve this responsibility to the system manager level, we think this is a good idea in the abstract, but in order to implement it we see potential issues with buy-in and adequate training. A remedy to these issues would of course be essential. Consequently, while we cannot commit at this time to such devolution, we can commit to strongly considering it.

Auditor Response:

We acknowledge that the "FEC Plan to Review and Reduce Holdings of Personally Identifiable Information and Eliminate Unnecessary Use of Social Security Numbers In Response to OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information" does state that a "review" of PII will be conducted every two years. If the review includes updating the PII inventory we agree that a plan is in place. We look forward to reviewing the results of the consideration of devolving the inventory responsibilities and the planned timeline for such consideration in the corrective action plan.

Management Response to 4b:

Management concurs: We agree with this recommendation and are already in the process of finalizing the Privacy Team's analysis of the PII Review Assessment Report. Upon approval of the Privacy Team's recommendations by the Chief Privacy Officers, the Privacy Team will develop a corrective action plan aimed at addressing the deficiencies found in the review.

Auditor Response:

The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation.

Management Response to 4c:

Management concurs: We agree with this recommendation and will work with affected offices to prepare action plans to address the SSN Phase 1 Report recommendations once they have been approved by the Chief Privacy Officers.

Auditor Response:

The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation.

Management Response to 4d:

Management concurs in part: We agree to complete Phases 2 and 3 of the plan as soon as practical, but believe this can best be accomplished by disclosing the findings of the Privacy Team's SSN Reduction Plan Phase 1 report to the applicable division heads, and working with those offices to prepare action plans to address the findings in the report as recommended in Finding 4c.

Auditor Response:

We agree that the recommendation in 4c should be completed first and encourage Phase 1-3 of the plan to be completed as quickly as practical as they are significantly behind schedule.

Finding 5: Current Risk Assessments of Systems Containing PII Are Not Performed

Since the 2007 Privacy and Data Protection Audit report was released, the Commission contracted for secure destruction containers and placed them throughout the building. This allows employees to securely dispose of paper and electronic medium that contains PII or other sensitive information. In addition, vulnerability and penetration tests of certain computer applications were conducted in 2009 and 2010. This annual process provides a point in time view into any application and network vulnerabilities, however, these vulnerabilities can change quickly over time. Further, contractors performed a comprehensive risk assessment in 2008 for the Administrative Fines, Case Management, ComprizonBuy/ComprizonSuite, Disclosure System, Presidential Matching Funds, PeopleSoft, and the FEC Local Area Network (LAN) using the NIST SP 800-30, *Risk Management Guide for Information Technology Systems*[4] framework. The risk assessments did include an evaluation of remote access to the FEC LAN, which management informed us is the only approved way to remotely access the FEC network. However, the risk assessments did not assess PII protection needs of all systems containing PII, and, since that time, no additional risk assessments have been conducted. The existing risk assessments have not been reviewed or updated for changes in agency systems.

OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*, 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".*

FEC Risk Management Policy, 58-2.1 states:

> *"c. A risk assessment framework should be established to ensure that risks to FEC electronic information and computing resources are regularly assessed. This framework should be designed to provide a basis for determining how technical, administrative, physical, and operational risks can be managed to an acceptable level;*
>
> *d. The risk assessment framework should provide for risk assessments on a recurring basis, in accordance with applicable federal guidance; risk assessment information should be updated with results of audits, inspections and identified incidents;"*

The FEC does not have a requirement to perform periodic risk assessments related to PII. The lack of periodic risk assessments which specifically assess PII protection needs prevents the FEC from knowing if PII is being appropriately safeguarded.

[4] This guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. In addition, this guide provides information on the selection of cost-effective security controls. These controls can be used to mitigate risk for the better protection of mission-critical information and the IT systems that process, store, and transmit this information.

Recommendations

We recommend that the FEC:

5a. Conduct a risk assessment annually for all existing and new applications that collect, process, transmit or store PII. If PIAs were performed, a risk assessment component could be built into that process to accomplish both the PIA and risk assessment recommendations.

5b. Prepare a documented corrective action plan for any deficiency noted for each risk assessment performed and report progress periodically until all corrective actions are implemented. The corrective action plan should be approved by management.

5c. Include all systems containing PII that are being retired in the risk assessments and develop action plans to ensure the proper transfer of PII to a new system or the secure destruction of the PII in the retired system.

Management Response to 5a:

Management concurs in part: We appreciate the auditors' clarification on February 3, 2011 that this recommendation relates to electronic systems containing PII, and any paper or electronic documents that can be generated from those systems. Based upon this clarification, management does not believe that an annual comprehensive formal risk assessment of such systems is necessary. However, we can agree to conduct an informal risk assessment in connection with the biennial PII Review similar to that conducted by STSI, since that review focuses specifically on PII in both electronic and paper systems.

Auditor Response:

While an informal documented risk assessment would be an improvement from the current state, we view the process conducted by STSI as a formal review and encourage the FEC Privacy Team to follow a similar process. We look forward to reviewing the details regarding the timing and nature of the planned risk assessment in the corrective action plan.

Management Response to 5b:

Management concurs in part: In connection with the biennial PII Review, management agrees to prepare an informal, but documented, assessment of its findings from the review, as well as recommended action items to address any deficiencies found during the review. Management does not agree to prepare and conduct such an assessment outside of the biennial PII Review process.

Auditor Response:

A documented corrective action plan should be prepared for each deficiency noted in any risk assessment regardless of whether the risk assessment is formal or informal or when the risk assessment is performed.

Management Response to 5c:

Management concurs in part: Management concurs with the need to ensure PII in retired systems is securely transferred, and to that end we agree to develop documented procedures addressing this issue. However, we disagree that this process requires a risk assessment, and note that we already have policies and standards in place that address the destruction and security of PII in retired systems (e.g., Media Disposal Standard and Policy 58-4.2 Media Management Security Policy).

Auditor Response:

We agree that documented procedures that are followed to ensure the secure transfer or destruction of PII in retired systems is sufficient and a risk assessment would not be necessary. We look forward to reviewing the details about the development of these procedures in the corrective action plan.

Finding 6: Mobile Computing Policy, Device Encryption and Controls

FEC Policy

FEC *Mobile Computing Security Policy*, Policy Number 58-4.3, states:

> *"All laptops that access the FEC Local Area Network (LAN) will be required to employ whole hard drive encryption."*

OMB M-06-16, Protection of Sensitive Agency Information, dated June 23, 2006 states:

> *"encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing."*

The policy and OMB requirement is not followed for all FEC laptops. Contrary to OMB and the FEC's own guidance, the FEC's current practice is to only encrypt laptops that leave the building. Further, the primary control to prevent any laptop device from leaving the building is issuance of a FEC property pass authorizing removal. This control is insufficient and relies on physical enforcement by the FEC security guards, whereby the guards may stop employees/contractors leaving the building, or employees/contractors voluntarily indicate to the guards that they have a computer and a current property pass as they leave the building. It is possible, however, that laptops without property passes can be removed from the building through the main entrance or from the exit to the parking garage and not be noticed. For example, a FEC contractor routinely brings a non-FEC laptop with a property pass into the building and leaves the building through the main entrance. The contractor has never been asked by the security guards whether he has a mobile device in his bag or asked to display the property pass. Given the FEC's building and security configurations, laptops, which may or may not be encrypted, could be stolen and easily removed without detection. Laptops are a prime target for theft because they can be easily sold for cash to pawn shops or other individuals over the internet. A stolen or lost unencrypted FEC laptop containing PII or sensitive information could create a significant liability for the agency. For this reason, the data on all FEC laptops and mobile devices should be encrypted as stated in the FEC policy.

Controls to Prevent Access by Non-Encrypted Devices

The *2007 Performance Audit of Privacy and Data Protection* audit report recommended that the FEC implement technical and/or policy controls to prevent local or remote access to Commission resources by non-encrypted devices. In response to the recommendation, management stated it planned to implement a network control device in fiscal year 2008. The device would "deny or restrict access to the FEC's network for devices not in compliance with the FEC's policies and minimum settings."

FEC *Mobile Computing Security Policy*, Policy Number 58-4.3, states:

> *"All staff/contractors who are issued a FEC laptop are authorized for remote access, i.e. (VPN and Dial-up)".*

FEC System Integrity Policy, 58-4.6, states:

> *"Information System Monitoring Tools and Techniques*
>
> *(a) System Owners shall employ automated tools to support near-real-time analysis of events, when feasible.*
>
> *(b) System Owners shall ensure information systems monitor inbound and outbound communications for unusual or unauthorized activities or conditions (e.g., the presence of malicious code, the unauthorized export of data, or signaling to an external information system)".*

FEC Privacy Protection Policies and Procedures, undated, states:

> *"I. Co-Chief Privacy Officers/Co-Senior Agency Officials for Privacy*
>
> *The Co-Chief Privacy Officers and Co-Senior Agency Officials for Privacy are responsible for:*
>
> *Assuring that the Commission's use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of information in an identifiable form;"*

OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*, 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.*

In the most recent corrective action plan provided for the Privacy follow-up audit, the Privacy Team stated the network control device "has not been implemented, however we have implemented policies and procedures to prevent access from non-encrypted laptops either locally or remotely." According to FEC management, a network control device was not implemented due to resource constraints, feasibility concerns, and it was deemed not to be cost-effective.

As noted above, only devices that are expected to leave the building are encrypted and the FEC does not maintain complete records, by device, listing which mobile computers are or are not encrypted. While there is limited information on device encryption, however, the information is not used to monitor or enforce the policy that all laptops that access the LAN "employ whole hard drive encryption." Detailed testing showed unencrypted devices access agency networks both locally and remotely. Further, the agency is not able to adequately track mobile devices that can access FEC networks. Refer to the sections on *Mobile Device Inventory Listing* and *Policy Exceptions* below. As such, we find that neither technical nor compensating controls have been implemented to prevent local or remote access to FEC networks by unencrypted devices.

Mobile Device Inventory

As part of our testing compliance with the FEC *Mobile Computing Security Policy*, 58-4, we requested a listing of all mobile devices issued to staff and contractors. The initial listing provided appeared to be incomplete based on our review for recent purchases of Apple computers, iPads, and laptop computers

issued to staff in the Office of the Inspector General. Therefore, a second listing was provided on January 11, 2011 with an assurance by management that the listing was complete and accurate, except for the iPads that had been recently purchased and issued, but not yet added to the inventory listing. Review of that updated listing again indicated it also might not be complete or accurate. We compared the second mobile device listing to the FEC staffing report at December 18, 2010 and identified 79 employees with no assigned mobile computers (i.e. Apple MacBook, Acer netbook, Dell laptop, or Apple iPad). The listing seemed inconsistent with roles, responsibilities, or grade level of many of the 79 individuals and the expectation that these individuals would have a mobile device based on their job function. Therefore, we judgmentally surveyed 28 of the 79 listed employees and requested they respond to whether they currently have mobile computing devices issued by the FEC, and if so, to provide the barcode if it was available. Twenty-four (24) responded and most indicated they had been issued mobile computing devices. Seven (7) of those responding had more than one device. One person had four laptop computers, none of which were included on the FEC's inventory listing. One respondent had two MacBooks, neither of which contained a barcode. Only two (2) of the 28 employees surveyed responded that they did not have a mobile computing device. In total, thirty-three (33) mobile computers were identified through our survey which were not included on the second asset listing provided. Our review of the details provided by some employees surveyed showed data collected via barcode scanner during the FEC's annual wall-to-wall inventory in July 2010 was not uploaded to the inventory listing; this appears to be at least one reason why the inventory listing is inaccurate.

We also noted several former employees and former contractors were included in the asset listings provided for the follow-up audit. The second asset listing had four (4) former contractors and five (5) former employees listed as still having mobile devices. One of the former employees listed left the FEC in August 2008, while another left in August 2009. We identified several other employees and contractors who left the agency between September and December 2010, and the asset listing was not updated to reflect the current location of the mobile devices assigned to the former employees/contractors.

Based on initial audit results reported to management, a third asset listing was provided, along with a system report of FEC users and devices encrypted. The 'listing of encrypted devices' had 209 records which could be linked, by barcode, to a specific mobile computing device. However, the 'asset listing' had 496[5] mobile computing devices which, according to the FEC policy, should be encrypted if issued to staff or contractors. Comparing the listing of encrypted devices to the asset listing provided the following results:

- Of the 209 listed encrypted devices, 186 encrypted devices were matched to mobile devices included on the asset listing, including one desktop system. Review of the desktop system showed encryption was not installed. This indicates at least one encryption record is not accurate.

