



# governmentattic.org

*"Rummaging in the government's attic"*

Description of document: All letter correspondence at the Federal Election Commission (FEC) to or from the Government Accountability Office (GAO), 2014-2017

Requested date: 13-March-2017

Released date: 19-April-2017

Posted date: 14-August-2017

Source of document: Federal Election Commission  
Attn: FOIA Requester Service Center  
Room 408  
999 E Street, NW  
Washington, DC 20463  
Fax: (202) 219-1043  
Email: [FOIA@fec.gov](mailto:FOIA@fec.gov)

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

From: FOIA <FOIA@fec.gov>  
Sent: Thu, Apr 20, 2017 9:32 am  
Subject: RE: Your Freedom of Information Act Request to the Federal Election Commission, FOIA 2017-066

Our response got kicked back. I believe that this reduced size version (nothing has been changed in the responsive documents) should get through to you.

Thanks,  
Robert

From: FOIA  
Sent: Wednesday, April 19, 2017 6:05 PM  
Subject: Your Freedom of Information Act Request to the Federal Election Commission, FOIA 2017-066

VIA ELECTRONIC MAIL

Re: Your Freedom of Information Act Request to the Federal Election Commission, FOIA 2017-066

This email is in response to your request for information under the Freedom of Information Act (FOIA) dated March 13, 2017, and received March 14, 2017 by the Federal Election Commission's (FEC) FOIA Requester Service Center. Specifically, you requested: A copy of all letter correspondence at the Federal Election Commission TO or FROM the Government Accountability Office (GAO) during calendar years 2014, 2015, 2016 and 2017 to date.

On April 10, 2017, in accordance with 5 U.S.C. § 552(a)(6)(B)(i) and 11 C.F.R. § 4.7(c), we extended the processing period to respond to your request by an additional ten (10) working days. This extension was necessary because your request required consultation with two or more components of the Commission which have a substantial subject matter interest in the request. 11 C.F.R. § 4.7(c)(3).

We have searched the Agency's records and located documents responsive to your request (attached). We are releasing all of responsive records we located without redaction; accordingly, your FOIA request has been granted in full.

You may contact our FOIA Public Liaison, Kate Higginbotham, at (202) 694-1650 for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi

Road-OGIS, College Park, Maryland 20740-6001, e-mail at [ogis@nara.gov](mailto:ogis@nara.gov); telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

If you are not satisfied with the response to this request, you may administratively appeal by writing to the Chief FOIA Officer, Federal Election Commission, 999 E Street, N.W., Washington, DC 20463, or sending an e-mail to [foia@fec.gov](mailto:foia@fec.gov). Any such appeal should follow the guidelines set forth in the Commission's FOIA regulations at 11 C.F.R. § 4.8. Thank you for contacting the FEC.

Sincerely,

Robert M. Kahn  
FOIA Requester Service Center

-----  
Robert M. Kahn  
Attorney  
OGC - Administrative Law  
Federal Election Commission

This email may contain attorney-client privileged or confidential information and is for the sole use of the intended recipient(s). If this email has been received in error, please notify the sender immediately at (202) 694-1650, or by reply email, and delete the message without copying or disclosing its contents. Thank you.



U.S. GOVERNMENT ACCOUNTABILITY OFFICE

---

441 G St. N.W.  
Washington, DC 20548

October 19, 2015

Alec Palmer  
Staff Director  
Federal Election Commission  
999 E Street, NW  
Washington, DC 20463

Dear Mr. Palmer,

This letter is to inform you of a new U.S. Government Accountability Office engagement on a review of Federal Digital Service Improvement Programs, code 100216. There are two enclosures. Enclosure I provides information on the engagement. Enclosure II provides a list of GAO's initial questions and requests.

We would appreciate your notifying the appropriate officials of this work. As indicated in the enclosure I of this letter, due to the scope of this government-wide review, we are not planning on holding a formal entrance conference with your agency unless requested by your staff.

Sincerely yours,

A handwritten signature in black ink that reads "Rebecca Gambler". The signature is written in a cursive, flowing style.

Rebecca Gambler, Director  
Homeland Security and Justice

Cc: Mr. Duane Pugh

## ENCLOSURE I

### Information on New Engagement

Engagement subject: Review of Federal Digital Service Improvement Programs

Engagement code: 100216

Source for the work: GAO is beginning this work in response to a request made by the Chairman of the Senate Committee on Homeland Security and Governmental Affairs and the Chairman of the House Committee on Oversight and Government Reform.

Issue(s) under review/Objective(s)/Key question(s): This review will focus on the following objectives

- 1) Describe and assess U.S. Digital Service (USDS) and 18F programs' efforts to improve IT projects.
- 2) Determine the extent to which USDS and 18F engage in overlapping activities.
- 3) Describe and assess agency plans to establish digital service teams.

Agencies and anticipated locations (HQ and field) to be notified: We have included a set of questions and document requests to be provided by the Federal Election Commission staff with the responsibility for managing (1) projects that USDS and/or 18F are involved in, and (2) the agency's digital service team. We also plan to send a short web-based survey to the Federal Election Commission managers of the projects that USDS and/or 18F are involved with. The survey will focus on satisfaction with services provided by USDS and/or 18F.

Other departments/agencies to be contacted: This is a government-wide review.

Estimated start date for the work: We are beginning work as soon as possible and would like to obtain the requested responses and documentation no later than close of business on November 6, 2015.

Time frame for holding the entrance conference: Although we held a formal entrance conference with the Office of Management and Budget and the General Services Administration, due to the scope of this government-wide review, we are not planning on holding a formal entrance conference with your agency unless requested by your staff.

GAO Team(s) performing the engagement: Information Technology

GAO contacts:

- David Powner, Director, 202-512-9286 [pownerd@gao.gov](mailto:pownerd@gao.gov)
- Nick Marinos, Assistant Director, 202-512-9342, [marinosn@gao.gov](mailto:marinosn@gao.gov)
- Kaelin Kuhn, Analyst-In-Charge, 202-512-4789, [kuhnkp@gao.gov](mailto:kuhnkp@gao.gov)

## ENCLOSURE II

### **GAO Questions and Document Request**

Please provide written responses to these questions and the requested documentation by November 6, 2015. GAO point of contact for delivery of requested information: Kaelin Kuhn, 202-512-4789, [kuhnkp@gao.gov](mailto:kuhnkp@gao.gov).

### **U.S. Digital Service (USDS) and 18F Projects**

1. Based on documentation received from the General Services Administration (GSA) and the Office of Management and Budget (OMB), 18F is working with you on the OpenFEC project and USDS is not working with you on any projects. Please confirm that this information is accurate and, if applicable, please identify any projects not listed above that USDS and/or 18F is working on with you.
2. For each of the projects that 18F are involved with, please
  - a. provide a brief description of the project;
  - b. provide contact information for your agency's project manager;
  - c. provide the associated unique investment identifier number (used for reporting to OMB) for the relevant IT investment; and
  - d. describe (1) the services that 18F provided (e.g., web site design, RFP consultation) (2) what 18F have delivered, and (3) any other outcomes associated with 18F's involvement in these projects (e.g., cost savings/increases, improved/degraded performance).
3. GSA provided us with an interagency agreement for the OpenFEC project. Please describe the extent to which the Chief Information Officer (CIO) or his/her designee approved this agreement and provide any relevant documentation of approval.

### **Agency Digital Service Team**

1. Based on documentation received from the Office of Management and Budget (OMB), it appears that OMB instructed the Chief Financial Officer Act agencies to establish digital services teams. Please confirm that your agency does not have any plans to establish a digital service team.



U.S. GOVERNMENT ACCOUNTABILITY OFFICE

---

441 G St. N.W.  
Washington, DC 20548

February 1, 2016

Alec Palmer  
Staff Director  
Federal Election Commission  
999 E Street, NW  
Washington, D.C. 20463

Dear Mr. Palmer,

This letter is to inform you of a new U.S. Government Accountability Office engagement to review Freedom of Information Act litigation costs. This work will be conducted under GAO engagement code 100329.

We would appreciate your notifying the appropriate officials of this work and identifying a point for contact for this engagement. If you have any questions regarding this engagement, please contact Anjalique Lawrence, Assistant Director, at 202-512-6308 or [lawrenceAJ@gao.gov](mailto:lawrenceAJ@gao.gov), or Jonathan Wall, IT Analyst, at 202-512-4970 or [walljm@gao.gov](mailto:walljm@gao.gov).

Sincerely yours,

A handwritten signature in black ink that reads "Rebecca Gambler".

Rebecca Gambler, Director  
Homeland Security and Justice

Enclosure

cc:  
Mr. Duane Pugh ([dpugh@fec.gov](mailto:dpugh@fec.gov))

Enclosure

Information on New Engagement

Engagement subject: Freedom of Information Act Litigation Costs

Engagement code: 100329

Source for the work: GAO is beginning this work in response to a request made by the Chairman and Ranking Member of the Senate Committee on the Judiciary.

Objective/Key question:

1. What are the FOIA litigation-related costs incurred by federal agencies for lawsuits in which the complainant prevailed?

Agencies and anticipated locations (HQ and field) to be notified: Within the Federal Election Commission, we anticipate contacting the central FOIA office and Counsel for FOIA issues.

Other departments/agencies to be contacted: This is a government-wide effort. During the course of our work, we plan to contact federal departments and agencies that were defendants in FOIA litigation cases where a decision was rendered during the time period of January 1, 2009 through December 31, 2014. A request for specific information pertaining to the case(s) identified for your agency is included with this enclosure.

Estimated start date for the work: Immediately

Time frame for holding the entrance conference: Immediately

GAO Team(s) performing the engagement: Information Technology

GAO contacts:

Valerie Melvin, Director, 202-512-6304 and [melvinv@gao.gov](mailto:melvinv@gao.gov)

Anjalique Lawrence, Assistant Director, 202-512-6308 and [lawrenceaj@gao.gov](mailto:lawrenceaj@gao.gov)

Eric Trout, Analyst-in-Charge, 202-512-4970 and [troute@gao.gov](mailto:troute@gao.gov)

Jonathan Wall, IT Analyst, 202-512-2966 and [walljm@gao.gov](mailto:walljm@gao.gov)



### Information Requested

For the FOIA litigation case(s) identified for your agency in the table below, please provide the following information:

1. The number of hours charged by each employee (i.e., Attorney, administrative assistant, FOIA staff) assigned to work on the case.
2. The annual salary for each employee (i.e., Attorney, administrative assistant, FOIA staff) that worked on the case.
3. An explanation as to whether the case was or was not exclusively related to FOIA.
4. The amount of litigation overhead and any other FOIA litigation-related expenses associated with the case.
5. The total amount of judgement paid, including date paid, if applicable.

<b>FOIA Case Number</b>	<b>Case Name</b>	<b>District</b>
11-00951	Citizens for Responsibility and Ethics in Washington v. Federal Election Commission	D.D.C.



FEDERAL ELECTION COMMISSION  
WASHINGTON, D.C. 20463

February 12, 2016

Ms. Valerie Melvin  
Director, Information Management  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Re: Freedom of Information Act Litigation Costs  
Engagement Code: 100329

Dear Ms. Melvin:

This letter responds to a U.S. Government Accountability Office's (GAO's) engagement on a review of Freedom of Information Act Litigation Costs, as described in the February 1, 2016, letter from Rebecca Gambler, Director, Homeland Security and Justice, GAO, which requested written responses to several questions and document requests.

The attached document was prepared by the FEC's Office of General Counsel. It presents GAO's questions in italics, followed by the FEC's response.

We trust that the information provided in this letter will be helpful to the GAO in this engagement. If you have any questions about the information provided in this response, please contact us again.

Sincerely,

David  
Palmer

Digitally signed by David Palmer  
DN: c=US, o=U.S. Government,  
ou=FEC, cn=David Palmer  
Date: 2016.02.12 10:03:52 -05'00'

Alec Palmer  
Staff Director  
Chief Information Officer

cc: Rebecca Gambler, Director, GAO  
Anjalique Lawrence, Assistant Director, GAO  
Eric Trout, Analyst-in-Charge, GAO  
Jonathan Wall, IT Analyst, GAO  
David Carrasquillo, GAO  
Andrew W. Bannister, IT Analyst, GAO



FEDERAL ELECTION COMMISSION  
WASHINGTON, D.C. 20463

November 6, 2015

Via e-mail

Mr. Kaelin P. Kuhn  
Analyst-in-Charge  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Re: Review of Federal Digital Service Improvement Programs  
Engagement Code: 100216

Dear Mr. Kuhn:

This letter responds to a U.S. Government Accountability Office's (GAO's) engagement on a review of Federal Digital Service Improvement Programs, as described in the October 19, 2015 letter from Rebecca Gambler, Director, Homeland Security and Justice, GAO, which requested written responses to several questions and document requests. Presented in italics below are GAO's questions and requests, followed by the FEC's response.

U.S. Digital Service (USDS) and 18F Projects

- 1. Based on documentation received from the General Services Administration (GSA) and the Office of Management and Budget (OMB), 18F is working with you on the OpenFEC project and USDS is not working with you on any projects. Please confirm that this information is accurate and, if applicable, please identify any projects not listed above that USDS and/or 18F is working on with you.*

**FEC Response:**

In partnership with 18F, the FEC is undertaking OpenFEC, an extensive effort to redesign the FEC's website and make FEC campaign finance data as well as legal and compliance information more accessible to the public. The FEC is not working with 18F on any other projects, and it is not working with USDS on any projects.

2. *For each of the projects that 18F are involved with, please*  
a. *Provide a brief description of the project;*

**FEC Response:**

In partnership with 18F, the FEC is developing an agile, navigable, user-based online platform to deliver campaign finance information to a diverse base of users. Once complete, the redesigned FEC website will better meet the needs of an audience that spans from individual citizens seeking information about federal candidates to journalists and researchers who specialize in campaign finance issues, to filers and other political participants seeking legal guidance and compliance information. The FEC provides the public with a wealth of complex information, including current and historical campaign finance data, detailed information regarding the requirements of the campaign finance law and legal resources such as advisory opinions issued by the Commission and information on closed enforcement matters. The redesign effort is a multiyear project, which will continue through FY 2017.