- Of the 209 listed encrypted devices, there were 23 devices which could not be linked to mobile devices included on the asset listing. These items were compared to asset disposal records from 2010, but it does not appear the items were disposed of by the agency. This indicates the third and most recent asset listing provided is not complete or accurate.

- Of the 496 mobile computers included in the third asset listing, there were 314 mobile devices that could not be linked, by barcode number, to encryption records. Based on a statement by ITD staff that the FEC has approximately 500 encryption licenses, it is likely the majority of the devices are encrypted, however there is no way to verify the encryption status the majority of FEC mobile computing devices without physically reviewing the device.

[5] The count is exclusive of Apple iPads mobile computing devices that are not encrypted and are undergoing test and evaluation by the FEC ITD division.

In order to further assess whether the FEC has a complete and accurate list of all encrypted mobile devices, we reviewed asset purchases and identified purchases of Dell D630 model laptops issued to FEC employees and contractors. One hundred and fifty (150) D630 computers were purchased in November 2007 and another one hundred (100) were purchased in August 2008, for a total of two hundred-fifty (250) computers. The first asset listing provided during the audit had 213 D630 laptops, the second listing 221, and the third asset listing provided showed 232 D630 laptops were issued to FEC employees and contractors. Our review of the agency's computer asset storage areas and ITD staff offices located another six (6) D630 laptops, and another two (2) were identified by reviewing the 2010 inventory scan listing for contractors. In total, ten (10) D630 computers were not located and could not be accounted for. Because the annual wall-to-wall inventory performed does not begin with a reconciliation of asset purchases to the fixed asset listing, the FEC may be missing any number of computer assets which are undetected.

The inability to produce a complete and accurate listing of all mobile devices appears to be due to a defect in the design or use of the fixed asset accounting system for mobile devices. Because of the lack of an accurate, updated inventory, the FEC cannot state with reasonable certainty that all mobile devices purchased and in use are encrypted, in accordance with the stated policy, and there may not be an adequate record of the current location or to whom the mobile devices are issued. Further, because the asset listing is not reconciled to assets purchased, or adequately maintained, the FEC must rely on employees reporting theft or loss to adequately control computer equipment. Lost or stolen devices could be used to gain unauthorized access to FEC systems that contain PII and the FEC may be unable to determine whether a breach of PII has occurred.

Exceptions to FEC Encryption Policy

The FEC grants exceptions to the policy requiring all laptops be encrypted, and all mobile devices be encrypted and/or password protected.

Apple MacBooks

During the 2007 Privacy and Data Protection Audit, the FEC had fourteen (14) Apple MacBooks and three (3) other laptop computers that were not encrypted. During this follow-up, because the initial asset listing provided did not include Apple computers, we specifically requested information on MacBook computers issued to staff and contractors, and whether or not the devices were encrypted. We were informed that thirteen (13) devices were issued to employees and that the devices were encrypted and had SecuriKeys; an additional three (3) MacBook devices were issued to ITD staff but not encrypted due to "testing purposes and are not removed from the building." FEC staff stated that exceptions to the policy that all laptops have encryption could only be made by the CIO. We note, however, that the policy does not stipulate: that exceptions are allowed; whether a documented risk assessment is required before granting an exception; who may approve the exception; or how the requests and approval of exceptions are to be documented. There were no documents to support the policy exceptions for mobile devices that were not encrypted noted during this follow-up audit.

We met with one of the Information Technology Division (ITD) employees issued an unencrypted MacBook who explained that encryption was not installed on the computer because no licenses were available at the time. The employee further explained that encrypting the device would have had no impact on device use and testing performed. The employee stated that the device was taken out of the FEC and used to access the network remotely. The device has since been encrypted and verified by auditors through direct observation. We were informed the other two MacBooks are scheduled for encryption once the employees bring them from home.

The January 2011 asset listing showed fourteen (14) employees were issued MacBooks. The following differences were noted between that inventory listing and the email provided by management listing the encrypted and unencrypted MacBooks in December 2010:

- Three Information Division employees listed as having MacBooks in the email were not included on the asset listing;
- One of these three employees has since responded to the audit inventory survey and stated they have two MacBooks, an older model and a new model. Both devices are barcoded. It appears some Information Division employees may have been issued laptops several years ago and those devices are not reflected in the asset listing or the 2010 inventory; and
- Three employees with four (4) total MacBooks were included in the asset listing but not in the email describing which MacBook devices were or were not encrypted.
- The asset listing does not reflect the three ITD staff described in the email as issued unencrypted MacBooks.
- None of the three asset listings provided nor the December 2010 email reflected two MacBooks held by one Information Division employee. The devices were not barcoded or encrypted[6].

The FEC purchased one (1) MacBook on February 26, 2010 and twenty (20) MacBooks on September 20, 2010. It is unclear how many MacBooks were previously purchased and issued to FEC staff and whether or not the devices were or were not encrypted. The discrepancies noted with the various asset listings indicate a complete inventory, based on agency purchases and disposals, is required.

Apple iPads

There are also seven mobile iPads being evaluated by the ITD that connect to the FEC network, are removed from the building and are not encrypted. The devices are not barcoded and are not included in the fixed asset listing[7]. These devices also have AT&T wireless data plans for six months. There is no documented approval for the iPad exception from the encryption policy, but ITD staff pointed out that the assets have the ability to be remotely wiped if the devices are reported lost or stolen. We were informed that the devices were password protected. Management represented that the password requirements for iPads is being evaluated and currently a 4 digit personal identification number (PIN) is the only requirement. In order to protect FEC data, we were told that staff issued iPads were verbally instructed to not save FEC information to the device.

We performed a quick query with Apple on iPad security features and learned that the device includes numerous security features, to include imbedded encryption ("iPad in Business Security Overview" published in April 2010 by Apple). Based on the information provided by ITD staff testing the devices, it appears an inadequate risk assessment and security research was performed for these devices prior to granting access to FEC networks. Instead, there was a reliance on verbal instructions to not download any FEC data on these devices.

Blackberrys

FEC *Mobile Computing Security Policy*, Policy Number 58-4.3, also states:

> *"All mobile computing devices including Blackberries and Palm Pilots must be encrypted and/or password protected."*

[6] Since initially reporting this finding to management, the newest MacBook issued to the employee has been encrypted and barcoded. The older MacBook has been returned to ITD for secure disposal.
[7] The devices have since been barcoded and were included in the third asset listing provided by management.

This statement in the policy is not clear on which devices may be only password protected, compared to others that must be encrypted and password protected. This standard is inconsistent with the statement on page 2 of the same policy that:

> *"All laptops that access the FEC Local Area Network (LAN) will be required to employ whole hard drive encryption."*

Blackberrys assigned to FEC employees and contractors are not encrypted. These devices are password protected and there is the ability to remotely "wipe" a Blackberry if it were reported lost or stolen. Blackberrys can and should be encrypted and password protected to the same standards as other mobile computing devices.

The FEC did not fully implement OMB M-06-16, Protection of Sensitive Agency Information, due to concerns about the amount of system overhead resulting from Blackberry encryption. The lack of encryption on all laptops, iPads, and Blackberrys places the data resident on these devices, which could include PII or FEC sensitive information, at greater risk of unauthorized disclosure if the devices are lost or stolen. The consequences could then be:

- damage to the individuals whose personal information was disclosed;
- adverse media coverage and embarrassment for the FEC and potential Congressional inquiry;
- financial consequences to address an unauthorized disclosure of information; and
- potential litigation.

Encryption Passphrases for Contractors

We were informed by the Information Systems Security Officer that encrypted laptops assigned to contractors use an encryption passphrase assigned by the FEC. This is done to allow access to the information on the laptop if the contractor suddenly or unexpectedly departed the FEC. This process differs from that of FEC employees, who choose their own unique passphrase. Based on mobile devices assigned to contract auditors as part of another follow-up audit, it appears the same passphrase is used for all contractors. The passphrase assigned to contractors is not suitably complex, is relatively intuitive, and could be easily guessed or "hacked" by using basic password detection or "cracking" software. The lack of a unique secret passphrase for each individual increases the risk that the data on that laptop could be accessed by an unauthorized individual.

Recommendations

We recommend that the FEC:

6a. Modify the *Federal Election Commission Mobile Computing Security Policy*, 58-4, to require all mobile devices, including Blackberrys, be encrypted.

6b. Revise *Federal Election Commission Mobile Computing Security Policy*, 58-4 to specify when any exceptions to policy may occur, who may approve the exception, the risks to PII if an exception is granted and any compensating controls, and the level of documentation required to support the exception.

6c. Record all mobile computing devices in inventory when received.

6d. Perform a review of the process and systems used to maintain the inventory of mobile devices to ensure that they are appropriately designed to maintain a complete and accurate inventory. A complete physical inventory of all mobile devices ***purchased*** less

those ***disposed*** should be performed and reconciled to the existing mobile device inventory listing.

6e. Include a record in the inventory listing of whether the device is encrypted or not.

6f. Implement a process and form requiring employees and contractors to sign when they receive a mobile device acknowledging their receipt of the asset and maintain a record of these sign-offs.

6g. Implement an alternative to assigning a generic laptop encryption passphrase to contractors so that every contractor has a unique self selected passphrase, while maintaining the ability to decrypt the stored data in the event of an unexpected departure. The ability to recover unencrypted data of an employee should also be in place.

Further Information on Encryption

There have been significant advances in encryption efficiency over the past few years. Encryption, when properly implemented can provide reasonable security to protect data from unauthorized disclosure. Implementing the recommendation to encrypt all mobile devices would provide consistency with OMB M-06-16 dated June 23, 2006 which states "encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing." In addition, encryption can provide an organization a safe harbor in the event of a security breach. For example, Senate bill S.139 – "Data Breach Notification Act" provides that the notification to affected individuals would be required unless a risk assessment concludes that there is no significant risk that a security breach has resulted in, or will result in, harm to the individual whose sensitive PII was subject to the security breach. There will be a presumption that no significant risk of harm to the individual whose sensitive PII was subject to a security breach if such information was encrypted. There is also a presumption of no significant risk or harm if the data was rendered indecipherable through the use of best practices or methods, such as redaction, access controls, or other such mechanisms, that are widely accepted as effective industry practice, or an effective industry standard. While this and similar bills have not passed into law as of yet, encryption of all mobile devices will allow the FEC to proactively address a likely legal protection for the future, as well as avoid an embarrassing event if an unencrypted mobile device with PII was lost or stolen and the PII was exposed or misused.

Management's General Response to Finding 6:

Prior to responding to the specific recommendations, we would like to generally respond to some of the statements made for this finding. While we concede that the physical inventory process could be improved, an audit of this process was recently completed during the Inspector General's Audit of the Commission's Property Management Controls. We respectfully suggest that pure inventory control issues were more appropriately within the scope of that audit than this one, and we therefore defer to management's responses to that audit where the findings in this report overlap. Also, the report contains many comments regarding unnamed employees who are in receipt of multiple laptops or mobile devices. However without knowing the names of these employees we cannot make a determination as to whether they possess the multiple devices for legitimate business reasons. For instance, several IT personnel possess multiple laptops for various legitimate technological testing purposes. In order to ensure the accuracy of those tests it is necessary that these employees maintain multiple devices, often times with differing security controls. Thus, the fact that an employee possesses multiple devices is not in and of itself a privacy or security danger.

Auditor Response:

Included in the scope of this review was testing of a sample of laptops to verify that encryption was installed on these devices in accordance with current FEC policy. To select a sample of devices for

testing from which we could draw a valid conclusion, we required a complete and accurate listing of laptops. For this reason, the laptop inventory listing was part of the scope. The original and revised listings provided to us contained numerous inaccuracies. As a result, we could not determine with a high degree of precision how many laptops exist at the FEC or to whom, if anyone, they were assigned. Therefore, we were not able to rely on these listings for testing. We acknowledge that multiple devices can be assigned to an employee; however, these devices should all be properly recorded in the inventory. We will provide all the details we have documented to management. We look forward to reviewing the results of management's review of the inventory records and explanation of whether employees with multiple devices are for legitimate business reasons.

Management Response to 6a:

Management concurs in part: Management agrees that encryption is a powerful tool in protecting sensitive information from breach. However, because the encryption process is tied to an individual user (e.g., an encrypted device requires that the user enter a unique passphrase and password tied to the individual in order to get into the laptop) encryption would not be practical for a device that is used by multiple people (e.g., laptops attached to scanners). For that reason, management agrees to ensure that all unencrypted laptops will be locked and secured with a security cable so as to prevent removal from the building. All other laptops (i.e. those assigned to a specific user) will be encrypted. With respect to Blackberries, it is our understanding that the transfer of information to Blackberries is encrypted while in transit, and that the Blackberries were recently updated to include encryption at rest. Management will continue to investigate mechanisms for securing other mobile devices. It should be noted that the OCIO has the ability to conduct remote wipes of information on mobile devices so as to minimize the effects of a loss. Finally, Management also agrees to modify its Mobile Computing Policy to accurately reflect its encryption practices.

Auditor Response:

We encourage management to confirm that the encryption functionality is activated for all FEC Blackberry devices. We also look forward to reviewing the details regarding the timing of the policy update in the corrective action plan. The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation.

Management Response to 6b:

Management concurs in part: We do not agree that exceptions to the Mobile Computing Security Policy should be noted in the policy itself, since exceptions are rare and are granted on a case-by-case basis. We do agree that the policy should be revised to reflect that exceptions to the policy must be granted by the CIO. We do not agree to specify risks to PII if an exception is granted, since that is already a component of the FEC's Certification & Accreditation program. Nor do we believe it is appropriate to include specific risks to PII, if an exception is granted, in this policy document since the risks will depend on the specific exception and the facts warranting the exception. We do however intend to inform those that are granted an exception of the risks to PII associated with the exception granted.

Auditor Response:

We are not recommending that the policy be modified to describe specific exception scenarios, but that the process by which an exception is requested, approved/denied and documented be a matter of policy. We believe it is important to consider the risks to PII for every exception request as they will vary on a case-by-case basis and may not have necessarily been considered as part of the FEC's Certification & Accreditation program.

Management Response to 6c:

Management does not concur: Management respectfully believes that this finding goes beyond the scope of this audit, and refers to its General Response to Finding 6. To the extent this finding relates to the securing of data on mobile devices, we agree that encryption can be used for that purpose and refer the auditors to our response to 6a.

Auditor Response:

See Auditor Response to Management's Response to Finding 6 and 6a.

Management Response to 6d:

Management does not concur: Management respectfully believes that this finding goes beyond the scope of this audit, and refers to its General Response to Finding 6. To the extent this finding relates to the securing of data on mobile devices, we agree that encryption can be used for that purpose and refer the auditors to our response to 6a.

Auditor Response:

See Auditor Response to Management's Response to Finding 6 and 6a.

Management Response to 6e:

Management does not concur: Management agrees to review its inventory process to determine whether it is necessary to combine the inventory list and the encryption list to ensure the protection of PII information.

Auditor Response:

We believe that maintaining a record of whether the device is encrypted in the inventory list will allow management to quickly know if a lost or stolen device was encrypted, which is necessary to understand the resulting risk to the information that was stored on the device. We look forward to reviewing the details in the corrective action plan for improvements to the inventory process.

Management Response to 6f:

Management does not concur: Management respectfully believes that this finding goes beyond the scope of this audit, and refers to its General Response to Finding 6. To the extent this finding relates to the securing of data on mobile devices, we agree that encryption can be used for that purpose and refer the auditors to our response to 6a.

Auditor Response:

See Auditor Response to Management's Response to Finding 6 and 6a.

Management Response to 6g:

Management concurs: Management agrees to provide contractors with unique passphrases for laptops.

Auditor Response:

The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation.

Finding 7: Safeguards Over Sensitive Agency Information and PII Need Improvement

We performed an after-hours walkthrough of the Commission building on November 10, 2010 and January 19, 2011, and noted some improvements since the prior walkthrough performed by Cotton & Company and OIG staff in November 2007, such as:

- Many offices were locked, effectively securing the contents from other employees, contractors or visitors, but not facility maintenance or cleaning staff that have a master key for all locks.
- There were secure shred bins and shredders throughout the building. The secure shred bins were padlocked.

During the walkthrough, we also identified several instances where sensitive information and PII was easily accessible to unauthorized personnel. We concluded that controls are not adequate to ensure that sensitive information, including personally identifiable information (PII) collected, processed, or stored by the FEC has been adequately safeguarded. Specific examples of weaknesses observed include:

- Individuals' applications for FEC employment containing names, addresses, phone numbers, and social security numbers were located in an unsecured office.
- Confidential blue folders possibly containing sensitive information or PII were in unsecured areas, such as in common area mail slots and on desks in common areas.
- FEC employee and contractor PII was noted in unclaimed print jobs near common area printers in unsecured areas.
- Some employees left their personal mail including credit card statements, bank statements, medical insurance information, and utility bills, etc. in plain view. One employee left their Federal credit card statement in plain view. This observation is potentially indicative of a lack of understanding of the importance of protecting not only employees' own personal PII, but also the PII that has been entrusted to the FEC.
- Modular workspaces and unlocked offices often had unsecured laptop computers that contained SecuriKeys (a hardware device that is inserted into the computer and is a second factor of authentication, in addition to the user ID and password), including a number of Apple laptops. None of the Apple laptops had a security cable attached to prevent someone from taking the laptops outside the building.
- One employee left a post-it note with an encryption pass phrase, network log-on, and password on their desk. Passwords on post-it notes were also noted for several employees in one division.
- Filing cabinets located in common storage areas for one division was deliberately left unlocked. Some had keys taped to the cabinets while others had the locks disabled with masking tape. Contents of many cabinets included documents marked "sensitive."
- "Matters Under Review" (MURs) and other sensitive work product documentation was found in unsecured areas, such as on employees' desks and in unlocked common area cabinets. Typically, the work products did not contain security classification labels such as "sensitive" or "confidential," but should have, to reflect the confidentiality of the information.
- FEC confidential and proprietary documents produced by three different contractors as part of their service to the FEC were left unsecured in modular work space for up to two years. Some of the documents contained process flow diagrams for FEC applications and assorted procedural documents. Some of the documents were labeled "Confidential" and "Confidential Do Not Distribute," while others appeared sensitive but were not labeled.

FEC Privacy Policies and Procedures[8], 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."*

Consolidated Appropriations Act, 2005, Section 522 states:

> *Section (a)(7): "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."*
>
> *Section (a)(1): "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."*

OMB M-05-08, *Designation of Senior Agency Officials for Privacy*, dated February 11, 2005, pg. 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."*

Commission Document Security Classification and Labeling

As noted above, the walkthrough showed improvement is needed in classifying and labeling documents that contain sensitive information or PII. The *FEC Information Classification Policy* 58.1.3 states:

> *"An information security model should be developed to assist FEC management with classifying and securing information. This information security model is to be used only as guidance not as a standard."*

Although the *Federal Election Commission Guide to Protecting Sensitive Information* describes the two classes of information held by the agency as "public" and "sensitive" (a.k.a. confidential), it does not

[8] The policy was approved by the Commission on December 4, 2007. The document is not dated.

specify the need to label electronic files so that when the files are printed, the documents indicate whether they are sensitive and need to be stored securely. The guide does state:

> *"Information identified as sensitive should not be left in areas where unauthorized persons may have an opportunity to view it. This includes your work area. A screen filter may be an option to consider. Sensitive documents that are to be disseminated via internal mail shall be enclosed in an envelope marked sensitive and/or confidential."*

The guide does not require the divisions to use templates that include security classification labels in the header and/or footer of a file so that the classification can be viewed on screen and on each printed page. Including a requirement to identify sensitive work products and develop standard forms with embedded security classifications markings would ensure printed documents are labeled so that the need to physically secure them is evident. As an example of a labeling weakness detected during the walkthrough, we noted a group of eleven (11) FEC forms, some one page and others multiple pages, left unsecured by former contractors. Seven of the forms were labeled "confidential" on the first page. One of the forms had the security classification included on *each* printed page. Three forms did not include the security classification on the first page, but the "confidential" label was located on at least one page of the multipage documents. It appears the security classification label intended for the first was displaced by the amount of data included on the first page of the form, forcing the security label to print on page two of the document. One form had no security classification label, but should have been labeled.

As noted above, filing cabinets in common areas of one division were disabled to prevent locking or had keys attached to ensure they could be accessed by all staff. Some of the cabinets had files marked sensitive and some had PII, such as copies of personal checks with banking information. A door to a common file room was unlocked and had a note requesting staff not lock the door. Most filing cabinets in that room were locked, however two were unlocked. The files in the two unlocked cabinets included some documents marked sensitive, and others that were not labeled, but due to the content, should have been labeled "sensitive."

The FEC does not have detailed procedures for classifying and labeling sensitive information. In addition, the divisions may not have adequately communicated secure storage needs, including the need to have secure storage accessed by a group of employees, to the FEC Security Officer and Records Manager. Sensitive documents, including those with PII, could be accessible by FEC staff, contractors, or service personnel such as cleaners and facilities maintenance staff that do not have a valid business need to access the records. This increases the risk of data breach and unauthorized disclosure.

Requirement to Review Current Security Designations

President Obama issued Executive Order 13556, *Controlled Unclassified Information* on November 4, 2010[9]. The executive order recognized the fact that:

> *"At present, executive departments and agencies (agencies) employ ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing. To address these problems, this order establishes a program for managing this information, hereinafter described as Controlled Unclassified Information, that emphasizes the openness and uniformity of Government-wide practice."*

[9] Executive Order 13556 is included as Attachment 4 of this report.

As a result of this executive order, by May 4, 2011, the FEC will be required to:

> *(1) "review all categories, subcategories, and markings used by the agency to designate unclassified information for safeguarding or dissemination controls; and*
>
> *(2) submit to the Executive Agent a catalogue of proposed categories and subcategories of CUI, and proposed associated markings for information designated as CUI under section 2(a) of this order. This submission shall provide definitions for each proposed category and subcategory and identify the basis in law, regulation, or Government-wide policy for safeguarding or dissemination controls."*

The National Archives and Records Administration (NARA) serves as the Executive Agent to implement this order and oversee agency actions to ensure compliance with this order. By implementing Executive Order 13556, the FEC will assess current categories, subcategories, and markings used by the agency to designate security classifications. Based on the assessment, the agency will then have the opportunity to propose standards and definitions for security categories and markings to NARA. Once the assessment process has been completed and approved by NARA, the FEC can implement procedures to ensure the standards are applied and enforced throughout the Commission.

Contractor Records

The FEC's Procurement Procedures – 020 Contracting Officer Technical Representative (COTR) Program, states:

> *"If contractor employees (or their subcontractors) will have access to FEC property (real, physical, or electronic), you must ensure that they follow the provisions of the contract and comply with the guidelines established by the FEC, including but not limited to, guidelines related to information about individuals and commercial information owned by other third parties, including personally identifiable information, protected by the Privacy Act and other federal laws for the protection of government property;…"*

Standard language in FEC contracts includes the following:

> *"NON-DISCLOSURE OF CONFIDENTIAL DATA STATEMENT: As Required in writing by either the Statement of Work, Contracting Officer or COTR - - Within ten business days of receipt of notice of award, the contractor shall provide a signed copy of the FEC Non-Disclosure Agreement (See Attachment 6) for all personnel involved in the engagement. Approved replacement personnel shall provide a completed agreement when assigned to this contract. No access will be given until the Non-Disclosure Agreements are provided to the Contracting Officer with a copy to the COTR."*

As part of the FEC's contracting process, contractors are required to sign a non-disclosure agreement which defines the standards for protecting sensitive information as well as PII during the course of service delivery.

2. "*Disclosure of FEC information*. I agree to hold the FEC's sensitive, protected, and confidential information, including personally identifiable information, in whatever form or format, in strict confidence, and to take all reasonable precautions to protect against unauthorized use or unauthorized disclosure of such information, including but not limited to compliance with the Rules of Behavior and Acceptable Use Standards for Federal Election Commission Information and System Resources.

4. *Duty to report.* I agree to report immediately to an appropriate employee of the FEC any unauthorized use, unauthorized disclosure, or other breach of sensitive, protected, and confidential information of which I become aware, or which I suspect has occurred or may occur."

The non-disclosure agreement also defines the return and destruction processes required at the conclusion of the contract as follows:

5. "*Return of FEC material and information.* At the conclusion of my work under this contract, I will return to the FEC (or destroy, upon written approval of the Contracting Officer) all FEC material, including copies, and all records containing FEC material and information.

6. *Destruction of Personally Identifiable Information (PII).* Prior to final payment on the contract, I will verify with the COTR and/or contracting officer that I have destroyed any and all FEC PII that has come into my custody while working for or at the FEC. The destruction method must be consistent with FEC IT Security Policies."