- b. *Provide contact information for your agency's project manager;*

**FEC Response:**

The FEC's project manager for OpenFEC is:

Mr. Wei Luo  
Deputy Chief Information Officer, Enterprise Architecture  
Federal Election Commission  
999 E Street, NW  
Washington, DC 20463  
Phone: (202) 694-1249  
Email: wluo@fec.gov

- c. *Provide the associated unique investment identifier number (used for reporting to OMB) for the relevant IT investment;*

**FEC Response:**

The FEC has confirmed with OMB that the FEC is not required to assign a unique investment identifier number for OpenFEC.

- d. *Describe (1) the services that 18F provided (e.g., web site design, RFP consultation).*

**FEC Response:**

18F is providing web site redesign services to the FEC as part of OpenFEC.

*Describe . . . (2) what 18F have delivered.*

**FEC Response:**

18F and the FEC approached the OpenFEC project with an API-first strategy. Decoupling data from its presentation allows agencies to create information once and publish it everywhere. The first publicly available deliverable by the 18F-FEC partnership was the campaign finance API, which was released to the public on July 8, 2015. An API (application programming interface) provides data in a structured, machine readable format that allows any member of the public to easily create customized visualizations and displays of campaign finance information. This first ever FEC API allows for new features and visualizations to be quickly developed based on existing data, either by the FEC or any outside group. The campaign finance API received over 400,000 hits in its first four months.

At the same time, with the help of 18F staff, FEC is migrating its public facing campaign disclosure database to a cloud environment. As discussed in further detail below, hosting the FEC's campaign finance information in the cloud allows for greater performance flexibility—faster, more granular data searches and a greater ability to meet peak usage demands—with the potential to decrease future hosting and infrastructure costs while improving and maintaining the security of the data. Both the campaign finance API and the FEC's newly-released beta site are supported by the cloud-hosted campaign finance database.

On October 29, 2015, the FEC and 18F released beta.fec.gov, which is a functioning prototype of a future Commission website. The prototype includes an interim homepage and an improved campaign finance data interface. To develop this prototype, 18F identified FEC website users and explored their needs; built prototypes based on user research and implemented changes to the prototypes based on user feedback. In the future, these efforts will significantly enhance the public's access to campaign finance data, including new features that are not available on the current FEC website:

- Contribution maps that show the sources of contributions by state for each committee.
- Ability to sort contributions by size, by committee, by employer and by occupation.
- Ability to sort and filter by purpose of disbursement, recipient name and recipient committee.
- Election pages that allow users to compare candidates within a single race according to the size of their contributions and the states from which those contributions were raised.
- A zip code search function that will allow users to easily find their Congressional district and identify all candidates in a particular race.
- A greater level of detail in searching and presenting transaction-level data, including the ability to search and sort disbursements.

The prototype also offers the following features available on the current website, [www.FEC.gov](http://www.FEC.gov):

- Ability to filter and browse receipts and disbursements from 2011 to 2015 and have easy access to committee filings.
- Ability to view images of filings.
- Ability to view transaction-level data.

The prototype website is designed to be viewed on any sized screen, making the site fully mobile responsive, and it reflects the new visual identity style guide 18F developed based on the feedback they received from FEC Commissioners.

*Describe . . . (3) any other outcomes associated with 18F's involvement in these projects (e.g., cost savings/increases, improved/degraded performance).*

**FEC Response:**

The FEC expects a number of positive outcomes from our partnership with 18F, including the strategic benefits highlighted below:

**Consolidation of FEC databases:** Once the Campaign Finance Data section of the new website is completed, work can begin to shut down the infrastructure that supports the campaign finance data section of the current website. Moving the campaign finance database entirely to a cloud environment will allow savings in future years on the costs of server hardware and hosting services while continuing to grow our database.

**Improved System Performance—Cloud Hosting:** A cloud environment provides greater elasticity compared to traditional server hosting which ensures sufficient infrastructure to support peak election-year workload usage for both receiving campaign finance data through the eFiling platform and presenting that data *via* the website.

**IT Security Enhancements—Cloud Hosting:** Hosting data in a cloud environment also provides a platform of security and privacy. The cloud-hosted site meets all National Institute of Standards and Technology (NIST) requirements for IT security and allows the FEC to share the costs and burdens of protecting information and systems.

**IT Security Enhancements—HTTPS:** The new website uses Hypertext Transfer Protocol Secure (HTTPS) authentication to provide bidirectional encryption of communications between a web browser and a website.

**Improved Content Management System:** 18F is implementing an open source CMS for the FEC website to ensure code sharing and modular development in the future. Implementing a robust, open source CMS will help to ensure that the FEC can continue to update and share information on the site using a standardized, reproducible and efficient shared process.

**Ability to Provide Content as Structured Data through APIs:** 18F will help the FEC to create a full library of APIs, giving users direct access to structured data about campaign finance activity, legal resources and other campaign finance information. The API library will make the FEC's information truly open to the public in that it will be easy to customize and use for any interface.

3. *GSA provided us with an interagency agreement for the OpenFEC project. Please describe the extent to which the Chief Information Officer (CIO) or his/her designee approved this agreement and provide any relevant documentation of approval.*

**FEC Response:**

The interagency agreement for the OpenFEC project was signed by Mr. Wei Luo, the FEC's Deputy Chief Information Officer for Enterprise Architecture and project manager for the OpenFEC project. As Staff Director and Chief Information Officer, I am his direct supervisor, and I also recommended approval of the agreement prior to execution. In addition, two Commissioners have served as "executive sponsors" on the OpenFEC project since its inception. The executive sponsors are FEC Chair Ann M. Ravel and Commissioner Lee E. Goodman, who was Chairman in 2014 when OpenFEC commenced.

**Agency Digital Service Team**

4. *Based on documentation received from the Office of Management and Budget (OMB), it appears that OMB instructed the Chief Financial Officer Act agencies to establish digital service teams. Please confirm that your agency does not have any plans to establish a digital service team.*

**FEC Response:**

The FEC is not included among the Chief Financial Officer Act agencies and, thus, is not subject to OMB's instruction to establish a digital services team. The FEC does not at present have any plans to establish an in-house digital service team, as we understand that term. We expect the collaboration with 18F to serve that function through the completion of this project.

---

We trust that the information provided in this letter will be helpful to the GAO in this engagement. If you have any questions about the information provided in this response, please contact us again.

Sincerely,

David Palmer



Digitally signed by David Palmer  
DN: c=US, o=U.S. Government, ou=FEC, cn=David Palmer  
Date: 2015.11.06 12:34:42 -0500

Alec Palmer  
Staff Director  
Chief Information Officer

cc: David Powner, Director, GAO  
Nick Marinos, Assistant Director, GAO



### Federal Election Commission Response

FOIA Case Number	Case Name	District
11-00951	Citizens for Responsibility and Ethics in Washington v. Federal Election Commission	D.D.C.

*1. The number of hours charged by each employee (i.e., Attorney, administrative assistant, FOIA staff) assigned to work on the case.*

Associate General Counsel for Litigation – 75.5 hours  
 Acting Associate General Counsel for Litigation – 140.5 hours  
 Assistant General Counsel – Litigation - 16  
 Acting Assistant General Counsel – Litigation (1) - 361  
 Acting Assistant General Counsel – Litigation (2) - 27  
 Litigation Attorney (1) – 1406 hours  
 Litigation Attorney (2) – 236 hours  
 Litigation Attorney (3) – 20 hours  
 Litigation Attorney (4) – 15 hours  
 Litigation Paralegal (1) – 188.5 hours  
 Litigation Paralegal (2) – 47.5 hours

*2. The annual salary for each employee (i.e., Attorney, administrative assistant, FOIA staff) that worked on the case.*

Associate General Counsel for Litigation – \$159,437  
 Acting Associate General Counsel for Litigation – \$136,134 - \$149,995  
 Assistant General Counsel - Litigation – \$148,510 - \$152,635  
 Acting Assistant General Counsel - Litigation (1) – \$122,744 - \$141,660  
 Acting Assistant General Counsel - Litigation (2) – \$140,259 - \$140,259  
 Litigation Attorney (1) – \$ 119,238 - \$123,970  
 Litigation Attorney (2) – \$136,771 - \$138,136  
 Litigation Attorney (3) – \$129,758  
 Litigation Attorney (4) – \$122,744  
 Litigation Paralegal (1) – \$68,712 - \$73,607  
 Litigation Paralegal (2) – \$81,204 - \$82,019

*3. An explanation as to whether the case was or was not exclusively related to FOIA.*

This case was exclusively related to FOIA.

*4. The amount of litigation overhead and any other FOIA litigation-related expenses associated with the case.*

The FEC had no significant litigation overhead or other FOIA litigation-related expenses associated with this case.

*5. The total amount of judgment paid, including date paid, if applicable.*

Total judgment paid - \$153,758.98 (\$153,258.98 in attorney fees and \$500 in costs)  
 Judgment paid on September 26, 2014.



United States Government Accountability Office  
Washington, DC 20548

---

December 1, 2016

Jeff Sandlass  
Micro Records Company

<b>File:</b>	B-414161	
<b>Protester:</b>	Micro Records Company	
<b>Agency:</b>	Federal Election Commission	
<b>Solicitation No.:</b>	1110623	
<b>Report Due:</b>	12/30/2016	<b>Decision Due:</b> 03/10/2017
<b>GAO Attorney:</b>	Paul N. Wengert	<b>Phone:</b> 202-512-3781
<b>Official Fax:</b>	202-512-9749	<b>Case Status:</b> 202-512-5436

## ACKNOWLEDGMENT OF PROTEST

We have received your protest concerning the referenced procurement. The contracting agency is required to file a report in response to the protest by the Report Due date indicated above. Under our Bid Protest Regulations, 4 C.F.R. § 21.3(i), you are required to submit written comments in response to the report. Written comments must be received in our Office within 10 calendar days of your receipt of the report--otherwise, we will dismiss your protest. For purposes of determining when your response to the agency report must be submitted, we will assume that you received the report by the Report Due date unless you notify us otherwise at that time.

Also, the agency has been advised that if you have filed a request for specific documents, the agency should provide to all parties and GAO, at least 5 days prior to the Report Due date, a list of those documents, or portions of documents, that the agency has released to the protester or intends to produce in the report, and of the documents that the agency intends to withhold and the reasons for the proposed withholding. You are requested to object to the scope of the agency's proposed disclosure or nondisclosure with GAO and the other parties within 2 days of receipt of the list.

Bid protests, and subsequent associated filings, may be filed using the following methods. Our Office hours are 8:30 a.m. until 5:30 p.m. eastern time, Monday through Friday.

- **Facsimile:** When filing with our Office, parties should rely on the use of facsimiles as much as possible. Facsimile transmitted documents are considered filed upon receipt of the entire text of the filing. Correspondence received, and transmissions completed, after our Office hours will be considered filed on the next business day. When filing a document by facsimile, it is not necessary to file a duplicate original. If a duplicate original is provided, please indicate on the face of the duplicate original that it previously has been telecopied. Please refrain from sending voluminous transmissions or lengthy exhibits. These exhibits should be hand delivered, or sent by mail or commercial carrier (e.g., UPS or FedEx).
- **E-mail:** Protest filings may be submitted to [protests@gao.gov](mailto:protests@gao.gov) (see the Legal Products section of our web site, [www.gao.gov](http://www.gao.gov), for more information).
- **Hand Delivery:** ***Please note the following changes for hand-deliveries.***

Effective March 3, 2008, the filing window at GAO's Headquarters Building will no longer accept deliveries. All packages must be delivered to GAO's new mail center located on the 4<sup>th</sup> street side of the GAO building. Anyone attempting to pick up or deliver packages will need to walk up to the door and ring the door bell in order to be let in to the Courier Reception Desk.

The new GAO mail center will accept deliveries for GAO's Bid Protest forum from 7:30 am to 5:30 pm. Packages **MUST** have one of the following labels:

"Procurement Law Control Group,"  
"Bid Protest,"  
"PLCG,"  
"Name of GAO attorney," or  
"Contract Appeals Board"

Packages will be scanned and may be opened and searched. After inspection, packages will be time/date stamped. Senders must leave enough time for timely delivery. Please, be advised that it may take some time for packages to be processed. Timeliness will be measured by the time/date-stamp. GAO employees **will not** meet couriers outside of the GAO building to accept packages. The window closes promptly at 5:30 p.m.; packages cannot be left after that time.

- **Regular Mail or Commercial Carrier (e.g., UPS or FedEx):** Documents transmitted using these methods are considered filed when time/date-stamped at GAO. Regular mail should not be used for time-sensitive filings.

GAO bid protest decisions not subject to protective orders are distributed via the GAO Worldwide Web Internet site ([www.gao.gov](http://www.gao.gov)), and in most cases are available within 1 business day of the decision date. We will provide you or your representative e-mail notice of the availability of the decision on this protest upon issuance if you furnish us the e-mail address.

Please refer to our file number in all future correspondence regarding the protest.

--For the Managing Associate General Counsel



United States Government Accountability Office  
Washington, DC 20548

---

December 1, 2016

Deborah Marks  
Federal Election Commission

<b>File:</b>	B-414161	
<b>Protester:</b>	Micro Records Company	
<b>Agency:</b>	Federal Election Commission	
<b>Solicitation No.:</b>	1110623	
<b>Report Due:</b>	12/30/2016	<b>Decision Due:</b> 03/10/2017
<b>GAO Attorney:</b>	Paul N. Wengert	<b>Phone:</b> 202-512-3781
<b>Official Fax:</b>	202-512-9749	<b>Case Status:</b> 202-512-5436

## CONFIRMATION OF REPORT REQUIREMENT

This confirms our telephonic notice of the protest and report due date indicated above. Please advise us immediately of the individual(s) that will be representing the agency in the protest, including name, address (and Internet e-mail address, if any), and the telephone and fax numbers.