In providing services to the Commission, contractors are given access to FEC systems and records that are sensitive or confidential. The results of the walkthrough showed that at least three contractors failed to comply with the policy and did not:

- take reasonable care to protect "FEC's sensitive, protected, and confidential information, including personally identifiable information"[10];
- include adequate security classifications and labeling on files to indicate the need to store printed documents in a secure location;
- return FEC materials and information to the COTRs at conclusion of service delivery; and
- remove and destroy excess records not needed for its own official record of service delivery to the Commission.

For these contracts, the Commission may not have received, and the COTRs may not have requested, a final certification from the contractor or verified that the certification was accurate prior to approving final payment. COTRs are not required to perform a walkthrough of the space used by contractors to verify that all paper or other documents or records were securely disposed of or filed at the end of the assignment. The FEC may not enforce the contract requirement that contractors certify secure disposal, destruction or return of FEC records prior to final payment.

Specialized Training

In the PII Assessment Report provided to the FEC on May 20, 2009 by STSI, the contractor recommended as a short term task that the agency "Expand training of employees and contractors on the specific procedures necessary to safeguard documentation containing PII processed during the course of their duties." The FEC has not yet developed division level or job/role specific privacy training to address the different operating environments throughout the agency. The results of the walkthrough indicated more specialized training for some divisions or job specific roles may be required to ensure adequate protection of sensitive information and/or PII. Lack of detailed training on business processes and forms unique to the various divisions in the agency prevents employees from fully adopting privacy and data protection best practices specific to their roles and responsibilities. The FEC has recently completed a draft evaluation of the recommendations of the STSI PII Assessment Report and has not

[10] Two contractors left their own PII unsecured in a modular workspace.

implemented the recommendation to develop more detailed training specific to divisions or roles/responsibilities.

Securing Mobile Computing Devices and Passwords

The *2007 Privacy and Data Protection Audit* walkthrough results showed that some FEC employees had not adequately secured their laptop computers by removing the SecuriKey device or protected their log-on and password. In response to the 2007 audit walkthrough results, the 2008 Mandatory Security Awareness Training stressed the need for employees and contractors to comply with *Rules Of Behavior and Acceptable Use Standards For Federal Election Commission Information systems and Resources,* specifically:

- *Section 8.d - "Protect your password from disclosure. Specifically, do not post your password in your area."*
- *Section 18 - "Protect FEC commuting 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."*

In the 2008 and 2009 FEC Privacy 101 Training presented to employees and contractors via PowerPoint, the slide on laptop security stressed that "all FEC laptops must be secured with a security cable" and "when leaving your office, the secure key (SecuriKey) should be removed or your door locked." The walkthrough results of this follow-up audit indicate that training alone is not sufficient to ensure employees and contractors comply with FEC privacy and data protection policies, procedures and standards. The annual IT Security and Privacy training may not be practiced by employees and contractors because neither the ISSO nor the Security Officer performs regular walkthroughs to verify that Commission staff complies with privacy and data protection standards.

Recommendations

We recommend that the FEC:

7a. ISSO, Physical Security Officer, and/or division management should conduct regular walkthroughs to ensure that agency staff complies with privacy and information security standards;

7b. Should emphasize document labeling requirements with all staff and standard document templates with labels be created and the use monitored;

7c. Should develop a plan to implement Executive Order 13556, *Controlled Unclassified Information*, and comply with future directives issued by NARA;

7d. Division managers should work with the Physical Security Officer and the Records Officer to assess records management and secure storage needs and address failures to adequately secure sensitive information noted during the walkthrough;

7e. Contracting Officer and COTRs should enforce the requirement for contractors to certify secure destruction or return of FEC information in both paper and electronic format;

7f. Should establish policy and procedures requiring COTRs to inspect the physical space occupied by contractors when the contractor departs to ensure paper and electronic records are securely disposed of or filed; and

7g. Should implement the plan to develop and deploy privacy training specific to the individual divisions.

Management Response to 7a:

Management concurs: Management will commit to having the ISSO, Physical Security Officer and other management officials as appropriate participate in occasional walkthroughs of the building to ensure privacy and information security standards are being met. This commitment is subject to Commission approval of this policy.

Auditor Response:

The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation. We look forward to reviewing the details regarding the timing and scope of the planned walkthroughs in the corrective action plan.

Management Response to 7b:

Management does not concur: Management does not believe it is practical to require staff to label every document created by employees. Such a requirement could slow down Commission work processes. Moreover, we believe that the prescribed privacy benefit of labeling (i.e. that persons will treat documents marked "Sensitive" in a different manner than documents that are not marked) is not necessarily realistic.

Auditor Response:

Currently, the lack of an agency-wide labeling process relies on each employee making a determination of how a particular document or file is to be protected. As a result, the protection of information may or may not be adequate or meet the expectations of FEC leadership. The recommendation would involve management establishing standard document templates so that staff would not be required to make these decisions.

Management Response to 7c:

Management concurs in part: Management agrees and has developed a plan to implement Executive Order (EO) 13556. However, based on our conversations with National Archives and Records Administration (NARA) officials, we believe the agency's responsibilities under this EO are different from what the auditors appear to think they are. We spoke to Carla Riner, Lead for Policy and Strategic Planning for the Controlled Unclassified Information Office of NARA, who was a part of the team that drafted Executive Order 13556. According to Ms. Riner, the purpose of EO 13556 is not to label every document in the agency, but to ensure that the labels agencies are currently using are legally mandated. To that end, agencies were asked to fill out a matrix by no later than May 4, 2011, including information the agency "would like to be considered controlled" and the law that requires that the information be protected. After agencies submit the matrix information, NARA will issue a series of instructions to "phase in" implementation of the government-wide labeling system. To the extent this recommendation asks management to comply with the EO and other NARA guidance, management concurs. To the extent this recommendation asks management to implement new procedures to ensure expanded labeling is applied and enforced throughout the Commission, management does not concur as that is not a mandate required by the EO or currently by NARA.

Auditor Response:

Our recommendation is for management to develop a plan to implement Executive Order 13556, which is independent of the labeling recommendation in 7b. We acknowledge management's concurrence to develop a plan to comply with Executive Order 13556 and other NARA guidance and when fully implemented, should satisfy the intent of the audit recommendation.

Management Response to 7d:

Management concurs: Management agrees to work with the Physical Security Officer and the Records Officer to address the securing of storage areas and records management. As a part of this process, management will look into the locking of suite doors after business hours as a potential security safeguard.

Auditor Response:

The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation.

Management Response to 7e:

Management concurs: Management concurs with this recommendation and will work with the Contracting Office to determine the best course of action for enforcing this requirement.

Auditor Response:

The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation.

Management Response to 7f:

Management concurs: Management concurs with this recommendation and will work with the Contracting Officer to develop said policies and procedures.

Auditor Response:

The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation.

Management Response to 7g:

Management concurs: Management concurs with this recommendation and is already in the process of developing division-specific training.

Auditor Response:

The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation.

Finding 8: Lack of Detailed Procedures and Periodic Review

The FEC has twenty-eight (28) separate policies governing data security (58.x documents, e.g., Federal Election Commission Personnel Security Policy 58-1.1, Federal Election Commission Security Training and Awareness Policy 58-1.2). Supporting the data security policies are four (4) procedures, eighteen (18) standards, and one (1) guideline. The FEC has two (2) policies governing privacy and data protection supported by one rule of conduct and one plan to reduce the use and retention of personally identifiable information.

Despite the volume of policies, there is a general lack of detailed procedures that describe how the requirements in the security and privacy policies are to be implemented beyond the four existing procedures: *Access Control Procedures*; *OIT Procedures for Disabling User Accounts*; *Office of Information Technology Incident Response Procedures;* and *Procedures for Managing Change Requests*. For instance, the *Federal Election Commission Privacy Protection Policies and Procedures* document does not contain any procedures. Section III, "Consent." states:

> *"Unless authorized by law, or qualifying for an exemption under the Privacy Act, consent should be obtained from an individual before a record pertaining to that individual, contained in a system of records, is:*
>
> *Used for a purpose other [missing the word "than"] the purpose for which it was collected; or*
>
> *Disclosed to any person or to another agency.*
>
> *However, use and disclosure without consent is permitted under certain circumstances as delineated in subsection (b) of the Privacy Act, such as the exception for routine uses published in the System of Records Notice. FEC offices should consult with the FEC Privacy Officer on questions regarding disclosure or alternative uses without consent."*

The policy does not contain procedures that clearly describe how the requirements would be accomplished. For example, the policy does not answer the following questions:

- Is there a standard form to request and document consent?
- Is written consent required or is electronic consent acceptable?
- Who is responsible for obtaining the consent?
- Are any identity verification procedures required?
- Where should the consent documents be filed?
- How long should the consent documents be maintained?

Another example is the *FEC Media Management Security Policy* 58.4-2, which states:

> *"It is FEC policy that:*
>
> *Procedures will be defined and implemented to protect computer media such as magnetic tapes, magnetic and optical disks, memory chips, CD ROMs, and other storage devices, throughout their life cycles, taking into consideration applicable property management policies and procedures;*
>
> *Procedures will be defined and implemented to prevent access to electronic information and software from computers, disks and other equipment or media when they are disposed of or transferred outside FEC control. These procedures should aim at preventing electronic data that*

has been deleted or disposed of from being retrieved. Disposal measures should be cost-effective, taking into account information sensitivity; FEC Media Disposal Standards are relevant here."

While there may be practices in place to address the above requirements, there are no documented procedures.

Definitions of policies, procedures, guidelines and standards used by the Information Systems Auditing and Control Association (ISACA), an independent, nonprofit, global association, that engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems are:

Policies are a document that records a high-level principle or course of action which has been decided upon. A policy's intended purpose is to influence and guide both present and future decision making to be in line with the philosophy, objectives and strategic plans established by the enterprise's management teams.

Standards are a mandatory requirement, code of practice or specification approved by a recognized external standards organization, such as International Standards Organization (ISO).

Procedures are a detailed description of the steps necessary to perform specific operations in conformance with applicable standards.

Guidelines are a description of a particular way of accomplishing something that is less prescriptive than a procedure.

Based on the standard definitions and detailed review of FEC documents, additional procedures and modification to existing supporting documents is required.

Further, the following documents do not have an adoption date or current version date.

- Federal Election Commission Privacy Protection Policies and Procedures;
- Federal Election Commission Guide to Protecting Sensitive Information;
- Federal Election Commission Policy and Plan for Responding to Breaches of Personally Identifiable Information;
- Federal Election Commission Privacy Rules of Conduct;
- Access Control Procedures; and
- the 18 IT Security standards.

There is no defined periodic review cycle, and updating as necessary, for the documents listed above. Dating policies and procedures is a common practice. There is not a standard template used for all FEC policy documents that includes dating.

FEC Directive 65, *Designation of Chief Privacy Officer and Senior Agency Official for Privacy*, December 4, 2007, references OMB M-05-08 and states the Senior Agency Official is responsible for *"Reviewing and updating policy procedures."*

The *International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 2700*2 , "Information technology-Security techniques-Code of practice for information security management", is a globally accepted information security standard and is considered best practice. This standard states:

"Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes."

The FEC has not implemented a framework or assigned responsibility to specific staff for designing, documenting, communicating and training staff on detailed procedures necessary to implement the existing policies. Instead, since the number of the FEC staff is relatively small, there is reliance on quick and close communication amongst staff to address any questions regarding policy implementation.

Without detailed procedures to support the documented policies, FEC staff may not be sure how to comply with the policies, and management may not be able to hold staff accountable for full compliance. As new employees assimilate into their positions at the FEC, they will not know for certain what the expected compliance procedures are. Instead they will have to ask or observe others and may or may not learn the appropriate procedures.

If privacy policies and supporting documents are not reviewed regularly and updated, they may not address the current legal requirements and risks. Failure to date the agency policies and procedures may result in employees not realizing they are referring to an outdated policy or authoritative document, and can decrease compliance with current requirements. Further, the current condition diminishes the FEC's ability to successfully enforce disciplinary action if an employee unknowingly relies on an outdated policy or procedure.

Recommendations

We recommend that the FEC:

8a. Should develop, implement and communicate detailed procedures to all employees for each security and privacy related policies. This may need to occur at the division or department level with the Privacy Team serving as subject matter experts. Detailed procedures will also be helpful for agency staff tasked with monitoring, enforcing and reporting on compliance with the requirements in the associated policies.

8b. Should directly link detailed procedures to the source policies and house them in a central, easily accessible location, such as the FEC Intranet.

8c. Should follow a standard template for all policies and supporting documents that includes an adoption and last revision date.

8d. Should review on a regular basis all of the privacy and data security policies, procedures, standards and guidelines on a defined timeframe (e.g., annually), and they should be dated, and updated as necessary and include a point of contact if employees have questions.

Management's General Response to Finding 8:

Prior to responding to specific recommendations, we had a few comments regarding some of the findings in this section of the report. First, we note that IT security policies are reviewed on an annual basis, thus it is not true that "[t]here is no defined periodic review cycle, and updating as necessary," for those policies. Second, we do not agree that the failure to place dates on policies would diminish the agency's ability to "successfully enforce" those policies if the employee has been provided with the new policy and

still relies on an outdated policy. Employees are held accountable to agency policies unless it is clear that the policies have been revised or overturned.

Auditor Response:

We acknowledge that IT security policies are reviewed on an annual basis. However, there are other documents that are important to the privacy and information protection program that do not appear to have a defined review cycle. Our recommendation was intended to address the review cycle for the following documents:

- Federal Election Commission Privacy Protection Policies and Procedures;
- Federal Election Commission Guide to Protecting Sensitive Information;
- Federal Election Commission Policy and Plan for Responding to Breaches of Personally Identifiable Information;
- Federal Election Commission Privacy Rules of Conduct;
- Access Control Procedures; and
- the 18 IT Security standards.

Management Response to 8a:

Management concurs in part: Management does not concur with this finding in that we do not believe overarching agency-wide procedures should be detailed to the level specified by the auditors. Nevertheless, we do agree that detailed procedures may be necessary at the division or departmental level. The Privacy Team will encourage and work with FEC division heads in their development of office-specific procedures when necessary.

Auditor Response:

Although FEC management does not concur with the finding, management has agreed to improve procedures at the division level. We look forward to reviewing the details of the plan to coordinate with FEC division heads in the corrective action plan.

Management Response to 8b:

Management concurs: At present, the agency's IT security policies are housed on the FEC-Wide network drive in the IT policies and standards folders. However, we agree that both privacy and IT security procedures should be housed in a centralized and easily accessible location, and that the FEC Intranet ("FECNet") would be an invaluable communication tool for that purpose. The Privacy Team has already commenced this process by working with OCIO to develop a Privacy FECNet page.

Auditor Response:

The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation.

Management Response to 8c:

Management concurs in part: Management concurs with the finding that privacy policies should contain an adoption and last revision date, and will revise its policies to ensure such designations are included. We will continue to evaluate whether confidential or sensitivity designations are appropriate for the privacy policies and procedures. We do not agree that a standardized template for privacy policies is always appropriate.

Auditor Response:

A standardized template provides consistent presentation of policy content and can make it easier for a reader to quickly find the information of most interest. However, the substance of the policy is ultimately more important than the format. The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation.

Management Response to 8d:

Management concurs in part: Management agrees that privacy and data security policies, procedures, standards and guidelines should be reviewed periodically to determine if updates are necessary. However, because most of these policies serve as overarching umbrella privacy policies for agency-wide use, it is unlikely that frequent revisions are necessary. We therefore agree to institute a biennial review of the privacy policies. We note that IT security policies are currently reviewed on an annual basis. We concur with the auditors' finding that policies, procedures, standards and guidelines should contain effective dates and revision dates as necessary, and should include a point of contact if they do not already (we note that many of the policies already list the Privacy Officers or the Information Systems Security Officer as key points of contact).

Auditor Response:

We recognize management's efforts to concur with our recommendation. However, we would still encourage that they increase the frequency of this review to annually because of the ever changing nature of privacy risks.

Finding 9: Logging

OMB M-06-16, Protection of Sensitive Agency Information, issued June 23, 2006 states:

> *"In an effort to properly safeguard our information assets while using information technology, it is essential for all departments and agencies to know their baseline of activities. The National Institute of Standards and Technology (NIST) provided a checklist for protection of remote information. (See attachment) The intent of implementing the checklist is to compensate for the lack of physical security controls when information is removed from, or accessed from outside the agency location. In addition to using the NIST checklist, I am recommending all departments and agencies take the following actions:*
>
> 1. *Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing;*
>
> 2. *Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;*
>
> 3. *Use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity; and*
>
> 4. *Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required."*

The agency agreed to implement the first three of the four recommendations. In an August 23, 2006 memo to the Commission from the CIO and ISSO, in response to M-06-16, the logging recommendation was not implemented given the opinion "that the cumulative effects of encrypting the entire hard local drive, requiring a 30 minute time out for inactivity and employing a two-factor authentication scheme reduces the Commission's risk exposure to an acceptable level."

Encrypting the entire local hard drive, requiring a 30 minute time out for inactivity and employing a two-factor authentication scheme is not a substitute for logging access to and extracts from systems containing sensitive data.

Logging of FEC systems activity is currently only performed at the network access level and does not include specific systems (databases) containing PII. Therefore, the details of file access are nonexistent and the following details are not recorded or monitored: 1) identity of individual/divisions accessing specific files; 2) the date/time and actions that were taken on individual files, such as created, copied, updated, or deleted.

FEC's Auditing and Monitoring Policy, 58-3.3, also states:

> *1. "PURPOSE*
>
> *This policy is designed to:*
>
> *a. Satisfy the purposes and policy goals of the Federal Election Commission (FEC) Information System Security Program Policy, Policy Number 58A.*
>
> *b. Establish control over the process of monitoring and logging system and user activities. This policy is designed to address the requirement to monitor systems to detect potential threats to electronic information, and record selected system activities that will be stored with integrity, and reviewed by management on a regular basis to detect problems. The policy is enabled by facilities and procedures for the monitoring, logging and reviewing system and user actions and high-risk transactions, detecting unauthorized activities are, and for enabling systems' and business processes' integrity to be quickly restored following a security incident. This policy takes into consideration:*
>
> *I. Authorization;*
> *II. High-risk transactions;*
> *III. Data integrity;*
> *IV. Risk assessments; and*
> *V. Security incidents.*
>
> *It is FEC policy that:*
>
> - *FEC information systems have capabilities to automatically monitor, log and review of selected user and system actions, events and transactions. Automated monitoring and audit logging facilities must record, at minimum, actions, events and high-risk transactions articulated in FEC Audit Event Standards;*
>
> - *Selected system and user actions, events and high-risk transactions to be automatically monitored and/or logged are identified and documented for each FEC computing resource. This list of auditable events is based upon the past experience of error misuse, criticality and interconnectivity of the system processes, events and information;*

- *Periodic reviews are conducted to ensure monitoring results and audit logs are valid;*

- *Audit logs are retained so as to preserve their value as legal evidence, and to help identify, prosecute, resolve and/or mitigate security incidents. A framework of controls exists to control physical and logical access to FEC logging facilities and storage media in a way that protects them from unauthorized access, use or modification;*

- *Audit logs' retention period is based upon FEC operational requirements, applicable federal guidance, laws and/or regulations;*

- *All FEC information systems that have the capability to operate a real-time clock will have the clock set to an agreed upon standard (e.g. Universal Coordinated time or local standard time) so that audit logs are both accurate and comparable. Procedures should be developed to check for and correct significant variations from this standard."*

The FEC has not implemented detailed system logs due to concerns about system storage resources and associated costs required to maintain and review such logs.

The lack of detailed system logs will result in a compromised ability to perform forensics should there be a data breach. Our discussion with the FEC Information Systems Security Officer (ISSO) indicated that there were no known system security or data breaches in 2010; however, without a logging and monitoring system in place, it is not possible to know if there were any attempted or successful system intrusions.

Recommendation

We recommend that the FEC:

9. Implement logging for all computer-readable data extracts from databases holding personally identifiable information (PII).

Further Information on System Logging

System logging is built into numerous applications. The feature can be enabled on a trial basis for some systems containing PII to establish a baseline for electronic storage needs and evaluate actual performance issues. The results will provide quantitative data upon which the Commission can make informed decisions about logging for all systems that contain PII. Depending on the results and individual division needs, logs can be rotated on a predetermined basis.

The Solutions Technology Systems, Inc. report issued in May 2009 contained a comprehensive inventory of applications that contain PII. The report also identified the divisions that process PII and the FEC ISSO can choose a relatively small division to pilot this project.

Management Response:

Management does not concur: Management continues to believe that the encryption, 30-minute time out, and two-factor authentication controls currently in place for FEC mobile devices and computers are sufficient to prevent and/or significantly reduce the agency's risk exposure. As noted by the auditors, the agency currently monitors and logs access to the agency's network. We manage access to sensitive information by properly managing access control, i.e. we only provide access to sensitive information to those individuals who need access in order to complete their authorized duties. Therefore additional

logging of persons already authorized to access, copy, delete, and/or move PII would not be cost effective.

Auditor Response:

We acknowledge that the controls management describes are appropriate. However, without logging, there is no record of system user activity and the nature of system activity which is essential for a forensic review in the event of a system intrusion or unauthorized activity. Effective logging not only captures the activity of employees but also the activity of unauthorized individuals or entities if they penetrate the FEC's network.

Finding 10: Protections for Remote Access to PII

The FEC Policy 58-4.5, *Virtual Private Network (VPN),* does not specifically require that employees must save work related data to FEC network drives instead of the local hard drive. FEC Directive 58 *Electronic Records, Software and Computer Usage* states:

> *"As the principal component of FEC System Security Program, end users take on the burden of protecting the confidentiality, integrity and availability of information when you bypass FEC security guidelines by saving your work to media other than the FEC network. As in the case of paper records, each individual user is also responsible for the erasure and/or destruction of any sensitive information the user chooses to store outside of the FEC network."*

As written, the policy is clear but is not adequate in that it provides employees the flexibility to save work locally as needed with the "burden of protecting the information." The policy does not limit the practice to specific working arrangements or emergency situations, such as remote audits or inability to access the FEC networks.

This is a prior audit finding that management disagreed with, and instead chose to rely on email reminders.

Users may save their work to local hard drives thus placing the information at greater risk of being accessible by an unauthorized individual. Also, the practice of saving information locally does not enable automatic back-up and recovery of information if a computer is lost, stolen or impaired. Failure to explicitly state the requirement to save all data to FEC networks in a policy compromises the agency's ability to monitor and enforce employee protection of work related data.

Recommendations

We recommend that the FEC:

10a. Should change Policy 58-4.5, *Virtual Private Network (VPN),* and Directive 58, *Electronic Records, Software and Computer Usage,* to state that work related data must be saved to the network and not downloaded and saved on local devices. Exceptions to the policy should be clearly documented and approved by management, and, where possible, compensating controls put in place.

10b. Should further re-enforce the key elements in Policy 58-4.5, *Virtual Private Network (VPN),* and other security policies and also design and implement a formal communications plan to re-enforce key privacy and security principles contained in the policies and training. This communication plan should include scheduled periodic reminders to employees and contractors on key principles that can be delivered through

such means as emails, log-in banners, newsletter articles, posters or other existing communication vehicles currently used to communicate with employees. The most effective messaging is typically brief and focused on a single topic. For example, an email message such as: REMINDER: Save all your work on the network and do not download to your computer.

10c. Modify the Intranet to contain a page with Privacy and data protection policies, procedures and updates. This would ensure that all FEC employees are aware of the policies with regard to PII, and privacy and data protection.

Management Response to 10a:

Management concurs in part: While management concurs with this concept in general, we note that some of the factual findings are inaccurate. The audit report assumes that employees are given a choice as to whether to save information on the FEC network and that current policies reflect that choice. However, the most current version of the Virtual Privacy Network (VPN) Policy 58-4.5 (adopted May 19, 2009 and revised in February 2010) requires that employees "[s]ave work-related data to the network to ensure proper backup occurs." Thus, our current policies already implement this recommendation. Nevertheless, we concur with the use of the verb "must" in future revisions to the policy and will make those changes in the Policy and in Directive 58 if necessary. It should further be noted that employees are informed in privacy training that "[e]mployees and contractors **must** save work-related data to the FEC network." We would also agree that the VPN policy should include information regarding requesting exceptions to the policy, namely that the policy will: 1) include a statement that exceptions will be made on a case-by-case basis; 2) name the agency official authorized to grant an exception (e.g., Chief Information Officer); and, if possible, 3) provide examples of the criteria used to grant an exception.

Auditor Response:

The quote from Policy 58-4.5 is: "All VPN users are encouraged to remember that: save work-related data to the network to ensure proper backup occurs." Our recommendation is that this wording be stronger. The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation. We look forward to reviewing the updated policy.