You should notify all intervenors that this protest has been filed and to communicate directly with us in connection with the protest. Copies of the report must be furnished to the protester and all intervenors not later than the date indicated above. Please advise the protester of its obligation to submit comments or request a decision on the existing record within 10 days of its receipt of the agency report. Please also advise all parties of their right to submit comments on the report to GAO within 10 days of its receipt. You should refer to our file number and the GAO attorney assigned in all future correspondence regarding the protest. Any request for dismissal should be filed as soon as practicable after receipt of this notice if the agency seeks resolution of the request by our Office prior to the stated report due date.

For your convenience, following is a list of the type of information to be included in your agency report:

--the contracting officer's statement of the relevant facts;

--a best estimate of the contract value;

--whether a statutory stay or suspension of performance is in place;

--a memorandum of law;

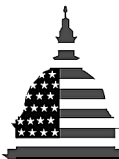
--a copy of all relevant documents, or portions of documents, not previously produced, including, as appropriate, any agency-level protest and decision, the bid or proposal submitted by the protester, the bid or proposal of the firm being considered for award or whose bid or proposal is being protested, all evaluation documents, the solicitation (with specifications), and the abstract of bids or offers; and

--an index identifying the contents of the report and the location of each document or enclosure. Where portions of the report have been redacted for any party (or where the agency has omitted certain documents from a party's report), please indicate which redactions or omissions apply to each party. Agency reports must be organized through the use of pagination, tabs, and binders, as appropriate.

If the protester has filed a request for specific documents, please provide to all parties and GAO, at least 5 days prior to the report due date, a list of those documents, or portions of documents, that you have released to the protester or intend to produce in your report, and of the documents you intend to withhold and the reasons for the withholding.

GAO bid protest decisions not subject to protective orders are distributed via the GAO Worldwide Web Internet site ([www.gao.gov](http://www.gao.gov)), and in most cases are available within 1 business day of the decision date. We will provide you or your representative e-mail notice of the availability of the decision on this protest upon issuance if you furnish us the e-mail address.

--For the Managing Associate General Counsel



G A O

Accountability \* Integrity \* Reliability

Comptroller General  
of the United States

United States Government Accountability Office  
Washington, DC 20548

## Decision

**Matter of:** JOD Enterprises, dba Micro Records Company Inc.

**File:** B-414161

**Date:** January 3, 2017

---

### DECISION

JOD Enterprises, doing business as Micro Records Company Inc., of Baltimore, Maryland, protests the issuance of a purchase order to e-ImageData Corp., of Hartford, Wisconsin, by the Federal Election Commission (FEC) under request for quotations (RFQ) No. 1110623 for image scanning equipment, software, installation, training, and on-site service. Micro Records argues that the FEC improperly issued the order to e-ImageData for equipment that cannot meet the specifications in the RFQ.

We dismiss the protest because the agency is terminating the awardee's contract and resoliciting the procurement. Specifically, in a letter dated December 29, 2016, counsel for the FEC state that the agency will terminate the order, return any items that have been delivered, and issue a new RFQ that accurately reflects the agency's needs.

When an agency terminates an awardee's contract and resolicits for its needs, the agency action renders a protest of that award academic. We do not consider academic protests because to do so would serve no useful public policy purpose. Dyna-Air Eng'g Corp., B-278037, Nov. 7, 1997, 97-2 CPD ¶ 132. We only consider protests against specific procurement actions and will not render to a protester what would be, in effect, an advisory decision. Id.

The protest is dismissed.

Susan A. Poling  
General Counsel

**UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE  
OFFICE OF THE GENERAL COUNSEL  
PROCUREMENT LAW DIVISION  
Washington, D.C. 20548**

**Matter of:** Protest of Micro Records Company, RFQ1110623

**File:** B-414161

**Agency:** Federal Election Commission

**NOTICE OF APPEARANCE**

Robert M. Kahn, Esq. and Steve N. Hajjar, Esq., hereby give notice of their appearance as representatives for the Federal Election Commission ("FEC") in the above-captioned matter. Mr. Kahn and Mr. Hajjar's contact information is provided as follows:

Robert M. Kahn  
Federal Election Commission  
999 E Street, NW  
Washington, D.C. 20463  
(202) 694-1542 (Office)  
(202) 219-3923 (Fax)  
rkahn@fec.gov

Steve N. Hajjar  
Federal Election Commission  
999 E Street, NW  
Washington, D.C. 20463  
(202) 694-1546 (Office)  
(202) 219-3923 (Fax)  
shajjar@fec.gov

Respectfully submitted,  
FEDERAL ELECTION COMMISSION

By: 

Robert M. Kahn, Esq.  
*Counsel for the FEC*

By: 

Steve N. Hajjar, Esq.  
*Counsel for the FEC*

Date: December 15, 2016

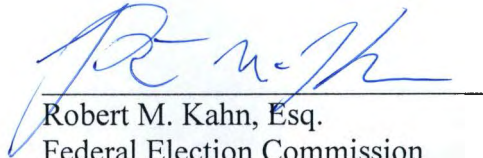


**CERTIFICATE OF SERVICE**

I hereby certify that on this 15th day of December, 2016, I served, via electronic mail, a copy of the foregoing Notice of Appearance upon:

VIA ELECTRONIC MAIL

Jeff Sandlass  
Micro Records Company  
9321D Philadelphia Road  
Baltimore, MD 21237  
410-686-7504  
jeffs@mdmicrographic.com  
*Representative for Micro Records Company*



Robert M. Kahn, Esq.  
Federal Election Commission  
999 E Street, NW  
Washington, D.C. 20463  
(202) 694-1542 (ph)  
(202) 219-3923 (Fax)  
rkahn@fec.gov



U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.  
Washington, DC 20548**Facsimile Transmission Sheet****Date:** December 29, 2016**Number of pages, including this cover sheet:** 2**Re:** B-414161If transmission problems occur, please  
call

202-512-4788.

Our fax number is 202-512-9749.

Protest of Micro Records Company Inc.

**From:** Paul N. Wengert, Attorney; Phone: 202-512-3781

Name	Firm/Agency	Phone	Fax
Jeff Sandlass	Micro Records Company Inc.	410-238-7480	410-238-1600
Steve N. Hajjar, Esq.	Federal Election Commission	202-694-1546	202-219-3923
James Westoby	e-ImageData Corp.	262-673-3476	262-673-3496

**Comments:**

This morning, our Office received a letter from the awardee (but dated December 27) that requests that we dismiss the protest. We are treating the letter as a request to intervene in the protest. As indicated in the accompanying Acknowledgement of Appearance of Intervenor, e-ImageData must send a copy of the letter to the protester's representative also. In the interest of efficiency, the protester may consolidate a response to the letter with a response to the agency's next filing.

The intervenor should direct its request for materials filed in this protest directly to the parties, and the parties should promptly provide the intervenor with protest filings submitted to date.

GAO has not issued protective order in this matter because the protester is not represented by counsel who could seek admission under such an order. So, if any filing contains proprietary or source selection material, a redacted copy (clearly marked as such) must be provided to the opposing party/ies instead. Both the redacted and unredacted documents (both clearly marked) must also be sent to GAO and to counsel for the FEC at the same time. GAO will generally review redactions to ensure that they appear reasonable. GAO can also review redactions if challenged by another party as being unjustified.



United States Government Accountability Office  
Washington, DC 20548

December 29, 2016

James Westoby  
e-ImageData Corp.

File:	B-414161	
Protester:	Micro Records Company Inc.	
Agency:	Federal Election Commission	
Solicitation No.:	1110623	
Report Due:	12/30/2016	Decision Due: 03/10/2017
GAO Attorney:	Paul N. Wengert	Phone: 202-512-3781
Official Fax:	202-512-9749	Case Status: 202-512-5436

#### **ACKNOWLEDGMENT OF APPEARANCE OF INTERVENOR**

This acknowledges receipt of your notice of appearance as an intervenor in connection with the captioned protest. Please note that under 4 C.F.R. § 21.3(a) copies of all correspondence, including a copy of your notice of appearance, must be sent to the protester, the contracting agency and any other intervenor that has entered a notice of appearance in this matter. To date, the following intervenors have also entered an appearance:

**None.**

In the event additional intervenors enter notices of appearance in this matter, they will be instructed to provide you with copies of such notices and you should add their names to the list of parties to receive copies of subsequently submitted correspondence.

--For the Managing Associate General Counsel

#### **FOR FURTHER INFORMATION**

GAO Attorney: Paul N. Wengert; 202-512-3781  
Case Status Calls: 202-512-5436  
FAX Number: 202-512-9749

**UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE  
OFFICE OF THE GENERAL COUNSEL  
PROCUREMENT LAW DIVISION  
Washington, D.C. 20548**

**Matter of:** Protest of Micro Records Company, RFQ1110623

**File:** B-414161

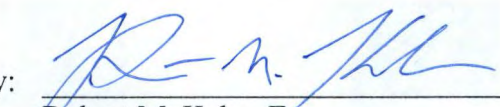
**GAO Attorney:** Paul N. Wengert

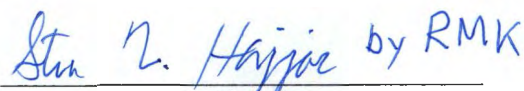
**Agency:** Federal Election Commission

**NOTICE OF CORRECTIVE ACTION**

The Federal Election Commission ("Commission") hereby provides notice that it will take corrective action in this matter. The Commission intends to terminate for convenience all actions consistent with the order that is the subject of this protest, return the purchased items, and issue a revised Request for Quotation with updated evaluation criteria that reflect the Commission's needs. In light of this corrective action, the Commission respectfully asks that it be excused from filing an agency report, or in the alternative, that the deadline for filing the report be extended until January 31, 2017.

Respectfully submitted,  
FEDERAL ELECTION COMMISSION

By:   
Robert M. Kahn, Esq.  
*Counsel for the FEC*

By:  by RMK  
Steve N. Hajjar, Esq.  
*Counsel for the FEC*

Date: December 29, 2016

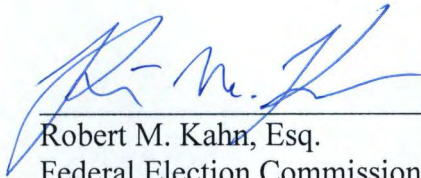
**CERTIFICATE OF SERVICE**

I hereby certify that on this 29th day of December, 2016, I served, via electronic mail, a copy of the foregoing Notice of Appearance upon:

**VIA ELECTRONIC MAIL**

Jeff Sandlass  
Micro Records Company  
9321D Philadelphia Road  
Baltimore, MD 21237  
410-686-7504  
jeffs@mdmicrographic.com  
*Representative for Micro Records Company*

James Westoby  
e-ImageData Corp.  
340 Grant St  
Hartford, WI 53027  
Ph 262-673-3476  
Fx 262-673-3496  
jwestoby@e-imagedata.com  
*Representative for e-ImageData Corp.*

  
Robert M. Kahn, Esq.  
Federal Election Commission  
999 E Street, NW  
Washington, D.C. 20463  
(202) 694-1542 (ph)  
(202) 219-3923 (Fax)  
rkahn@fec.gov

**Robert Kahn**

---

**From:** Robert Kahn  
**Sent:** Wednesday, December 07, 2016 4:07 PM  
**To:** 'fisma@gao.gov'  
**Cc:** Katie Higginbothom  
**Subject:** Federal Election Commission FY 2016 Annual Privacy Management Report  
**Attachments:** FY 2016 FEC Privacy Management Report.pdf

The Honorable Gene L. Dodaro  
Comptroller General of the United States  
Government Accountability Office  
441 G St., NW  
Washington, DC 20548

Dear Comptroller General Dodaro:

Attached please find, in accordance with 44 U.S.C. § 3554, the FY 2016 Annual Privacy Management Report of the Federal Election Commission's Co-Senior Agency Officials for Privacy, as submitted to the Office of Management and Budget.

Respectfully submitted,  
Robert M. Kahn

-----  
Robert M. Kahn  
Attorney  
OGC - Administrative Law  
Federal Election Commission  
(202) 694-1542 (Office)

This email may contain attorney-client privileged or confidential information and is for the sole use of the intended recipient(s). If this email has been received in error, please notify the sender immediately at (202) 694-1650, or by reply email, and delete the message without copying or disclosing its contents. Thank you.



FEDERAL ELECTION COMMISSION  
WASHINGTON, D.C. 20463

November 10, 2016

The Honorable Shaun Donovan  
Director  
Office of Management and Budget  
725 17th Street, NW  
Washington, DC 20503

Dear Director Donovan:

I am transmitting herewith the Annual Privacy Management Report of the Federal Election Commission's Co-Senior Agency Officials for Privacy, Edward W. Holder, Acting Deputy Staff Director, Management and Administration, and Gregory R. Baker, Deputy General Counsel - Administration.

I am advised that because the FEC is not included in the applicable definition of "agency" under the Federal Information Security Management Act (FISMA) or the E-Government Act, the FEC historically has not responded to those parts of OMB's request for an annual report that derive from those statutes, and that the attached report follows that historic practice. Consequently, I am advised, the attached report contains only responses to those questions directed to the Senior Agency Officials for Privacy.

Also appended to this report is the FEC Co-SAOP's progress update on the FEC's plan for eliminating the unnecessary use of social security numbers and its review and reduction of its holdings of personally identifiable information (PII), a memorandum describing the Agency's Privacy Program, a description of the Agency's efforts to comply with the privacy-related requirements in OMB M-16-04 policy, the Agency's written policy for ensuring that any new collection or use of Social Security numbers is necessary, a description of the Agency's efforts to comply with the privacy-related requirements in OMB M-16-04, and a description of the FEC's privacy training for employees and contractors.

The FEC is an independent regulatory commission charged with administering and enforcing federal campaign finance law. In the course of carrying out its responsibilities, the FEC has always taken very seriously the privacy of information it collects and maintains on individuals.