Management Response to 10b:

Management concurs: Management agrees to develop a communication plan that will include methods of re-enforcing key privacy and security principles via the use of log-in banners, emails and/or other vehicles (e.g., using FECNet as a communicating tool).

Auditor Response:

The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation. We look forward to reviewing the communication plan.

Management Response to 10c:

Management concurs: Management agrees to develop a Privacy page on FECNet and has already begun this process.

Auditor Response:

The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation.

Finding 11: Vendor Due Diligence

The FEC privacy governance framework should be expanded to include not only PII that is collected, processed, transmitted or stored by the FEC, but also PII that is provided to and/or stored by vendors. Currently, there is no comprehensive list of all vendors that handle FEC PII and there is no formal process in place to understand, document, and assess the controls in place at vendors, prior to, or after, providing access to FEC PII. Instead, the agency primarily relies on protective language in the contractual agreements with these vendors. While including confidentiality and non-disclosure language in contracts with vendors helps to protect the FEC's interests, it does not address or provide reasonable assurance that the vendor can adequately protect FEC PII.

The FEC plans to conduct a review of a random sample of agency contracts every two years, as required by Circular A-130 (1) section (m):

> *"Review every two years a random sample of agency contracts that provide for the maintenance of a system of records on behalf of the agency to accomplish an agency function, in order to ensure that the wording of each contract makes the provisions of the Act binding on the contractor and his or her employees. (See 5 U.S.C. 552a(m)(1))"*

As part of this review, the terms and conditions relating to privacy and data protection is also performed. As planned, the biennial review is performed based on a random sample and is not focused on the contracts of vendors who have access to FEC PII. Further, the biennial contract review conducted to satisfy the requirements of OMB Circular A-130 has not been completed on time due to resource constraints in the Office of General Counsel (OGC). The last biennial review of a sample of contracts was completed October 7, 2008.

The purpose of the *FEC Third Party Services Policy*, 58-1.5. is to:

a. *"Satisfy the purposes and policy goals of the Federal Election Commission (FEC) Information System Security Program Policy, Policy Number 58A;*

b. *Establish control over the process of managing to risks associated with use of third parties by the FEC. This policy addresses the requirement to prevent non-FEC users who have been authorized access to FEC electronic information and computing assets from compromising the FEC systems security environment. This policy is enabled by control measures to review and monitor existing contracts and procedures for their effectiveness and compliance with FEC policy, and takes into consideration:*

    i. Third-party service agreements;
    ii. Non-disclosure agreements;
    iii. Legal and regulatory requirements; and
    iv. Service delivery monitoring."

The FEC Privacy Protection Policies and Procedures states:

> *"Co-Chief Privacy Officers/Co-Senior Agency Officials for Privacy are responsible for: ensuring compliance with applicable privacy and data protection laws, regulation and policies."*

A formal risk assessment process inclusive of assessing the risks around FEC PII that has been entrusted to vendors has not been adopted. Resource constraints limit the ability to complete vendor reviews consistently and in a timely manner.

The absence of a comprehensive list of all vendors that handle FEC PII results in the inability to fully assess the privacy related risks these vendors pose to the agency. It may also result in the biennial contract review process being based on a sample of contracts that is selected from an incomplete population of all vendors that handle FEC PII and could result in a false conclusion from the review.

Failure to review the security and privacy controls at vendors prior to sharing FEC PII places the agency at risk for litigation if the information is lost or compromised. If a breach of FEC data held by its vendors occurred, it could result in:

- damage to the individuals whose personal information was disclosed;
- adverse media coverage and embarrassment for the FEC and potential Congressional inquiry;
- financial consequences to address an unauthorized disclosure of information; and
- potential litigation.

Recommendations

We recommend that the FEC:

11a. Should develop and maintain a comprehensive list of all vendors that handle PII.

Further Information

This information could be gathered from each of the Contracting Officer's Technical Representative (COTRs) and the STSI inventory results, after review and update, to get an initial comprehensive list. A form that could be used by COTRs for all new contracts should be developed and implemented to document if the vendor will have access to FEC PII, with a copy of the form provided to the co-Chief Privacy Officers before the contract is signed, so that a risk assessment of the vendor could be performed.

11b. Should develop a policy and supporting procedures to assess and approve vendors with access to FEC PII to reasonably ensure that the vendor has adequate controls in place to protect the information before any PII is provided to the vendor.

Further Information

The policy should include a risk rating system whereby service providers are ranked (e.g., high, medium, low) based on the nature and volume of FEC PII that they will be provided access. The higher the risk rating, the more comprehensive the level of review that should be exercised by the FEC. Approaches to gather information from the vendors and perform a review of the information security and privacy controls can range from the vendor completing a security and privacy questionnaire, an on-site review of the vendor's controls by FEC staff or contractors, or relying on a review of the vendor's controls as performed by a third party (e.g., SAS 70 report). Any reliance on SAS 70 reports provided by the vendor should include a step to ensure that the scope of that work was inclusive and sufficient to cover the systems and processes used to collect, process, transmit or store FEC PII. The "user control considerations" section of any SAS 70

report should also be reviewed by the FEC to ensure that the agency has these controls in place as they are specifically excluded from the vendor's responsibility in the report.

11c. Should formally document the process used to review the FEC's vendors and the results should be retained to evidence the review procedures performed. In addition, there should be documented management approval from the department head that is the source of the information to be shared with the vendor and either of the co-Chief Privacy Officers before the vendor is provided access to FEC PII. There may be more than one department head that should review and approve a specific vendor if the PII affected pertains to more than one department.

Management Response to 11a:

Management concurs: Management agrees it will work with the Contracting Officer to develop a process to maintain a comprehensive list of PII vendors. However, we note that OMB Circular A-130 only requires that a random sample of "Section (m)" contracts be reviewed, and that having a comprehensive list will not necessarily "result in a false conclusion from the review."

Auditor Response:

While only a sample of contracts needs to be reviewed, selection of the sample should be from a complete and accurate list. The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation.

Management Response to 11b:

Management concurs in part: We agree that policies and procedures to assess and approve vendor controls for FEC PII are important, and have already done so by incorporating privacy policies for vendors in the FEC Privacy Protection and Policies and Procedures, FEC Third Party Services Policy 58-1.5, Privacy Rules of Conduct, and the Nondisclosure Agreement for Contractors. We will work with the agency's Contracting Officer and Chief Financial Officer to develop policies and supporting procedures that will require prospective contractors to provide sufficient evidence of internal controls that will safeguard the agency's sensitive information or PII that the contractor has access to. We do not agree that a risk rating system is necessary, and thus decline to implement this part of the recommendation at this time, but will strongly consider it.

Auditor Response:

The agency's planned action is responsive to most of the audit issue identified and when fully implemented, should satisfy the basic intent of the audit recommendation. We look forward to reviewing the details regarding consideration of a risk rating as part of the vendor review process in the corrective action plan.

Management Response to 11c:

Management concurs in part: We agree that the process for reviewing the FEC's vendors for privacy controls should be developed and documented, and will work with the agency's Contracting Officer to accomplish this purpose. Moreover, we agree that there should be some sort of approval before a vendor is provided access to FEC PII; however, we do not believe the division head may be the appropriate person. Instead, we believe that approval by a CPO or their designee would be sufficient. We will consider various options for ensuring that an approval process is implemented, including but not limited

to revising the Nondisclosure Agreement for Contractors to contain an approval statement and a signature block for the approving official.

Auditor Response:

We recognize management's efforts to concur with our recommendation. However, we still believe division head involvement in the vendor approval process is appropriate because they have primary fiduciary responsibility for the information in their respective division. We look forward to reviewing the details of the planned actions in the corrective action plan.

Finding 12: System of Records Notice (SORN) Updates

Controls are not adequate to ensure the FEC Systems of Records (SOR) is updated and published in accordance with the Privacy Act of 1974 and OMB Circular A-130. Since the prior audit report was released on December 7, 2007, the FEC has taken the following steps toward governance and to ensure compliance with OMB Circular A-130, appendix I, and the Privacy Act:

- the FEC published an updated System of Record Notice (SORN) in the Federal Register on January 2, 2008;
- Office of General Counsel (OGC) developed SORNs Review Guidelines February 4, 2009 that detailed the review period between January and June 2009;
- the Privacy Team provided training to FEC managers on the Privacy Act System of Records Notice Review on March 26, 2009;
- the Privacy Team required system managers, using the training provided, to review existing SORs with the goal to amend or revise them for new systems or changes to existing systems, as well as deleting obsolete systems. The deadline established for review, updates and reporting from systems managers was April 20, 2009; and
- the FEC contracted with Solution Technology Systems, Inc. (STSI) to conduct a comprehensive analysis and inventory of PII documents and how they are used throughout the Commission. The inventory and a report of recommendations were provided by the contractor on May 20, 2009.

STSI also provided a *Procedures for Conducting the Circular A-130 Systems of Records Notices Review* general guidance document for conducting the agency's biennial SORNs review. The document provides an eight step sequential process for conducting the biennial review but does not include a timetable for performing the review or monitoring and reporting whether the review was completed timely. During the 2009 SORN review, and consistent with prior biennial review efforts, the agency reviewed its existing SORs, received feedback from system managers[11], analyzed the information received, and prepared a report on revisions necessary to the published SORN. The agency, however, failed to publish an updated SORN. Although the training for system managers and requests to provide feedback on the need to revise and publish new SOR was completed in March and April 2009, the *Privacy Act System of Records Notice Recommendations* memorandum was issued by Privacy Team members on August 31, 2010, well after the planned review period of January to June 2009, and eight months after the January 2010 biennial update deadline had passed.

The *Privacy Act System of Records Notice Recommendations* identified several systems requiring new SORNs: Skillport training database; FEC Systems Access (FSA) database; FORCES Commenter Systems; and Grievance and Arbitration Files. It also identified major and minor revisions required to existing SORs: HSPD-12; Payroll (to reflect WebTA); Garnishments, Grievance and Arbitration files;

[11] The FEC OIG provided updates to SOR 12, Inspector General Investigative Files, to the Privacy Team on April 2, 2009.

and OIG Investigation files. Skillport has been in use by the FEC since November 2006 and WebTA time and attendance system was implemented in November 2008. The FSA system was implemented in December, 2009. Due to the delay in documenting and publishing the SORNs, the FEC is not compliant with OMB A-130, and its own *SORN Review Guidelines,* which states:

> *"Our last SORNs were published in January 2008 – any "major alterations" to the SORNs must be reported to Congress and OMB within 40 days after the operation of the new SOR[12]. Minor changes to a SOR (e.g., system manager name changes) can be grouped into one annual comprehensive publication on the Federal Register without any report to Congress or OMB. Cir. A-130(3)(a)(8) ."*

The process to ensure that the FEC's SOR is updated and published in accordance with the Privacy Act of 1974 and the OMB Circular A-130, Appendix I, is not fully documented or performed to ensure compliance with the Privacy Act and OMB standards.

The *Federal Election Commission Privacy Protection Policies and Procedures* states:

> *"FEC Privacy Officer is responsible for: reviewing (every two years) the FEC System of Records Notices for accuracy and ensuring amended notices are published in the Federal Register. The general public shall be notified of the FEC's systems of records through notice in the Federal Register, in compliance with the Privacy Act. The notice shall include, among other things, the name and location of the system, the purpose of the system, the categories of records maintained in the system and the routine uses of the records. If a routine use needs to be changed or added, modifications will be published in the Federal Register 30 days prior to those changes going into effect, and will allow for interested persons to submit comments."*

Consolidated Appropriations Act of 2005, Section 522 (a) (3) states:

> *"Each agency shall have a Chief Privacy Officer (CPO) to assume primary responsibility for privacy and data protection policy, including 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."*

OMB Circular A-130, Appendix I, *Federal Agency Responsibilities for Maintaining Records about Individuals*, states:

> *Section 5 Publication Requirements: "The Privacy Act requires agencies to publish notices or rules in the Federal Register in the following circumstances: when adopting a new or altered system of records, when adopting a routine use, when adopting an exemption for a system of records, or when proposing to carry out a new or altered matching program."*

[12] OMB defines "major alterations" as: (a) A significant increase in the number, type, or category of individuals about whom records are maintained. For example, a system covering physicians that has been expanded to include other types of health care providers, e.g., nurses, technicians, etc., would require a report. Increases attributable to normal growth should not be reported; (b) A change that expands the types or categories of information maintained. For example, a benefit system which originally included only earned income information that has been expanded to include unearned income information; (c) A change that alters the purpose for which the information is used; (d) A change to equipment configuration (either hardware or software) that creates substantially greater access to the records in the system of records. For example, locating interactive terminals at regional offices for accessing a system formerly accessible only at the headquarters would require a report; (e) The addition of an exemption pursuant to Section (j) or (k) of the Act. Note that, in examining a rulemaking for a Privacy Act exemption as part of a report of a new or altered system of records, OMB will also review the rule under applicable regulatory review procedures and agencies need not make a separate submission for that purpose; (f) The addition of a routine use pursuant to 5 U.S.C. 552a(b)(3). *See* OMB Cir. A-130, App. I.