I trust this information is responsive. Should you have any questions, please contact Mr. Holder at (202) 694-1250 or Mr. Baker at (202) 694-1650.

On behalf of the Commission,



Matthew S. Petersen  
Chair

cc: Edward Holder  
Gregory Baker

Enclosure

2016 FEC Privacy Management Report (with attachments)



**FEDERAL ELECTION COMMISSION  
PRIVACY MANAGEMENT REPORT  
FISCAL YEAR 2016**



**PROGRESS UPDATE ON THE  
FEDERAL ELECTION COMMISSION'S  
REVIEW & REDUCTION OF  
PERSONALLY IDENTIFIABLE  
INFORMATION AND THE  
ELIMINATION OF THE  
UNNECESSARY USE OF SOCIAL  
SECURITY NUMBERS**



FEDERAL ELECTION COMMISSION  
Washington, DC 20463

November 10, 2016

The Honorable Shaun Donovan  
Director  
Office of Management and Budget  
725 17th Street, NW  
Washington, DC 20503

Dear Director Donovan:

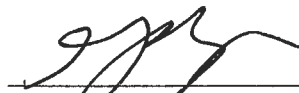
As part of the Fiscal Year 2016 Federal Information Security Management Act (FISMA) and Agency Privacy Management Report, the Office of Management and Budget has requested that agencies submit a progress update on their plans for eliminating the unnecessary use of social security numbers (SSNs) (hereinafter "SSN Reduction Initiative"), and their review and reduction of personally identifiable information (PII) holdings (hereinafter "PII Review Initiative"). The Federal Election Commission's (FEC) plan for eliminating SSNs and reducing its PII holdings has been solidified into one policy document entitled 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" (hereinafter FEC PII Plan). *See* FEC PII Plan, attached hereto as Appendix 1. Because the FEC's plans in this regard have been merged into one policy document, and its efforts for both initiatives are largely intertwined, this report provides a progress update on both initiatives.

In FY 2011, the Commission completed Phase 1 of its SSN Reduction Initiative (the collection and review of the agency's SSN holdings and co-Senior Agency Official for Privacy approval of recommendations for eliminating such holdings) and began Phase 2 of the initiative (collaborate with effected offices to develop feasible alternatives to SSN use). For two years the Privacy Team collected information from each of the Commission's offices and divisions regarding its SSN use. By using data from the Commission's PII inventory, as well as using information gained from interviews with FEC employees in each office, the team was able to determine which offices collected SSNs, the rationale for the collection, and whether there was a valid business justification for the collection. In FY 2012, the Privacy Team continued working with the affected offices to determine how best to address the recommendations, and reduce or diminish their SSN vulnerabilities, and also commenced a review of the Commission's PII holdings, which is following-up on the comprehensive inventory of the agency's PII holdings conducted by STSI during FY 2010.

During FY 2016, the Privacy Team continued to close out and implement items in the *2010 Follow-Up Audit of Privacy and Data Protection Corrective Action Plan* finalized by the Agency's Co-Chief Privacy Officers to address the PII Assessment Report recommendations from the review conducted by STSI. In FY 2017, the Co-Chief Privacy Officers will continue to focus on completing Phase 2 of the PII Plan by again reaching out the heads of all Agency offices and divisions to provide assistance with implementing any outstanding recommendations from the Phase 1 report. The Privacy Team will also continue working with points-of-contact from each Agency office and division to obtain updated PII inventories, so that the Privacy Team can determine what changes to the Agency's PII holdings have occurred since the previous review.

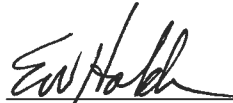
Should you have any questions, please contact the undersigned, Gregory Baker, Deputy General Counsel - Administration and Co-Senior Agency Official for Privacy, at (202) 694-1650, or Edward Holder, Deputy Staff Director, Management and Administration (Acting), and Co-Senior Agency Official for Privacy, at (202) 694-1250.

Sincerely,



---

Gregory R. Baker  
Deputy General Counsel - Administration  
Co-Senior Agency Official for Privacy



---

Edward W. Holder  
Deputy Staff Director, Management and Administration (Acting)  
Co-Senior Agency Official for Privacy

#### Attachments

FY 2016 Progress Update Report



FEDERAL ELECTION COMMISSION  
Washington, DC 20463

## **PROGRESS UPDATE ON THE FEDERAL ELECTION COMMISSION'S REVIEW & REDUCTION OF PERSONALLY IDENTIFIABLE INFORMATION AND THE ELIMINATION OF THE UNNECESSARY USE OF SOCIAL SECURITY NUMBERS (SSNs)**

### **I. Introduction**

In December 2007, the Federal Election Commission ("Commission" or "Agency") issued 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 07-16 (OMB M-07-16), Safeguarding Against and Responding to the Breach of Personally Identifiable Information" [hereinafter "FEC PII Plan"], which outlined the Commission's plans for reducing personally identifiable information (PII) holdings and eliminating the use of social security numbers (SSNs). The FEC PII Plan comprehensively outlines the Agency's goals for reducing, and in some cases eliminating, the Commission's use of PII and SSNs, and also serves as a basic framework for how the Agency will monitor its use of, and properly safeguard, its PII for years to come. This report provides an update on how the Commission has met, or is meeting, the goals outlined in the FEC PII Plan to date.

### **II. Plan to Review and Reduce Holdings of PII**

In determining the best way to safeguard the Agency's PII holdings, and in accordance with OMB M-07-16, the Commission outlined the following steps in the FEC PII Plan for reviewing and reducing its PII holdings:

1. Publish a schedule for periodic review of its holdings on the FEC website;
2. Publish revised Systems of Records Notices (SORNs) to accurately reflect the number of Privacy Act systems of records held by the Agency, the information contained in those systems of records, routine uses for the information by Agency, the system's location and system manager/owner, and other information as required under the Privacy Act;
3. Conduct a biennial review of the Agency's system of records to ensure accuracy of the published SORNs; and

4. Conduct a biennial review of the Agency's overall PII holdings found in all Agency systems (paper and electronic), regardless of whether such PII is in a system of records.

This year, the FEC has continued to make progress on fulfilling many of the goals outlined in the Plan as explained below.

**a) Biennial Review of Agency Systems of Records & Publication of Revised Systems of Records Notices (SORNs)**

In FY 2011, the Privacy Team completed a review of the Agency's systems of records in an effort to publish new and updated SORNs by doing the following:

- Conducting follow-up interviews with FEC managers who reported new systems of records, or changes to existing systems of records, to determine whether new or revised SORNs were needed for those systems.
- Conducting follow-up interviews with various system administrators to determine how the reported systems worked, and whether they were structured in such a way as to make them Privacy Act systems of records.
- Attending presentations whereby system administrators demonstrated how the reported systems worked.
- Identifying new systems requiring SORNs and existing SORNs requiring updates/revisions.

The Privacy Team then drafted SORNs for five new systems at the Agency and revised three existing SORNs to reflect changes in the systems of records. In FYs 2012 and 2013, the Privacy Team completed drafting and revising the SORNs, which were reviewed and approved by the Co-Chief Privacy Officers.

**Next Steps:** The Privacy Team anticipates that the SORNs will be submitted to the Commission for approval in calendar year 2017 and be published shortly thereafter. Simultaneously, the team is also conducting another review of the Agency's systems of records to ensure the accuracy of the FEC's SORNs.

**b) Biennial Review of the Commission's PII Holdings ("PII Review Initiative")**

In FY 2012, the Privacy Team began its review of the Commission's PII holdings following-up on the comprehensive inventory of the agency's PII holdings conducted by STSI during FY 2010. The Privacy Team worked with points-of-contact (POCs) in each office and division in the Agency to obtain updated PII inventories. The Privacy Team provided the POCs with detailed instructions on how to update their inventories and the questionnaire forms, which included their respective office's PII inventories from the STSI review.

In FY 2013, the Privacy Team worked with POCs in various offices and divisions to obtain the outstanding updated PII inventories, which the Team has been reviewing to determine



what changes to the Agency's PII holdings have occurred since the prior PII review was conducted. The Privacy Team also continued working to implement the items in the 2010 Follow-Up Audit of Privacy and Data Protection Corrective Action Plan (CAP) finalized by the Agency's Co-Chief Privacy Officers to address the PII Assessment Report recommendations from the review conducted by STSI. After closing out more than ten corrective action plan recommendations in FY 2015—including using relevant Generally Accepted Privacy Principles (GAPP) to protect PII, encrypting mobile devices, and ensuring that contractors are required to handle PII safely—the Privacy Team corrected and closed out in the last year, three CAP recommendations, including creating a FEC Privacy and Security Communication. Moreover, the Privacy Team provided the Office of the Inspector General access to information that supports the closing of many recommendations. Additionally, the Privacy Team will add language developed by the Office of Government Information Services and the Department of Justice as a new routine use for its Freedom of Information Act/Privacy Act SORN.

**Next Steps:** The Agency's Chief Information Security Officer will be conducting informal risk assessments on the systems containing PII to determine whether there any deficiencies in the systems. Based on the results of these risk assessments the Privacy Team will prepare a report to the Co-Chief Privacy Officers' approval that will propose corrective actions, if necessary, to address any deficiencies discovered through the assessments.

### **III. Plan to Eliminate Unnecessary SSNs**

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 07-16 (OMB M-07-16), Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (hereinafter "FEC PII Plan") outlines three phases for the Agency's elimination of unnecessary SSN use:

1. Phase 1: The FEC's CISO and the Office of General Counsel, Administrative Law Team (OGC-ALT) will collect information from each of the FEC offices to determine which offices collect and use SSNs; the rationale for its collection and use; the SSNs' necessity; and whether alternative identifying information may be used instead of SSNs.
2. Phase 2: The Co-Chief Privacy Officers will work with affected offices to explore alternatives to the collection and use of SSNs.
3. Phase 3: The FEC will implement decisions regarding the collection and use of SSNs and alternative identifiers. The CISO and OGC-ALT will also monitor the impact of the implemented decisions to determine their effectiveness, and to make modifications if necessary. The Co-Chief Privacy Officers will review the Agency's collection and use of SSNs biennially.

To prevent the duplication of efforts for SSN information gathering, the Privacy Team rolled Phase 1 of the SSN Reduction Initiative into the PII Review Initiative. Following the PII Review Initiative, the Privacy Team analyzed the SSN information collected during, and prior to,

the Initiative.<sup>1</sup> Using this information, the Privacy Team produced a “Social Security Numbers (SSNs) Reduction Plan Phase 1 Report Recommendations for Reducing Agency SSN Use.” This report, provided to the Co-Chief Privacy Officers, suggests alternatives for eliminating the unnecessary SSN use found throughout the agency. It signifies the completion of Phase 1 of the Agency’s FEC PII Plan.

Beginning in FY 2013, the Co-Chief Privacy Officers moved forward with Phase 2 of the PII plan by recirculating the Phase 1 report to the heads of each office and division in the Agency and offering support to those offices that need assistance in addressing any unresolved issues concerning the recommendations in the report. Although the Agency’s PII Plan has not yet reached its completion, several FEC Offices have eliminated use of SSNs. For example, the Office of General Counsel regularly instructs employees not to place their SSNs on training forms, even if the training form requests such information, and the responsible staff will not process forms containing such information.

**Next Steps:** The Co-Chief Privacy Officers will continue implementing Phases 2 and 3 of the PII Plan. The Privacy Team will also continue to work with specific agency offices to address any identified SSN handling and/or use weaknesses noted in the Phase 1 Report. The Privacy Team will monitor the impact of those alternatives on work processes to determine their effectiveness and to make adjustments as necessary to promote the goal of reducing and eliminating to the extent feasible, SSN use throughout the agency.

We hope that this information is helpful to you. If you have any questions regarding the contents of this report, please contact Gregory Baker, Deputy General Counsel - Administration and Co-Chief Privacy Officer, at (202) 694-1650, or Edward Holder, Acting Deputy Staff Director, Management and Administration and Co-Chief Privacy Officer, at (202) 694-1250.

---

<sup>1</sup> Prior to the PII Review Initiative, the Privacy Team conducted an initial presentation on the SSN elimination project with support staff from every division and office in the agency. The Team conducted follow-up interviews with the support staff, who acted as points-of-contact in identifying documents containing PII within their respective work units. Information collected during this process was incorporated into the PII Review Initiative.

**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**

**Introduction**

Safeguarding personally identifiable information<sup>1</sup> in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. The Social Security Number (SSN) is a powerful piece of personally identifiable information, which has come to be used for numerous purposes other than those required by law or Social Security. The widespread use of SSNs beyond their intended purpose raises privacy concerns and enables the continued rise in identity theft.

In accordance with the Privacy Act and related laws, on May 22, 2007, OMB issued Memorandum M-07-16, Safeguarding and Responding to the Breach of Personally Identifiable Information. M-07-16 requires agencies to, among other things, review their current holdings of personally identifiable information and to ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete and reduce such holdings to the minimum necessary for the proper performance of a documented agency function. Additionally, agencies are required to review their use of SSNs and establish a plan to eliminate the unnecessary collection and use of SSNs<sup>2</sup>. M-07-16 also requires that agencies participate in government-wide efforts to explore alternatives to agency use of SSNs as a personal identifier for both Federal employees and in Federal programs (e.g., surveys, data calls, etc.).

In our ongoing effort to comply with the Privacy Act and applicable OMB guidelines, the FEC supports the goals of M-07-16, and has developed this plan to review and reduce the holdings of personally identifiable information and to eliminate its unnecessary use of SSNs by mid-November 2008.

---

<sup>1</sup> The term “personally identifiable information” refers to information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.

<sup>2</sup> There are two requirements to any agency’s collection, use, maintenance, or dissemination of an SSN. Section 7(a)(1) of the Privacy Act provides that it shall be unlawful for any Federal, State, or local government agency to deny any individual any right, benefit, or privilege provided by law because of the individual’s refusal to disclose his social security account number unless required by Federal statute or pursuant to a preexisting statute or regulation. If an agency requests an individual to disclose his SSN, it shall inform that person whether that disclosure is mandatory or voluntary; the statutory or other authority under which the number is solicited; and what uses will be made of it. See 5 U.S.C. § 552a note.



#### **A. Plan to Review and Reduce Holdings of Personally Identifiable Information**

M-07-16 requires agencies to develop and make public a schedule for periodic review of holdings of personally identifiable information. The FEC has published the schedule on its website at [http://www.fec.gov/law/privacy\\_act\\_notices.shtml](http://www.fec.gov/law/privacy_act_notices.shtml). The schedule states that the Federal Election Commission will be publishing revised systems of records notices (SORNs) in 2007 and will conduct periodic reviews of its holdings of personally identifiable information on a biennial (two-year) basis. In connection with publishing revised SORNs, the General Law and Advice Division of the Office of General Counsel (OGC GLA) reviewed the FEC's holdings of personally identifiable information to ensure that they are accurate, relevant, timely, and complete. As a result of that review, OGC GLA revised the agency's SORNs, deleted two systems of records, and added new systems of records. The plan to ensure that the FEC maintains its holdings of personally identifiable information to the minimum necessary for agency function is to continue to review the holdings on a biennial basis in connection with the biennial review of agency systems of records. The PII review, however, will include PII contained in all records, and will not be limited to the review of agency systems of records that are subject to the Privacy Act's notice requirements.

#### **B. Plan to Eliminate Unnecessary Use of SSNs**

The FEC plan to eliminate unnecessary use of SSNs is composed of three main phases. During the first phase, the FEC's Information Systems Security Officer (ISSO) and OGC GLA will collect information from each of the FEC offices to determine which ones collect and use SSNs; the rationale for the collection and use; and whether the collection and use is necessary, or whether alternative identifying information may be used. During the second phase, the Co-Chief Privacy Officers will work with affected offices to explore alternatives to the collection and use of SSNs. During the third phase, the FEC will implement decisions regarding collection, use, and alternative identifiers. At the midpoint of the third phase, the ISSO and OGC GLA will monitor the impact that our decisions have had, to determine whether the plan is working as envisioned and to make adjustments as necessary. Thereafter, the Co-Chief Privacy Officers will review the agency's collection and use of SSNs on a biennial (two year) basis.

##### **Phase 1: Review (May 2007 through January 2008)**

In Phase 1, the ISSO will collect information from all offices within the FEC documenting whether the office collects or uses SSNs, why, and whether there are alternatives to the use of SSNs. This work is already underway; the ISSO has requested this information, several offices have responded, and the ISSO and OGC GLA will soon follow-up to obtain missing responses. Once the survey is complete, OGC GLA will review each collection to ensure that it is required by statute or regulation and authorized for the specific purpose for which it is actually used. The ISSO and OGC GLA will also interview appropriate personnel to confirm and clarify such responses.

### **Phase 2: Explore Options (January 2008 through May 2008)**

During this phase the Co-Chief Privacy Officers and their staffs will work with affected offices, the Staff Director, or her designee, and the Chief Financial Officer to explore feasible alternatives to the collection and use of SSNs. There may be instances where the collection and use of SSNs is justified, necessary, and unavoidable and where no satisfactory alternative is available. In those instances, the Co-Chief Privacy Officers will approve the collection and use of SSNs.

### **Phase 3: Implement Options and Assess (June, 2008 through November 2008)**

During this phase the decisions made during Phase 2 will be implemented. During August 2008, the ISSO will contact the offices whose practices regarding SSNs have changed to confirm that the practices have in fact changed, that the practices are in compliance with the plan, and to determine the effect of the change in practices on the functioning of the department. This will provide the Co-Chief Privacy Officers with an opportunity to assess the plan and to make any additional changes before November, 2008.

### **Biennial Review**

A review of the FEC's collection and use of SSNs will be conducted on a biennial basis in conjunction with our review of our systems of records and personally identifiable information holdings. Every two years, the ISSO will send a memorandum to each office asking whether it continues to collect and use SSNs, whether it has begun any new collections or uses of SSNs in the previous two years, why it collects and uses SSNs and whether alternatives are feasible. The Co-Chief Privacy Officers will then undertake a process similar to Phases 2 and 3 of this plan. The agency's efforts in this regard should be described in our Privacy Reports to OMB, Congress, and the FEC Office of Inspector General.

**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**

**Introduction**

Safeguarding personally identifiable information<sup>1</sup> in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. The Social Security Number (SSN) is a powerful piece of personally identifiable information, which has come to be used for numerous purposes other than those required by law or Social Security. The widespread use of SSNs beyond their intended purpose raises privacy concerns and enables the continued rise in identity theft.

In accordance with the Privacy Act and related laws, on May 22, 2007, OMB issued Memorandum M-07-16, Safeguarding and Responding to the Breach of Personally Identifiable Information. M-07-16 requires agencies to, among other things, review their current holdings of personally identifiable information and to ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete and reduce such holdings to the minimum necessary for the proper performance of a documented agency function. Additionally, agencies are required to review their use of SSNs and establish a plan to eliminate the unnecessary collection and use of SSNs<sup>2</sup>. M-07-16 also requires that agencies participate in government-wide efforts to explore alternatives to agency use of SSNs as a personal identifier for both Federal employees and in Federal programs (e.g., surveys, data calls, etc.).

In our ongoing effort to comply with the Privacy Act and applicable OMB guidelines, the FEC supports the goals of M-07-16, and has developed this plan to review and reduce the holdings of personally identifiable information and to eliminate its unnecessary use of SSNs by mid-November 2008.

---

<sup>1</sup> The term “personally identifiable information” refers to information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.

<sup>2</sup> There are two requirements to any agency’s collection, use, maintenance, or dissemination of an SSN. Section 7(a)(1) of the Privacy Act provides that it shall be unlawful for any Federal, State, or local government agency to deny any individual any right, benefit, or privilege provided by law because of the individual’s refusal to disclose his social security account number unless required by Federal statute or pursuant to a preexisting statute or regulation. If an agency requests an individual to disclose his SSN, it shall inform that person whether that disclosure is mandatory or voluntary; the statutory or other authority under which the number is solicited; and what uses will be made of it. See 5 U.S.C. § 552a note.

#### **A. Plan to Review and Reduce Holdings of Personally Identifiable Information**

M-07-16 requires agencies to develop and make public a schedule for periodic review of holdings of personally identifiable information. The FEC has published the schedule on its website at [http://www.fec.gov/law/privacy\\_act\\_notices.shtml](http://www.fec.gov/law/privacy_act_notices.shtml). The schedule states that the Federal Election Commission will be publishing revised systems of records notices (SORNs) in 2007 and will conduct periodic reviews of its holdings of personally identifiable information on a biennial (two-year) basis. In connection with publishing revised SORNs, the General Law and Advice Division of the Office of General Counsel (OGC GLA) reviewed the FEC's holdings of personally identifiable information to ensure that they are accurate, relevant, timely, and complete. As a result of that review, OGC GLA revised the agency's SORNs, deleted two systems of records, and added new systems of records. The plan to ensure that the FEC maintains its holdings of personally identifiable information to the minimum necessary for agency function is to continue to review the holdings on a biennial basis in connection with the biennial review of agency systems of records. The PII review, however, will include PII contained in all records, and will not be limited to the review of agency systems of records that are subject to the Privacy Act's notice requirements.

#### **B. Plan to Eliminate Unnecessary Use of SSNs**

The FEC plan to eliminate unnecessary use of SSNs is composed of three main phases. During the first phase, the FEC's Information Systems Security Officer (ISSO) and OGC GLA will collect information from each of the FEC offices to determine which ones collect and use SSNs; the rationale for the collection and use; and whether the collection and use is necessary, or whether alternative identifying information may be used. During the second phase, the Co-Chief Privacy Officers will work with affected offices to explore alternatives to the collection and use of SSNs. During the third phase, the FEC will implement decisions regarding collection, use, and alternative identifiers. At the midpoint of the third phase, the ISSO and OGC GLA will monitor the impact that our decisions have had, to determine whether the plan is working as envisioned and to make adjustments as necessary. Thereafter, the Co-Chief Privacy Officers will review the agency's collection and use of SSNs on a biennial (two year) basis.

##### **Phase 1: Review (May 2007 through January 2008)**

In Phase 1, the ISSO will collect information from all offices within the FEC documenting whether the office collects or uses SSNs, why, and whether there are alternatives to the use of SSNs. This work is already underway; the ISSO has requested this information, several offices have responded, and the ISSO and OGC GLA will soon follow-up to obtain missing responses. Once the survey is complete, OGC GLA will review each collection to ensure that it is required by statute or regulation and authorized for the specific purpose for which it is actually used. The ISSO and OGC GLA will also interview appropriate personnel to confirm and clarify such responses.

### **Phase 2: Explore Options (January 2008 through May 2008)**

During this phase the Co-Chief Privacy Officers and their staffs will work with affected offices, the Staff Director, or her designee, and the Chief Financial Officer to explore feasible alternatives to the collection and use of SSNs. There may be instances where the collection and use of SSNs is justified, necessary, and unavoidable and where no satisfactory alternative is available. In those instances, the Co-Chief Privacy Officers will approve the collection and use of SSNs.

### **Phase 3: Implement Options and Assess (June, 2008 through November 2008)**

During this phase the decisions made during Phase 2 will be implemented. During August 2008, the ISSO will contact the offices whose practices regarding SSNs have changed to confirm that the practices have in fact changed, that the practices are in compliance with the plan, and to determine the effect of the change in practices on the functioning of the department. This will provide the Co-Chief Privacy Officers with an opportunity to assess the plan and to make any additional changes before November, 2008.

### **Biennial Review**

A review of the FEC's collection and use of SSNs will be conducted on a biennial basis in conjunction with our review of our systems of records and personally identifiable information holdings. Every two years, the ISSO will send a memorandum to each office asking whether it continues to collect and use SSNs, whether it has begun any new collections or uses of SSNs in the previous two years, why it collects and uses SSNs and whether alternatives are feasible. The Co-Chief Privacy Officers will then undertake a process similar to Phases 2 and 3 of this plan. The agency's efforts in this regard should be described in our Privacy Reports to OMB, Congress, and the FEC Office of Inspector General.

**FEDERAL ELECTION COMMISSION  
MEMORANDUM DESCRIBING  
AGENCY'S PRIVACY PROGRAM**

As part of the Federal Information Security Management Act (FISMA) and Agency Privacy Management Report, the Office of Management and Budget (OMB) has instructed agencies to provide a description of their privacy program. The Federal Election Commission (FEC) provides the following description of its privacy program as part of the Agency's Privacy Management Report.

OMB, in its memorandum M-16-03, titled "Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements," required that all agencies submit a document describing the agency privacy program, including: (1) a description of the structure of the agency's privacy program, including the role of the Senior Agency Official for Privacy and the resources that the agency has dedicated to privacy-related functions; (2) an assessment of whether the Senior Agency Official for Privacy has the necessary authority, independence, access to agency leadership, subject matter expertise, and resources to effectively manage and oversee all privacy-related functions across the agency; and (3) any other information OMB should know about how privacy-related functions are performed at the agency.

The FEC's privacy program is managed jointly by the FEC's Office of the Staff Director and Office of General Counsel. The FEC has designated Co-Senior Agency Officials for Privacy (Co-SAOPs): Edward Holder, Acting Deputy Staff Director for Management and Administration, and Gregory Baker, Deputy General Counsel – Administration. The Co-SAOPs directly oversee the frontline employees who implement the agency's privacy program (the "Privacy Team"). In the Office of the Staff Director, these employees are the members of the Office of the Chief Information Officer (OCIO) Security team including the Chief Information Security Officer ("CISO"), Saady Abd-Elfattah—who is the only Agency employee who works at least half the time on privacy-related functions (noted in the Agency's answer to Question 2c of the FY 2016 SAOP FISMA reporting metrics. In the Office of General Counsel, these employees are the Assistant General Counsel for Administrative Law and attorneys in the Administrative Law Team. The only change to this management team over the last year was Mr. Abd-Elfattah, who replaced the Agency's previous CISO. This structure allows the Agency to quickly identify and nimbly address privacy issues from both the legal and technical perspectives. Additionally, this structure facilitates direct communication between the two offices, thereby preventing any bureaucratic delays. Thus, the Co-SAOPs have knowledgeable staff resources in the areas that privacy issues generally touch upon, and the staff easily shares information and works together to ensure agency compliance with all applicable privacy requirements.

The Co-SAOPs hold senior-level positions in the FEC's management hierarchy, reporting directly to the Staff Director and General Counsel, respectively. Given these positions, the Co-SAOPs have excellent access to agency leadership while remaining as independent as the Agency structure allows in overseeing the privacy program. Mr. Holder has served as Co-SAOP for 5 years and has 12 additional years working with privacy issues. Mr. Baker has served as Co-SAOP for 5 years and has 10 additional years working with privacy issues. Although the FEC is too small of an agency to have employees solely dedicated to privacy matters, the two

offices that jointly manage the privacy program have sufficient Privacy Team employees who are able to devote time to respond to privacy issues. The FEC Privacy Team also continues to work with the FEC's Office of Inspector General to satisfactorily complete Privacy Correction Action Plan recommendations that buttress other privacy requirements.

The Agency's Website Privacy Policy is located here: <http://www.fec.gov/privacy.shtml>. Additionally, the Agency's Privacy Act regulations, codified at 11 C.F.R. § 1.1, et seq. may be found on the Commission's website at: [http://www.fec.gov/law/cfr/cfr\\_2009.pdf](http://www.fec.gov/law/cfr/cfr_2009.pdf). Finally, the Agency's current systems of records notices may be found in Volume 73, No.1 of the Federal Register, or on the Commission's website at: [http://www.fec.gov/law/cfr/ej\\_compilation/2008/notice\\_2007-28.pdf](http://www.fec.gov/law/cfr/ej_compilation/2008/notice_2007-28.pdf).