Section 5.a (2) (a) System Notice: "The system of records notice must appear in the Federal Register before the agency begins to operate the system, e.g., collect and use the information".

Privacy Act of 1974, Section § 552a (e) (4), states:

"Publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records."

During discussion with Privacy Team members responsible for performing the biennial review and publishing the revised SORN, team members indicated that although required changes to the SORN were known, documenting SORs for new systems and amending existing systems was a large task that would take a great deal of time. Members of the FEC Privacy Team stated resource constraints and other priorities as the reason timely SORNs are not published. The Commissioners may not be aware that the agency is not compliant with Federal regulations with respect to SORN publication.

For the period reviewed, the Commission was not in full compliance with the Privacy Act of 1974 and OMB Circular A-130, Appendix I. The public was not made aware of all sensitive information being retained by the Commission. In addition, the public is not informed of the FEC systems that contain PII and given the opportunity to request access and/or changes to their records on a timely basis.

Recommendations

We recommend the FEC Privacy Officer:

12a. Develop a standardized template to allow system managers to accurately document SORs independently of the Privacy Team.

12b. Enhance existing guidelines and procedures to include timelines and deadlines that promote regular review and timely updates to SORs.

12c. Work with ITD management to incorporate SORs assessment processes into systems under development and IT lifecycle management processes.

12d. Work with the Physical Security Officer, the FEC Records Officer, and FEC management to incorporate SORs assessment processes into electronic and paper records management processes.

12e. Develop and implement policies and procedures that define monitoring and reporting processes to ensure SORs are updated and amendments published in accordance with Federal regulations by:

- providing regular training to FEC managers and SOR system owners/managers;
- establish deadlines, based on the legal requirements of OMB A-130, for documenting the new SORs, revisions to existing SORs, and publish the updated SORN;
- providing legal assessment of potential changes in SORs and quality assuring the SORs produced by system owners/managers;
- including performance standards in employee performance plans that are linked to successful compliance with Federal regulations; and
- requiring regular reporting of compliance with the timelines to the Commission.

Management Response to 12a:

Management concurs in part: Management believes that devising a template that can be used to allow system managers to report systems of records is a good idea, and will strongly consider it. However, we

foresee some issues in implementing such a process, namely getting the necessary support for the idea from managers; providing adequate training to system managers on privacy issues; and establishing accountability to ensure that managers complete the template. For that reason, we cannot commit to implementing this recommendation but will strongly consider it.

Auditor Response

At this time management has not committed to implementing this recommendation; however, we look forward to reviewing the details of management's planned approach to addressing this recommendation in the corrective action plan.

Management Response to 12b:

Management concurs: We agree to update the SORNs Review Guidelines and the Procedures for Conducting the Circular A-130 System of Records Notices Review to include internal benchmarks and goals for biennial reviews and updates of SORNs and SORs.

Auditor Response

The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation.

Management Response to 12c:

Management concurs: There are times when a new IT system is developed for a particular purpose that is not already covered by a SORN. For example, a commenter rulemaking system is being developed with the purpose of collecting certain personal information from commenters to Commission proposed rulemakings, and the Commission's storage of that information, and the way that that information is organized in the system (i.e. by the commenter's name), may make it a system of records. Under these circumstances, where a new IT system is being developed that would not be covered by existing SORNs, we agree that a SOR assessment should be done and privacy considerations taken into account.

On the contrary, where IT systems are developed in such a way that they are not system of records (e.g., they store PII but are not organized by a personal identifier), or the information that they hold may already be covered by an existing SORN (e.g., a new system for storing FOIA requests), a SOR assessment is not necessary.

Auditor Response

The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation.

Management Response to 12d:

Management concurs: We agree to work with the Administrative Services and the Commission Secretary's Office to ensure that SORs are considered during records management and physical security operations.

Auditor Response

The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation.

Management Response to 12e:

Management concurs in part: We agree that regular system manager training should take place and are in the process of creating such training. Some system manager training was previously conducted in 2009 in connection with the SORNs review. The deadlines for SORNs review and publication are already prescribed by OMB Circular A-130 and therefore do not need to be established by the agency. However, we will agree to create internal benchmarks or goals to improve our timeliness in this area, consistent with the Circular A-130 deadlines, and subject to staff resources. As evidenced by the August 31, 2010 SORNs Review Memorandum, we agree to continue providing legal assessments of the potential changes in SORs.

We do not concur with the finding that performance standards will need to be revised to include compliance with SORNs deadlines. As mentioned in response to Finding 1b, the CIO and AGC-GLA are explicitly responsible for privacy duties under Directive 65. They, in turn, hold the other Privacy Team members accountable for their privacy responsibilities. Privacy duties are already an inherent part of the team members' performance evaluations.

Finally, Commissioners are annually notified of the agency's privacy progress in several ways, for example: through submission of the 522 Privacy Act Report to Congress to the Commission; and through submission of the FISMA/Privacy Management Report to the Commission's Chair. Moreover, the Commissioners at any time may receive progress updates by the Chief Privacy Officers (CPOs).

Auditor's Response:

We recognize management's efforts to concur with our recommendation. However, we still recommend that compliance with SORN deadlines be explicitly added to performance plans as stated in our auditor response for recommendation 1b.

Finding 13: Training Workstations

While completing the required training as part of the contractor on-boarding process on November 2, 2010, we noted that generic user IDs and passwords were taped to the top of each training station with NT login and Lotus Notes generic login credentials. We noted that workstations had access to a network drive that contained numerous confidential documents, such as: an employee position classification and assessment document; a compilation of informal guidance provided by the Public Financing Audit Advice team in response to diverse legal questions from other Commission Divisions; a large deposition from a matter under review; and other such confidential documents. We also noted during the afterhours walkthroughs that the door to the training room was not locked, thus anyone in the building could have potentially accessed the network files.

The *Federal Election Commission Privacy Protection Policies and Procedures* states:

> *"Systems managers are responsible for overseeing the implementation of administrative, technical, and physical safeguards for the system(s) they manage in order to prevent unauthorized disclosure of personal information.*
>
> *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:*

A. Physical security of both hard copy and electronic data;
B. Personnel security for employee and contractor access to data;
C. Network security for data in transit; and
D. 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."

The generic user IDs and passwords are posted on the workstations to facilitate employee and contractor training. The FEC training instructor was not aware that non-training related materials were accessible on the training workstations. Trainees could access FEC confidential information before completing the privacy and data security training. Employees, contractors or other individuals with physical access to the building could obtain sensitive information by using the generic user IDs and passwords.

Recommendation

We recommend that the FEC:

13. Restrict the training workstations to only be able to access training materials.

Management Response:

Management concurs: The Commission takes serious its responsibility to properly secure sensitive information and will immediately take action to restrict training workstations and student accounts to only training materials.

Auditor Response:

The agency's planned action is responsive to the audit issue identified and when fully implemented, should satisfy the intent of the audit recommendation.

ATTACHMENT 1
COVER MEMO TO MANAGEMENT RESPONSES

Cover Memo to Management Responses to the Cherry Bekaert & Holland LLP 2010 Follow-up Audit of Privacy and Data Protection Report

March 16, 2011

MEMORANDUM

TO: Lynne McFarland
Inspector General

Jonathan Hatfield
Deputy Inspector General

FROM: Alec Palmer
Acting Staff Director
Chief Information Officer
Co-Chief Privacy Officer

Lawrence L. Calvert
Associate General Counsel for General Law and Advice
Co-Chief Privacy Officer

SUBJECT: Management Responses to the 2010 Follow-Up of the 2007 Performance Audit of Privacy and Data Protection Report

We appreciate the opportunity to respond to the 2010 Follow-Up of the 2007 Performance Audit of Privacy and Data Protection Report, 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.

Since 2007, the agency has gone through great lengths to improve its privacy program. In 2008, the agency published its first updated systems of records notice (SORN) in thirteen years, and issued multiple privacy policies and procedures based on the 2007 audit findings. Since 2008, the agency has completed several OMB Circular A-130 mandated reviews, including: two Section (m) contract reviews, a comprehensive SORNs review, and a privacy training review. Additionally, since 2008, the agency has conducted annual privacy and security awareness training for both contractors and employees. In 2010 that training was revised to incorporate test questions aimed at ensuring employees understood their privacy duties. The agency is also in the midst of developing office-specific privacy training. In 2009, the agency developed a comprehensive inventory of its Personally Identifiable Information (PII), and as a part of that project created draft procedures for updating the inventory. In 2010, the agency completed Phase 1 of its plan to eliminate unnecessary social security number (SSN) use, and created a report of recommendations for the Chief Privacy Officers to consider. Additionally, the agency has conducted

reviews of its SSN use and is in the midst of completing its report on the PII Review findings. Finally, the agency has annually published its Privacy Management Report to OMB and its Privacy Act Report to Congress, has updated its website to include Privacy Act complaint and contact information, and is developing a privacy intranet page. We believe that these accomplishments show the Commission's commitment to privacy and our desire to improve our data protection practices.

It is also because of these accomplishments that we must respectfully disagree with the auditors' characterizations of management's response to the 2007 performance audit findings. The 2010 findings summary chart characterizes most of the recommendations as "repeat finding[s]" from the 2007 performance audit. This characterization is also found in the executive summary, where it states that "[s]ixteen (16) of nineteen (19) previous recommendations are still open…." These are not accurate characterizations. The majority of the findings from the 2007 report were in fact addressed and closed; the findings in the 2010 report are, as one might expect from a follow-up audit, follow-up findings which appear to be aimed at addressing actions that need to be taken to maintain or improve upon the actions taken in response to the 2007 audit. We disagree with the characterization of these findings as "repeat findings" to the extent that label is intended to imply that the 2007 report findings were ignored or never addressed. None of the 2007 findings were ignored, and all but the two with which management disagreed at that time were addressed. For example, the 2007 report found that "a comprehensive inventory of personally identifiable information has not been documented." As a result of this finding, in 2009 the agency created a documented comprehensive inventory of its PII. The current audit finds that "a current PII inventory is not maintained." While we acknowledge below the need to maintain and expand on our efforts in this area, we reject any implication that the previous finding was not acted on.

Privacy and data protection is a work always in progress. We always welcome recommendations for improvement in our program, and indeed we believe that under the standards of this audit for "repeat" or "open" findings there will as a result be findings in future audits that always remain "open." We simply wish to make it clear that, except for the findings from 2007 on which management disagreed with the findings and recommendations, we acted on all of those findings.

We also disagree with the characterization in the Executive Summary that the other duties of the co-CPOs and the other members of the privacy team leads to the spending of "minimal" time on privacy duties. None of the accomplishments described above could have occurred as the result of a "minimal" investment of time. We do agree that at any given moment, privacy related functions may have a greater or lesser amount of resources devoted to them depending on their priority relative to other demands on the agency.

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 believe we have accomplished a good deal with our Privacy Program, given its relative youth and the budgetary and human resource limitations that we face as a small agency of fewer than 400 employees.

ATTACHMENT 2
Status of 2006 and 2007 Privacy Findings and Recommendations
PRIVACY AND DATA PROTECTION FOLLOW-UP AUDIT

OIG 2006 Inspection Report on Personally Identifiable Information

Finding	Recommendation	Auditor verified Status December 2007	2010 Follow-up Audit Status and Link to Report Findings
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. Completed in 2009	Open (Modified repeat finding) Refer to Finding 5. *Current Risk Assessments of Systems Containing PII Are Not Performed* on page 26.
	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 Cisco 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. The NAC has not been implemented, however we have implemented policies and procedures to prevent access from non-encrypted laptops either locally or remotely.	Open (Repeat finding) Refer to Finding 6. *Mobile Computing Policy, Device Encryption and Controls* on page 28.