## **FEDERAL ELECTION COMMISSION PRIVACY TRAINING FOR EMPLOYEES AND CONTRACTORS**

As part of the Federal Information Security Management Act (FISMA) and Agency Privacy Management Report, OMB has instructed agencies to provide a description of their privacy training for employees and contractors. The Federal Election Commission (FEC) provides the following description of its privacy training policies and practices as part of the Agency's Privacy Management Report.

The FEC conducts privacy training for new employees and annual refresher training for existing employees through an electronic training management system, Skillport, which employees access through the Agency's intranet. The Skillport training consists of a two-part PowerPoint slideshow—Part 1 (Privacy Training 101) addresses protection of personally identifiable information (PII) and Part 2 (Privacy Training 102) addresses Privacy Act requirements.<sup>1</sup> Privacy Training 101 provides employees with information on how to identify PII, how to properly secure and transmit information containing PII, and the potential impacts of failing to properly secure PII. Privacy Training 102 explains the requirements of the Privacy Act, including Systems of Records Notices, Privacy Act Statements, and records requests, as well as penalties for violating the Privacy Act. The training materials also include relevant Agency privacy policies. Following both parts of the training, employees are required to complete short multiple-choice quizzes containing scenario-based questions to test employee comprehension of the material. Employees must successfully answer all test questions to complete the training. The training materials are annually reviewed by the FEC's Privacy Team and updated as necessary.

New employees typically complete privacy training on their first day at the Agency, as completion of the training is a requirement for accessing the FEC's computer network. Existing employees are generally provided with a two-week window of time each year within which they must complete the annual refresher training. By conducting privacy training through Skillport, the Agency is able to track employees' progress with respect to the training and verify that employees have successfully completed all portions of the training.

The Agency's contractors do not have access to the Skillport database. Therefore, the Agency provides its contractors with the privacy training materials in hard copy. Contractors are required on their first day at the Agency to review the training slides, quiz questions, and relevant Agency policies, and must sign and submit to the Office of the Chief Information Officer (OCIO) a certification form verifying they have completed the training. Contractors are not permitted access to the Agency's information technology network until they have completed the training and submitted their certification form to OCIO.

In addition to the new employee and annual refresher privacy training, the Agency's Privacy Team periodically conducts live job-specific training for different offices and divisions within the Agency. The training content is targeted to the specific needs of the employees working in that office or division, and provides an opportunity for employees to ask questions of

---

<sup>1</sup> Since the FEC is exempt from FISMA and the E-Government Act, the Agency's privacy training focuses on the requirements of the Privacy Act and does not address provisions of FISMA and the E-Government Act.



the Privacy Team and discuss with their colleagues common privacy-related issues within their office or division.

## **Federal Election Commission**

### **Description of the Agency's Efforts to Comply with the Privacy-related Requirements in OMB M-16-04**

OMB Memorandum M-16-04, titled "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government" and issued by the Federal Chief Information Officer (FCIO), was published simultaneously with OMB Memorandum M-16-03 on October 30, 2015. This OMB memorandum "is the result of the [30-day] Cybersecurity Sprint," which was initiated by the FCIO on June 12, 2015. The Cybersecurity Sprint, as described by an OMB fact sheet, "instructed Federal agencies to immediately take a number of steps to further protect Federal information and assets and improve the resilience of Federal networks." OMB, "FACT SHEET: Enhancing and Strengthening the Federal Government's Cybersecurity" (June 12, 2015) at <https://www.whitehouse.gov/blog/2015/06/17/fact-sheet-enhancing-and-strengthening-federal-government-s-cybersecurity>. However, the FCIO "is the head of the Office of E-Government, an entity created by the E-Government Act. The E-Government Act relies upon the definition of 'agency' in 44 U.S.C. § 3502(1), which specifically excludes the FEC. 44 U.S. C. § 3601 (applying all definitions under 44 U.S.C. § 3502). Thus, the FEC may follow Office of E-Government guidance as a best practice but it is not binding on the FEC.

OMB Memo M-16-04 does not cite to authority for its mandates, but rather describes the mandates "buil[t] on existing policy work" and as being "part of a broader series of actions to bolster Federal civilian cybersecurity, which includes the issuance of updated guidance" on the Federal Information Security Management Act (FISMA) and OMB Circular A-130. FISMA applies the Paperwork Reduction Act's (PRA) definition of "agency," which explicitly excludes the FEC. 44 U.S.C. § 3502(1)(8 ). Circular A-130 establishes policy for the management of federal information resources. Authority for the Circular derives from several sources, some of which do not apply to the FEC. In addition, the CSIP "emphasizes the government-wide adherence to NIST standards and guidelines and builds on the core concepts of the Framework for Improving Critical Infrastructure Cybersecurity, which NIST developed in accordance with Executive Order 13636, Improving Critical Infrastructure Cybersecurity." The Executive Order (EO) relies on the definition of "agency" in 44 U.S.C. § 3502(1), which specifically excludes the FEC. See 44 U.S.C. § 3502(l)(B). Therefore, the EO does not apply to the FEC. The National Institute of Standards and Technology Act, 15 U.S.C. §278g-3, which authorizes NIST to create computer standards, also uses the PRA's definition of "agency," and is thus inapplicable to the FEC. Thus, the provisions of OMB M-16-04 were found to be inapplicable to the FEC.

Specifically, OMB seeks the following information related to the Agency's compliance with OMB M-16-04:

- The number of the agency's systems containing PII that have been identified by the agency as High Value Assets (HVAs).
- For all systems containing PII that have been identified as HVAs, whether the SAOP has reviewed each system to determine whether it requires new or updated system of records notices (SORNs) and/or privacy impact assessments (PIAs)

- Whether all HVAs containing PII that require SORNs and/or PIAs are covered by complete, up-to-date SORNs and/or PIAs
- The number of SORNs and/or PIAs that were established or updated pursuant to the SAOP's review

Because the FEC is exempt from the E-Government Act, it is exempt from any requirements established under the Act, including conducting PIAs. As the CSIP described in M-16-04 created HVAs, the inapplicability of the OMB memorandum to the FEC meant that the Agency did not need to identify HVAs. Accordingly, because the five questions posed each concern actions that are inapplicable to the FEC, the Agency's answer to each question is simply "not applicable."



FEDERAL ELECTION COMMISSION  
WASHINGTON, D.C. 20463

November 13, 2015

The Honorable Shaun Donovan  
Director  
Office of Management and Budget  
725 17th Street, NW  
Washington, DC 20503

Dear Director Donovan:

I am transmitting herewith the Annual Privacy Management Report of the Federal Election Commission's Co-Senior Agency Officials for Privacy, Edward W. Holder, Acting Deputy Staff Director, Management and Administration, and Gregory R. Baker, Deputy General Counsel - Administration. The Privacy Management Report responds to OMB's memorandum M-16-03 to heads of executive departments and agencies entitled "Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements."

I am advised that because the FEC is not included in the applicable definition of "agency" under the Federal Information Security Management Act (FISMA) or the E-Government Act, the FEC historically has not responded to those parts of OMB's request for an annual report that derive from those statutes, and that the attached report follows that historic practice. Consequently, I am advised, the attached report contains only responses to those questions directed to the Senior Agency Officials for Privacy.

Also appended to this report is the FEC Co-SAOP's progress update on the FEC's plan for eliminating the unnecessary use of social security numbers and its review and reduction of its holdings of personally identifiable information (PII), a copy of the FEC's breach notification policy, and a description of the FEC's privacy training for employees and contractors.

The FEC is an independent regulatory commission charged with administering and enforcing federal campaign finance law. In the course of carrying out its responsibilities, the FEC has always taken very seriously the privacy of information it collects and maintains on individuals.

I trust this information is responsive. Should you have any questions, please contact Mr. Holder at (202) 694-1250 or Mr. Baker at (202) 694-1650.

On behalf of the Commission,



Ann M. Ravel  
Chair

cc: Edward Holder  
Gregory Baker

Enclosure

2015 FEC Privacy Management Report (with attachments)

**FEDERAL ELECTION COMMISSION  
PRIVACY MANAGEMENT REPORT  
FISCAL YEAR 2015**



**PROGRESS UPDATE ON THE  
FEDERAL ELECTION COMMISSION'S  
REVIEW & REDUCTION OF  
PERSONALLY IDENTIFIABLE  
INFORMATION AND THE  
ELIMINATION OF THE  
UNNECESSARY USE OF SOCIAL  
SECURITY NUMBERS**





FEDERAL ELECTION COMMISSION  
Washington, DC 20463

November 13, 2015

The Honorable Shaun Donovan  
Director  
Office of Management and Budget  
725 17th Street, NW  
Washington, DC 20503

Dear Director Donovan:

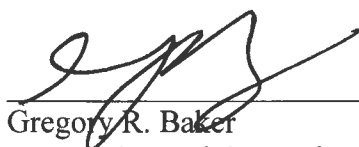
As part of the Fiscal Year 2015 Federal Information Security Management Act (FISMA) and Agency Privacy Management Report, the Office of Management and Budget has requested that agencies submit a progress update on their plans for eliminating the unnecessary use of social security numbers (SSNs) (hereinafter "SSN Reduction Initiative"), and their review and reduction of personally identifiable information (PII) holdings (hereinafter "PII Review Initiative"). The Federal Election Commission's (FEC) plan for eliminating SSNs and reducing its PII holdings has been solidified into one policy document entitled 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" (hereinafter FEC PII Plan). *See* FEC PII Plan, attached hereto as Appendix 1. Because the FEC's plans in this regard have been merged into one policy document, and its efforts for both initiatives are largely intertwined, this report provides a progress update on both initiatives.

In FY 2011, the Commission completed Phase 1 of its SSN Reduction Initiative (the collection and review of the agency's SSN holdings and Co-Chief Privacy Officer approval of recommendations for eliminating such holdings) and began Phase 2 of the initiative (collaborate with effected offices to develop feasible alternatives to SSN use). For two years the Privacy Team collected information from each of the Commission's offices and divisions regarding its SSN use. By using data from the Commission's PII inventory, as well as using information gained from interviews with FEC employees in each office, the team was able to determine which offices collected SSNs, the rationale for the collection, and whether there was a valid business justification for the collection. In FY 2012, the Privacy Team continued working with the affected offices to determine how best to address the recommendations, and reduce or diminish their SSN vulnerabilities, and also commenced a review of the Commission's PII holdings, which is following-up on the comprehensive inventory of the agency's PII holdings conducted by STSI during FY 2010.

During FY 2015, the Privacy Team continued to close out and implement items in the *2010 Follow-Up Audit of Privacy and Data Protection Corrective Action Plan* finalized by the Agency's Co-Chief Privacy Officers to address the PII Assessment Report recommendations from the review conducted by STSI. In FY 2016, the Co-Chief Privacy Officers will continue to focus on completing Phase 2 of the PII Plan by again reaching out the heads of all Agency offices and divisions to provide assistance with implementing any outstanding recommendations from the Phase 1 report. The Privacy Team will also continue working with points-of-contact from each Agency office and division to obtain updated PII inventories, so that the Privacy Team can determine what changes to the Agency's PII holdings have occurred since the previous review.

Should you have any questions, please contact the undersigned, Gregory Baker, Deputy General Counsel - Administration and Co-Senior Agency Official for Privacy, at (202) 694-1650, or Edward Holder, Deputy Staff Director, Management and Administration (Acting), and Co-Senior Agency Official for Privacy, at (202) 694-1250.

Sincerely,



Gregory R. Baker  
Deputy General Counsel - Administration  
Co-Senior Agency Official for Privacy



Edward W. Holder  
Deputy Staff Director, Management and Administration (Acting)  
Co-Senior Agency Official for Privacy

#### Attachments

FY 2015 Progress Update Report  
FEC Plan (Appendix 1)





FEDERAL ELECTION COMMISSION  
Washington, DC 20463

## **PROGRESS UPDATE ON THE FEDERAL ELECTION COMMISSION'S REVIEW & REDUCTION OF PERSONALLY IDENTIFIABLE INFORMATION AND THE ELIMINATION OF THE UNNECESSARY USE OF SOCIAL SECURITY NUMBERS (SSNs)**

### **I. Introduction**

In December 2007, the Federal Election Commission ("Commission" or "Agency") issued 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 07-16 (OMB M-07-16), Safeguarding Against and Responding to the Breach of Personally Identifiable Information" [hereinafter "FEC PII Plan"], which outlined the Commission's plans for reducing personally identifiable information (PII) holdings and eliminating the use of social security numbers (SSNs). The FEC PII Plan comprehensively outlines the Agency's goals for reducing, and in some cases eliminating, the Commission's use of PII and SSNs, and also serves as a basic framework for how the Agency will monitor its use of, and properly safeguard, its PII for years to come. This report provides an update on how the Commission has met, or is meeting, the goals outlined in the FEC PII Plan to date.

### **II. Plan to Review and Reduce Holdings of PII**

In determining the best way to safeguard the Agency's PII holdings, and in accordance with OMB M-07-16, the Commission outlined the following steps in the FEC PII Plan for reviewing and reducing its PII holdings:

1. Publish a schedule for periodic review of its holdings on the FEC website;
2. Publish revised Systems of Records Notices (SORNs) to accurately reflect the number of Privacy Act systems of records held by the Agency, the information contained in those systems of records, routine uses for the information by Agency, the system's location and system manager/owner, and other information as required under the Privacy Act;
3. Conduct a biennial review of the Agency's system of records to ensure accuracy of the published SORNs; and

4. Conduct a biennial review of the Agency's overall PII holdings found in all Agency systems (paper and electronic), regardless of whether such PII is in a system of records.

This year, the FEC has continued to make progress on fulfilling many of the goals outlined in the Plan as explained below.

**a) Biennial Review of Agency Systems of Records & Publication of Revised Systems of Records Notices (SORNs)**

In FY 2011, the Privacy Team completed a review of the Agency's systems of records in an effort to publish new and updated SORNs by doing the following:

- Conducting follow-up interviews with FEC managers who reported new systems of records, or changes to existing systems of records, to determine whether new or revised SORNs were needed for those systems.
- Conducting follow-up interviews with various system administrators to determine how the reported systems worked, and whether they were structured in such a way as to make them Privacy Act systems of records.
- Attending presentations whereby system administrators demonstrated how the reported systems worked.
- Identifying new systems requiring SORNs and existing SORNs requiring updates/revisions.

The Privacy Team then drafted SORNs for five new systems at the Agency and revised three existing SORNs to reflect changes in the systems of records. In FYs 2012 and 2013, the Privacy Team completed drafting and revising the SORNs, which were reviewed and approved by the Co-Chief Privacy Officers.

**Next Steps:** The Privacy Team anticipates that the SORNs will be submitted to the Commission for approval in calendar year 2016 and be published shortly thereafter. Simultaneously, the team will also be conducting another review of the Agency's systems of records to ensure the accuracy of the FEC's SORNs.

**b) Biennial Review of the Commission's PII Holdings ("PII Review Initiative")**

In FY 2012, the Privacy Team began its review of the Commission's PII holdings following-up on the comprehensive inventory of the agency's PII holdings conducted by STSI during FY 2010. The Privacy Team worked with points-of-contact (POCs) in each office and division in the Agency to obtain updated PII inventories. The Privacy Team provided the POCs with detailed instructions on how to update their inventories and the questionnaire forms, which included their respective office's PII inventories from the STSI review.

In FY 2013, the Privacy Team worked with POCs in various offices and divisions to obtain the outstanding updated PII inventories, which the Team has been reviewing to determine

what changes to the Agency's PII holdings have occurred since the prior PII review was conducted. The Privacy Team also continued working to implement the items in the 2010 Follow-Up Audit of Privacy and Data Protection Corrective Action Plan corrective action plan finalized by the Agency's Co-Chief Privacy Officers to address the PII Assessment Report recommendations from the review conducted by STSI. In FY 2015, the Privacy Team closed out more than ten corrective action plan recommendations, including using relevant Generally Accepted Privacy Principles (GAPP) to protect PII, encrypting mobile devices, and ensuring that contractors are required to handle PII safely.

**Next Steps:** The Agency's Chief Information Security Officer will be conducting informal risk assessments on the systems containing PII to determine whether there any deficiencies in the systems. Based on the results of these risk assessments the Privacy Team will prepare a report to the Co-Chief Privacy Officers' approval that will propose corrective actions, if necessary, to address any deficiencies discovered through the assessments.

### **III. Plan to Eliminate Unnecessary SSNs**

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 07-16 (OMB M-07-16), Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (hereinafter "FEC PII Plan") outlines three phases for the Agency's elimination of unnecessary SSN use:

1. Phase 1: The FEC's CISO and the Office of General Counsel, Administrative Law Team (OGC-ALT) will collect information from each of the FEC offices to determine which offices collect and use SSNs; the rationale for its collection and use; the SSNs' necessity; and whether alternative identifying information may be used instead of SSNs.
2. Phase 2: The Co-Chief Privacy Officers will work with affected offices to explore alternatives to the collection and use of SSNs.
3. Phase 3: The FEC will implement decisions regarding the collection and use of SSNs and alternative identifiers. The CISO and OGC-ALT will also monitor the impact of the implemented decisions to determine their effectiveness, and to make modifications if necessary. The Co-Chief Privacy Officers will review the Agency's collection and use of SSNs biennially.

To prevent the duplication of efforts for SSN information gathering, the Privacy Team rolled Phase 1 of the SSN Reduction Initiative into the PII Review Initiative. Following the PII Review Initiative, the Privacy Team analyzed the SSN information collected during, and prior to, the Initiative.<sup>1</sup> Using this information, the Privacy Team produced a "Social Security Numbers (SSNs) Reduction Plan Phase 1 Report Recommendations for Reducing Agency SSN Use." This

---

<sup>1</sup> Prior to the PII Review Initiative, the Privacy Team conducted an initial presentation on the SSN elimination project with support staff from every division and office in the agency. The Team conducted follow-up interviews with the support staff, who acted as points-of-contact in identifying documents containing PII within their respective work units. Information collected during this process was incorporated into the PII Review Initiative.

report, provided to the Co-Chief Privacy Officers, suggests alternatives for eliminating the unnecessary SSN use found throughout the agency. It signifies the completion of Phase 1 of the Agency's FEC PII Plan.

Beginning in FY 2013, the Co-Chief Privacy Officers moved forward with Phase 2 of the PII plan by recirculating the Phase 1 report to the heads of each office and division in the Agency and offering support to those offices that need assistance in addressing any unresolved issues concerning the recommendations in the report. Although the Agency's PII Plan has not yet reached its completion, several FEC Offices have eliminated use of SSNs. For example, the Office of General Counsel regularly instructs employees not to place their SSNs on training forms, even if the training form requests such information, and the responsible staff will not process forms containing such information.

**Next Steps:** The Co-Chief Privacy Officers will continue implementing Phases 2 and 3 of the PII Plan. The Privacy Team will also continue to work with specific agency offices to address any identified SSN handling and/or use weaknesses noted in the Phase 1 Report. The Privacy Team will monitor the impact of those alternatives on work processes to determine their effectiveness and to make adjustments as necessary to promote the goal of reducing and eliminating to the extent feasible, SSN use throughout the agency.

We hope that this information is helpful to you. If you have any questions regarding the contents of this report, please contact Gregory Baker, Deputy General Counsel - Administration and Co-Chief Privacy Officer, at (202) 694-1650, or Edward Holder, Acting Deputy Staff Director, Management and Administration and Co-Chief Privacy Officer, at (202) 694-1250.

## APPENDIX 1

**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**

**Introduction**

Safeguarding personally identifiable information<sup>1</sup> in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. The Social Security Number (SSN) is a powerful piece of personally identifiable information, which has come to be used for numerous purposes other than those required by law or Social Security. The widespread use of SSNs beyond their intended purpose raises privacy concerns and enables the continued rise in identity theft.

In accordance with the Privacy Act and related laws, on May 22, 2007, OMB issued Memorandum M-07-16, Safeguarding and Responding to the Breach of Personally Identifiable Information. M-07-16 requires agencies to, among other things, review their current holdings of personally identifiable information and to ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete and reduce such holdings to the minimum necessary for the proper performance of a documented agency function. Additionally, agencies are required to review their use of SSNs and establish a plan to eliminate the unnecessary collection and use of SSNs<sup>2</sup>. M-07-16 also requires that agencies participate in government-wide efforts to explore alternatives to agency use of SSNs as a personal identifier for both Federal employees and in Federal programs (e.g., surveys, data calls, etc.).

In our ongoing effort to comply with the Privacy Act and applicable OMB guidelines, the FEC supports the goals of M-07-16, and has developed this plan to review and reduce the holdings of personally identifiable information and to eliminate its unnecessary use of SSNs by mid-November 2008.

---

<sup>1</sup> The term “personally identifiable information” refers to information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.

<sup>2</sup> There are two requirements to any agency’s collection, use, maintenance, or dissemination of an SSN. Section 7(a)(1) of the Privacy Act provides that it shall be unlawful for any Federal, State, or local government agency to deny any individual any right, benefit, or privilege provided by law because of the individual’s refusal to disclose his social security account number unless required by Federal statute or pursuant to a preexisting statute or regulation. If an agency requests an individual to disclose his SSN, it shall inform that person whether that disclosure is mandatory or voluntary; the statutory or other authority under which the number is solicited; and what uses will be made of it. See 5 U.S.C. § 552a note.

#### **A. Plan to Review and Reduce Holdings of Personally Identifiable Information**

M-07-16 requires agencies to develop and make public a schedule for periodic review of holdings of personally identifiable information. The FEC has published the schedule on its website at [http://www.fec.gov/law/privacy\\_act\\_notices.shtml](http://www.fec.gov/law/privacy_act_notices.shtml). The schedule states that the Federal Election Commission will be publishing revised systems of records notices (SORNs) in 2007 and will conduct periodic reviews of its holdings of personally identifiable information on a biennial (two-year) basis. In connection with publishing revised SORNs, the General Law and Advice Division of the Office of General Counsel (OGC GLA) reviewed the FEC's holdings of personally identifiable information to ensure that they are accurate, relevant, timely, and complete. As a result of that review, OGC GLA revised the agency's SORNs, deleted two systems of records, and added new systems of records. The plan to ensure that the FEC maintains its holdings of personally identifiable information to the minimum necessary for agency function is to continue to review the holdings on a biennial basis in connection with the biennial review of agency systems of records. The PII review, however, will include PII contained in all records, and will not be limited to the review of agency systems of records that are subject to the Privacy Act's notice requirements.

#### **B. Plan to Eliminate Unnecessary Use of SSNs**

The FEC plan to eliminate unnecessary use of SSNs is composed of three main phases. During the first phase, the FEC's Information Systems Security Officer (ISSO) and OGC GLA will collect information from each of the FEC offices to determine which ones collect and use SSNs; the rationale for the collection and use; and whether the collection and use is necessary, or whether alternative identifying information may be used. During the second phase, the Co-Chief Privacy Officers will work with affected offices to explore alternatives to the collection and use of SSNs. During the third phase, the FEC will implement decisions regarding collection, use, and alternative identifiers. At the midpoint of the third phase, the ISSO and OGC GLA will monitor the impact that our decisions have had, to determine whether the plan is working as envisioned and to make adjustments as necessary. Thereafter, the Co-Chief Privacy Officers will review the agency's collection and use of SSNs on a biennial (two year) basis.

##### **Phase 1: Review (May 2007 through January 2008)**

In Phase 1, the ISSO will collect information from all offices within the FEC documenting whether the office collects or uses SSNs, why, and whether there are alternatives to the use of SSNs. This work is already underway; the ISSO has requested this information, several offices have responded, and the ISSO and OGC GLA will soon follow-up to obtain missing responses. Once the survey is complete, OGC GLA will review each collection to ensure that it is required by statute or regulation and authorized for the specific purpose for which it is actually used. The ISSO and OGC GLA will also interview appropriate personnel to confirm and clarify such responses.

### **Phase 2: Explore Options (January 2008 through May 2008)**

During this phase the Co-Chief Privacy Officers and their staffs will work with affected offices, the Staff Director, or her designee, and the Chief Financial Officer to explore feasible alternatives to the collection and use of SSNs. There may be instances where the collection and use of SSNs is justified, necessary, and unavoidable and where no satisfactory alternative is available. In those instances, the Co-Chief Privacy Officers will approve the collection and use of SSNs.

### **Phase 3: Implement Options and Assess (June, 2008 through November 2008)**

During this phase the decisions made during Phase 2 will be implemented. During August 2008, the ISSO will contact the offices whose practices regarding SSNs have changed to confirm that the practices have in fact changed, that the practices are in compliance with the plan, and to determine the effect of the change in practices on the functioning of the department. This will provide the Co-Chief Privacy Officers with an opportunity to assess the plan and to make any additional changes before November, 2008.

### **Biennial Review**

A review of the FEC's collection and use of SSNs will be conducted on a biennial basis in conjunction with our review of our systems of records and personally identifiable information holdings. Every two years, the ISSO will send a memorandum to each office asking whether it continues to collect and use SSNs, whether it has begun any new collections or uses of SSNs in the previous two years, why it collects and uses SSNs and whether alternatives are feasible. The Co-Chief Privacy Officers will then undertake a process similar to Phases 2 and 3 of this plan. The agency's efforts in this regard should be described in our Privacy Reports to OMB, Congress, and the FEC Office of Inspector General.



## **FEDERAL ELECTION COMMISSION PRIVACY TRAINING FOR EMPLOYEES AND CONTRACTORS**

As part of the Federal Information Security Management Act (FISMA) and Agency Privacy Management Report, OMB has instructed agencies to provide a description of their privacy training for employees and contractors. The Federal Election Commission (FEC) provides the following description of its privacy training policies and practices as part of the Agency's Privacy Management Report.

The FEC conducts privacy training for new employees and annual refresher training for existing employees through an electronic training management system, Skillport, which employees access through the Agency's intranet. The Skillport training consists of a two-part PowerPoint slideshow—Part 1 (Privacy Training 101) addresses protection of personally identifiable information (PII) and Part 2 (Privacy Training 102) addresses Privacy Act requirements.<sup>1</sup> Privacy Training 101 provides employees with information on how to identify PII, how to properly secure and transmit information containing PII, and the potential impacts of failing to properly secure PII. Privacy Training 102 explains the requirements of the Privacy Act, including Systems of Records Notices, Privacy Act Statements, and records requests, as well as penalties for violating the Privacy Act. The training materials also include relevant Agency privacy policies. Following both parts of the training, employees are required to complete short multiple-choice quizzes containing scenario-based questions to test employee comprehension of the material. Employees must successfully answer all test questions to complete the training. The training materials are annually reviewed by the FEC's Privacy Team and updated as necessary.

New employees typically complete privacy training on their first day at the Agency, as completion of the training is a requirement for accessing the FEC's computer network. Existing employees are generally provided with a two-week window of time each year within which they must complete the annual refresher training. By conducting privacy training through Skillport, the Agency is able to track employees' progress with respect to the training and verify that employees have successfully completed all portions of the training.

The Agency's contractors do not have access to the Skillport database. Therefore, the Agency provides its contractors with the privacy training materials in hard copy. Contractors are required on their first day at the Agency to review the training slides, quiz questions, and relevant Agency policies, and must sign and submit to the Office of the Chief Information Officer (OCIO) a certification form verifying they have completed the training. Contractors are not permitted access to the Agency's information technology network until they have completed the training and submitted their certification form to OCIO.