OIG 2006 Inspection Report on Personally Identifiable Information			
Finding	**Recommendation**	**Auditor verified Status December 2007**	**2010 Follow-up Audit Status and Link to Report Findings**
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 Commission 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. Laptop and Blackberry data transmissions are encrypted at the server level.	Open (Repeat finding) Refer to Finding 6. *Mobile Computing Policy, Device Encryption and Controls* on page 28.
Implement protections for remote access to personally identifiable information	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.	Open (Repeat finding) Refer to Finding 10. *Protections for Remote Access to PII* on page 52.

OIG 2006 Inspection Report on Personally Identifiable Information

Finding	Recommendation	Auditor verified Status December 2007	2010 Follow-up Audit Status and Link to Report Findings
	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. The 30 minute timeout is set at the server level, so even if the user changed it, it would change back.	Closed
Additional Agency Requirements	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.	Open (Repeat finding) Refer to Finding 9. *Logging* on page 49.

OIG 07-02 Performance Audit of Privacy and Data Protection

Finding	Recommendation	Management Status May 2010	2010 Follow-up Audit Testing NFR
1. A Comprehensive Inventory of Personally Identifiable Information Has Not Been Documented	1a. Conduct a comprehensive review to identify and document all PII collected, processed, and stored within the FEC.	Complete April 2009	Closed. An inventory of FEC PII was prepared by contractor STSI (dated May 2009). Modified repeat finding concept of inventory prepared but not maintained is included Finding 4. *A Current PII Inventory is not Maintained* on page 22.

OIG 07-02 Performance Audit of Privacy and Data Protection

Finding	Recommendation	Management Status May 2010	2010 Follow-up Audit Testing NFR
	1b. Develop, document, and implement procedures for periodically updating the FEC's inventory of PII.	The FEC conducted a PII review in 2009 and procedures for periodically updating PII are in development	Open (Repeat finding) Refer Finding 4. *A Current PII Inventory is not Maintained* on page 22.
2. Safeguards Over Sensitive Personally Identifiable Information Need Improvement	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.	Completed April 2009	Open (Repeat finding) Refer to Finding 7. *Safeguards Over Sensitive Agency Information and PII Need Improvement* on page 37 and Finding 12. *System of Records Notice* (*SORN) Updates* on page 57.
	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.	Completed April 2009	Open (Repeat finding) Refer to Finding 11. *Vendor Due Diligence* on page 54.
3. Privacy Policies and Procedures Have Not Been Approved and Implemented	3. Finalize, approve, and fully implement privacy policies, procedures, and directives in accordance with Federal laws and regulations.	Completed	Open (Modified repeat finding) Refer to Finding 8. *Lack of Detailed Procedures and Periodic Review* on page 45.
4. Privacy Roles and Responsibilities Are Not Adequately Documented	4a. Consider identifying one individual (position), such as the FEC Staff Director, as Chief Privacy Officer.	Management disagrees with Finding 4 and does not feel bound to comply with these Recommendations. In our response to the Finding, we agreed that "To the extent this Finding is about the specificity of the	Open (Repeat finding) Refer to Finding 1. *Privacy Roles and Accountability* on page 14.

OIG 07-02 Performance Audit of Privacy and Data Protection

Finding	Recommendation	Management Status May 2010	2010 Follow-up Audit Testing NFR
	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.	assignment of other responsibilities in the draft [Privacy] document [or document(s)], we will, of course, carefully consider the recommendations."	Open (Repeat finding) Refer Finding 1. *Privacy Roles and Accountability* on page 14.
	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.	Completed	Closed. The concept on training *effectiveness* is included in the Finding 7. *Safeguards Over Sensitive Agency Information and PII Need Improvement* on page 37.
6. Privacy Impact Assessments Have Not Been Conducted	6a. Identify and implement a governance framework to ensure that controls within the FEC are appropriately identified, documented, and implemented.	Management disagrees with Finding 6 and does not feel bound to comply with these Recommendations. In our response to the Finding, we agreed to "carefully consider the recommendation regarding PIAs," and with regard to the governance framework, stated that "management will need to obtain more	Open (Repeat finding) Refer Finding 2. *Privacy Impact Assessments Have Not Been Conducted* on page 17.

OIG 07-02 Performance Audit of Privacy and Data Protection			
Finding	**Recommendation**	**Management Status May 2010**	**2010 Follow-up Audit Testing NFR**
	6b. Conduct privacy impact assessments in accordance with Section 522.	information" and that the recommendation "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."	Open (Repeat finding) Refer Finding 2. *Privacy Impact Assessments Have Not Been Conducted* on page 17.
	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.		Open (Repeat finding) Refer Finding 3. *Monitoring and Review of Regulatory Requirements* on page 20.
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.	Completed July 2008	Open (Repeat finding) Refer Finding 7. *Safeguards Over Sensitive Agency Information and PII Need Improvement* on page 37. Open (New finding) Refer Finding 13. *Training Workstations* on page 61.
Additional Follow-up Verification Item			
Finding	**Recommendation**	**Management Status August 2010**	**Follow-up Audit Testing NFR**
Controls are not adequate to ensure the Federal Election Commission's (FEC) System of Records (SOR) is updated	Develop, document, and implement procedures for periodically updating the FEC's inventory of PII (recommendation 1b of main report).	In addition to reviewing and publishing the SORNs, many of the remaining concerns raised in this finding and the recommendations have already been addressed. The FEC has finalized and implemented procedures for periodically	Open (Repeat finding) Refer Finding 12. *System of Records Notice (SORN) Updates* on page 57.

OIG 07-02 Performance Audit of Privacy and Data Protection

Finding	Recommendation	Management Status May 2010	2010 Follow-up Audit Testing NFR
and published in accordance with the Privacy Act of 1974 and the Office of Management and Budget (OMB) Circular A-130 Appendix I.	Finalize, approve, and fully implement privacy policies, procedures, and directives in accordance with Federal laws and regulations (recommendation 3 of main report).	updating the FEC's inventory of personally identifiable information (in connection with the biennial review of its systems of records), privacy protection policies, procedures, and directives and has identified Co-Chief Privacy Officers responsible for monitoring compliance with Federal and FEC privacy requirements.	Open (Repeat finding) Refer Finding 12. *System of Records Notice* (*SORN) Updates* on page 57.
	Identify, document, and assign roles and responsibilities for monitoring compliance with Federal and FEC privacy requirements (recommendation 4c of main report)		

ATTACHMENT 3
DEFINITIONS

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): is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

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.

Federal Register

Vol. 75, No. 216 Tuesday,

November 9, 2010

Presidential Documents

Executive Order 13556 of November 4, 2010

Title 3— The

President

Controlled Unclassified Information

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Purpose.* This order establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.

At present, executive departments and agencies (agencies) employ ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing. The fact that these agency-specific policies are often hidden from public view has only aggravated these issues.

To address these problems, this order establishes a program for managing this information, hereinafter described as Controlled Unclassified Information, that emphasizes the openness and uniformity of Government-wide practice.

Sec. 2. *Controlled Unclassified Information (CUI).*

(a) The CUI categories and subcategories shall serve as exclusive designations for identifying unclassified information throughout the executive branch that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.

(b) The mere fact that information is designated as CUI shall not have a bearing on determinations pursuant to any law requiring the disclosure of information or permitting disclosure as a matter of discretion, including disclosures to the legislative or judicial branches.

(c) The National Archives and Records Administration shall serve as the Executive Agent to implement this order and oversee agency actions to ensure compliance with this order.

Sec. 3. *Review of Current Designations.*

(a) Each agency head shall, within 180 days of the date of this order:

(1) review all categories, subcategories, and markings used by the agency to designate unclassified information for safeguarding or dissemination controls; and

(2) submit to the Executive Agent a catalogue of proposed categories and subcategories of CUI, and proposed associated markings for information designated as CUI under section 2(a) of this order. This submission shall provide definitions for each proposed category and subcategory and identify the basis in law, regulation, or Government-wide policy for safeguarding or dissemination controls.

(b) If there is significant doubt about whether information should be designated as CUI, it shall not be so designated.

Sec. 4. *Development of CUI Categories and Policies.*

(a) On the basis of the submissions under section 3 of this order or future proposals, and in consultation with affected agencies, the Executive Agent shall, in a timely manner, approve categories and subcategories of CUI and associated markings to be applied uniformly throughout the executive branch and to become effective upon publication in the registry established under subsection (d) of this section. No unclassified information meeting the requirements of section 2(a) of this order shall be disapproved for inclusion as CUI, but the Executive Agent may resolve conflicts among categories and subcategories of CUI to achieve uniformity and may determine the markings to be used.

(b) The Executive Agent, in consultation with affected agencies, shall develop and issue such directives as are necessary to implement this order. Such directives shall be made available to the public and shall provide policies and procedures concerning marking, safeguarding, dissemination, and decontrol of CUI that, to the extent practicable and permitted by law, regulation, and Government-wide policies, shall remain consistent across categories and subcategories of CUI and throughout the executive branch. In developing such directives, appropriate consideration should be given to the report of the interagency Task Force on Controlled Unclassified Information published in August 2009. The Executive Agent shall issue initial directives for the implementation of this order within 180 days of the date of this order.

(c) The Executive Agent shall convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

(d) Within 1 year of the date of this order, the Executive Agent shall establish and maintain a public CUI registry reflecting authorized CUI categories and subcategories, associated markings, and applicable safeguarding, dissemination, and decontrol procedures.

(e) If the Executive Agent and an agency cannot reach agreement on an issue related to the implementation of this order, that issue may be appealed to the President through the Director of the Office of Management and Budget.

(f) In performing its functions under this order, the Executive Agent, in accordance with applicable law, shall consult with representatives of the public and State, local, tribal, and private sector partners on matters related to approving categories and subcategories of CUI and developing implementing directives issued by the Executive Agent pursuant to this order.

Sec. 5. *Implementation.*

(a) Within 180 days of the issuance of initial policies and procedures by the Executive Agent in accordance with section 4(b) of this order, each agency that originates or handles CUI shall provide the Executive Agent with a proposed plan for compliance with the requirements of this order, including the establishment of interim target dates.

(b) After a review of agency plans, and in consultation with affected agencies and the Office of Management and Budget, the Executive Agent shall establish deadlines for phased implementation by agencies.

(c) In each of the first 5 years following the date of this order and biennially thereafter, the Executive Agent shall publish a report on the status of agency implementation of this order.

Sec. 6. *General Provisions.*

(a) This order shall be implemented in a manner consistent with:

(1) applicable law, including protections of confidentiality and privacy rights;

(2) the statutory authority of the heads of agencies, including authorities related to the protection of information provided by the private sector to the Federal Government; and

(3) applicable Government-wide standards and guidelines issued by the National Institute of Standards and Technology, and applicable policies established by the Office of Management and Budget.

(b) The Director of National Intelligence (Director), with respect to the Intelligence Community and after consultation with the heads of affected agencies, may issue such policy directives and guidelines as the Director deems necessary to implement this order with respect to intelligence and intelligence-related information. Procedures or other guidance issued by Intelligence Community element heads shall be in accordance with such policy directives or guidelines issued by the Director. Any such policy directives or guidelines issued by the Director shall be in accordance with this order and directives issued by the Executive Agent.

(c) This order shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, and legislative proposals.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(e) This order shall be implemented subject to the availability of appropriations.

(f) The Attorney General, upon request by the head of an agency or the Executive Agent, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(g) The Presidential Memorandum of May 7, 2008, entitled "Designation and Sharing of Controlled Unclassified Information (CUI)" is hereby rescinded.

THE WHITE HOUSE,
November 4, 2010.

[FR Doc. 2010–28360 Filed 11–8–10; 8:45 am] Billing code 3195–W1–P

Federal Election Commission
Office of Inspector General

Fraud Hotline
202-694-1015

or toll free at 1-800-424-9530 (press 0; then dial 1015)
Fax us at 202-501-8134 or e-mail us at oig@fec.gov
Visit or write to us at 999 E Street, N.W., Suite 940, Washington DC 20463

Individuals including FEC and FEC contractor employees are encouraged to alert the OIG to fraud, waste, abuse, and mismanagement of agency programs and operations. Individuals who contact the OIG can remain anonymous. However, persons who report allegations are encouraged to provide their contact information in the event additional questions arise as the OIG evaluates the allegations. Allegations with limited details or merit may be held in abeyance until further specific details are reported or obtained. Pursuant to the Inspector General Act of 1978, as amended, the Inspector General will not disclose the identity of an individual who provides information without the consent of that individual, unless the Inspector General determines that such disclosure is unavoidable during the course of an investigation. To learn more about the OIG, visit our Website at: http://www.fec.gov/fecig/fecig.shtml

Together we can make a difference.