In addition to the new employee and annual refresher privacy training, the Agency's Privacy Team periodically conducts live job-specific training for different offices and divisions within the Agency. The training content is targeted to the specific needs of the employees working in that office or division, and provides an opportunity for employees to ask questions of

---

<sup>1</sup> Since the FEC is exempt from FISMA and the E-Government Act, the Agency's privacy training focuses on the requirements of the Privacy Act and does not address provisions of FISMA and the E-Government Act.

the Privacy Team and discuss with their colleagues common privacy-related issues within their office or division.

**FEDERAL ELECTION COMMISSION  
MEMORANDUM DESCRIBING  
AGENCY'S PRIVACY PROGRAM**

As part of the Federal Information Security Management Act (FISMA) and Agency Privacy Management Report, the Office of Management and Budget (OMB) has instructed agencies to provide a description of their privacy program. The Federal Election Commission (FEC) provides the following description of its privacy program as part of the Agency's Privacy Management Report.

OMB, in its memorandum M-16-03, titled "Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements," required that all agencies submit a document describing the agency privacy program, including: (1) a description of the structure of the agency's privacy program, including the role of the Senior Agency Official for Privacy and the resources that the agency has dedicated to privacy-related functions; (2) an assessment of whether the Senior Agency Official for Privacy has the necessary authority, independence, access to agency leadership, subject matter expertise, and resources to effectively manage and oversee all privacy-related functions across the agency; and (3) any other information OMB should know about how privacy-related functions are performed at the agency.

The FEC's privacy program is managed jointly by the FEC's Office of the Staff Director and Office of General Counsel. The FEC has designated Co-Senior Agency Officials for Privacy (Co-SAOPs): Edward Holder, Acting Deputy Staff Director for Management and Administration, and Gregory Baker, Deputy General Counsel – Administration. The Co-SAOPs directly oversee the frontline employees who implement the agency's privacy program (the "Privacy Team"). In the Office of the Staff Director, these employees are the members of the Office of the Chief Information Officer (OCIO) Security team, and in the Office of General Counsel, these employees are the Assistant General Counsel for Administrative Law and attorneys in the Administrative Law Team. This structure allows the Agency to quickly identify and nimbly address privacy issues from both the legal and technical perspectives. Additionally, this structure facilitates direct communication between the two offices, thereby preventing any bureaucratic delays. Thus, the Co-SAOPs have knowledgeable staff resources in the areas that privacy issues generally touch upon, and the staff easily shares information and works together to ensure agency compliance with all applicable privacy requirements.

The Co-SAOPs hold senior-level positions in the FEC's management hierarchy, reporting directly to the Staff Director and General Counsel, respectively. Given these positions, the Co-SAOPs have excellent access to agency leadership while remaining as independent as the Agency structure allows in overseeing the privacy program. Mr. Holder has served as Co-SAOP for 4 years and has 12 additional years working with privacy issues. Mr. Baker has served as Co-SAOP for 4 years and has 10 additional years working with privacy issues. Although the FEC is too small of an agency to have employees solely dedicated to privacy matters, the two offices that jointly manage the privacy program have sufficient Privacy Team employees who are able to devote time to respond to privacy issues. The FEC Privacy Team also continues to work with the FEC's Office of Inspector General to satisfactorily complete Privacy Correction Action Plan recommendations that buttress other privacy requirements.

# **Federal Election Commission**

## **Policy and Plan for Responding to Breaches of Personally Identifiable Information**

### **I. Introduction and Overview**

The Federal Election Commission (FEC) developed this policy and plan for responding to breaches of personally identifiable information in response to memoranda that the Office of Management and Budget (OMB) issued in 2006<sup>1</sup> and 2007<sup>2</sup>. To mitigate the risk of harm (including identity theft) should a data breach occur, the OMB Memoranda recommend that agencies establish a core management group to respond to the loss of certain categories of sensitive personal information.<sup>3</sup>

This core management team will be convened and conduct an initial evaluation of any potential breach to help guide the Commission's further response. OMB's experience suggests that such a core group should include, at minimum, an agency's chief information officer, chief legal officer, Inspector General and a senior management official (or their designees). The group should ensure that the agency has brought together staff with expertise in information technology, legal authorities, the Privacy Act and law enforcement, as necessary, to respond to a data breach.

This breach plan identifies appropriate senior agency management officials within the FEC and provides a high-level strategy to handle data security breaches, including those incidents posing a potential risk of identity theft. The breach plan also specifies the responsibilities of the FEC Breach Notification and Response Team (Breach Team), whose mission is to provide advance planning, guidance, an initial analysis and a recommended course of action in response to a breach. In the event of a breach, the Breach Team will be convened promptly, conduct a risk analysis to determine whether the breach poses risks related to identity theft or other harms,<sup>4</sup> and timely implement a risk-based, tailored response to each breach.

---

<sup>1</sup> OMB Memorandum regarding "Recommendations for Identity Theft Related Data Breach Notification," issued on September 20, 2006 (hereafter "2006 OMB Memo," attached at Tab A). The 2006 OMB Memo also is available at [http://www.whitehouse.gov/omb/memoranda/fy2006/task\\_force\\_theft\\_memo.pdf](http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf).

<sup>2</sup> OMB Memorandum 07-16 regarding "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," issued on May 22, 2007 (hereafter "2007 OMB Memo," attached at Tab B). The 2007 OMB Memo also is available at <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf>.

<sup>3</sup> Although the 2007 OMB memo specifically references the Federal Information Security Management Act of 2002 (FISMA) and its associated requirements from which the FEC is exempt, the Commission has nevertheless developed this breach plan. In addition, the Commission has implemented the following steps to minimize its risk of a breach of Personally Identifiable Information (PII):

- Whole drive encryption of all FEC laptops.
- 30 minute time out for inactivity of all mobile devices.
- Password protection of all mobile devices.
- Two factor authentication for all FEC laptops.
- Issuance of Guidelines to Protect Sensitive Information.

<sup>4</sup> In this context, when assessing the risk of potential harms, consistent with the Privacy Act of 1974, agencies are expected to consider a wide range of harms, including embarrassment, inconvenience, or unfairness to any

## **A. Definitions for Purposes of the Breach Plan**

- 1. Personally Identifiable Information (PII)** — As set forth in the 2007 OMB Memo, PII refers to information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. (See 2007 OMB Memo footnote (1)).
- 2. Covered Information** — As set forth in the 2006 OMB Memo, Covered Information refers to PII posing a risk of identity theft. Covered Information shall include, at minimum, the following information, whether in paper, in electronic form, or communicated orally:
  - (1) An individual's Social Security number alone; or
  - (2) An individual's name or address or phone number in combination with one or more of the following: date of birth; Social Security number; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; credit or debit card number.
- 3. Breach and/or breach incident** — The terms "breach" and/or "breach incident" include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII or Covered Information, whether physical or electronic.

## **II. Breach Notification Response Team Membership and Roles**

Consistent with the OMB Memoranda, the Breach Team will consist of the following members:

- Staff Director or Deputy Staff Director.
- Deputy Chief Information Officer (DCIO).
- Inspector General (IG) or Deputy IG.
- General Counsel (GC) or Deputy GC.
- Deputy General Counsel - Administration.
- Information Systems Security Officer (ISSO).

The Deputy General Counsel - Administration and Deputy Chief Information Officer (DCIO) currently share the roles of Chief Privacy Officer and Senior Agency Official for Privacy (SAOP) at the FEC.

---

individual on whom information is maintained. Accordingly, the Breach Team will consider in its analysis a wide range of harms such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial information is involved in the breach.

The DCIO will serve as the Chair of the Breach Team, preside over meetings and initiate responses to breaches as appropriate. The Deputy General Counsel - Administration will serve as the Co-Chair of the Breach Team.

The IG may play a central role in the investigation of any breach. The IG shall be consulted in any determination of the risk of harm and the need for providing individuals with notice. In addition, in accordance with the Inspector General Act and other applicable laws, the IG may conduct an investigation to determine, among other things: (1) if the theft of PII or Covered Information was intentional; (2) if employee misconduct was involved; (3) if the theft or compromise was a one-time breach incident or the subject of a broad based criminal effort; (4) if the breach incident is the subject of an ongoing investigation by the FBI, Secret Service, or other federal, state, or local law enforcement; or (5) if notice to individuals or third parties would compromise an ongoing law enforcement investigation. In addition, in accordance with the IG Act, the IG has a responsibility to report to the Attorney General whenever the IG has reasonable grounds to believe there has been a violation of Federal criminal law.

The GC shall be responsible generally for providing legal support and guidance in responding to a suspected or actual breach. The GC's responsibilities, for example, include:

(1) Preparing new or revised Privacy Act system of records notices or other notices or routine uses or implementing other requirements of the Privacy Act of 1974 relating to the collection, maintenance, use or disclosure of Agency systems of records subject to that Act; (2) identifying and providing legal opinions on other applicable requirements of statutes, rules, orders or policies, including those relating to personnel, acquisitions, computer security, access and disclosure, etc.; (3) coordinating with the IG and other appropriate agency officials and staff, whether referral of a matter to other authorities is warranted as a matter of law; and (4) serving as the Agency's official legal representative in any formal administrative or judicial proceedings that might arise as a result of a suspected or actual breach.

Once it has been determined that a breach has occurred, the Staff Director will immediately inform all Commissioners and provide all relevant known details. The Staff Director will provide to all Commissioners as soon as it is available the Breach Team's proposed response plan and ensure the Commissioners are kept informed of the progress of the Breach Team's decision-making about further actions to be taken under this Breach Plan.

The ISSO will participate in all phases of the agency's planning, preparation, management reviews and response to breaches involving PII and Covered Information. The ISSO also will provide support to the Breach Team by ensuring that it receives information in a timely manner, subject matter expertise and operational support in analyzing and responding to a suspected or actual breach.

Other FEC divisions/offices that the Breach Team may ask to assist in responding to a breach include representatives from the Information Technology Division (ITD) and Office of General Counsel (OGC), the Office of Human Resources and the Press Officer. In addition, responding to a particular breach likely will require assistance from the managers and employees of the Office that experienced the breach.

The Breach Team also will coordinate with other FEC offices to ensure that appropriate risk-based, tailored responses to data breaches are developed and implemented. In addition, the Breach Team will work closely with other Federal agencies, offices, and teams as deemed appropriate.

### **III. Taking Steps to Contain and Control the Breach**

The DCIO, in coordination with the ITD Computer Incident Response Team, will take all necessary steps to contain, control and mitigate the risks from the breach and prevent further unauthorized access to or use of individual information, including: (1) monitoring, freezing, or closing affected accounts; (2) modifying computer access codes or physical access controls; and (3) taking other necessary and appropriate action.

In addition, for paper records and physical security incidents generally that may affect privacy, the FEC Physical Security Officer shall ensure that necessary steps are taken to contain and control a breach and prevent further unauthorized access to or use of individual information. Such steps may include changing locks or key codes, deactivating ID cards, adding further physical security to entrances/exits, alerting the Federal Protective Service, development or implementation of special instructions, reminders, or training, etc. The FEC Physical Security Officer shall take these steps without undue delay and do so in coordination with the Breach Team, ITD, Office of the Inspector General (OIG), OGC and other appropriate offices.

### **IV. Reporting of Incidents**

Pursuant to FEC internal policy, all agency officials, employees and contractors are directed to immediately report any suspected computer security incidents (whether involving a paper or electronic format) to their managers and to the ITD HelpDesk, 202-694-1255. Such incident reports shall be initially forwarded to and reviewed by the ISSO to determine whether they merit notification of United States Computer Emergency Response Team (US-CERT). The IG shall be provided a copy of all breach incident reports. These reports also shall be immediately forwarded to the DCIO and the SAOP, who shall determine whether the Breach Team should review the reported breach incident to determine any other appropriate agency response. The Breach Team, in coordination with the representatives from OGC and ITD, will ensure that employees are trained how to respond to and report any confirmed or potential breach. Formal incident response requirements shall be part of the FEC's mandatory Security Awareness and Privacy Training.

### **V. Initial Response to Breaches**

#### **A. Initial Assessment**

Within 24 hours of being notified of an incident involving or potentially involving Covered Information or PII, the DCIO (or SAOP if the DCIO is not available) will notify all members of the Breach Team. The ISSO will brief the Breach Team of the initial assessment of the situation and if possible at that time provide a report on whether an actual breach occurred and the probability of a loss of PII or Covered Information.

The Breach Team will, as appropriate, evaluate the ISSO's report and any other pertinent data and decide whether further response is required.

Determining what data have been compromised or potentially compromised is vital to making an accurate risk assessment and charting an appropriate course of action.

As part of the initial evaluation, the following issues should be addressed:

- Date of breach incident.
- Nature of breach incident and the means by which the breach occurred:
  - Unauthorized access to information.
  - Unauthorized use of information.
  - Lost computer, storage device, or portable media.
  - System or network intrusion.
  - Loss of control of paper documents containing sensitive information.
- Person who reported breach incident.
- Person who discovered breach incident.
- Number of individuals potentially affected.
- The accessibility of the information.<sup>5</sup>

## **B. Management Review and Investigative Responsibilities**

- If an incident appears to involve the unintentional or negligent loss of control or disclosure of PII or Covered Information, the DCIO may have primary responsibility for undertaking a review. The DCIO shall promptly notify the IG if additional information becomes available that indicates the intentional loss of control or disclosure of PII or Covered Information.
- If an incident appears to involve the intentional or grossly negligent disclosure of PII or Covered Information or possible criminal activity, the IG will have responsibility for undertaking an investigation.
- If intent cannot be ascertained as part of the initial evaluation, the DCIO may have initial responsibility, in consultation with the IG, until intent can be determined.

## **VI. Identity Theft Risk Analysis**

To determine if a breach causes identity theft risks, the Breach Team should evaluate the factors identified in the 2006 OMB Memo. These factors include not only the type of Covered Information that was compromised, but also:

- How easy or difficult it would be for an unauthorized person to access the information given how it was protected;

---

<sup>5</sup> For example, the Breach Team will determine whether the information was properly encrypted or otherwise rendered unusable. The fact that information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals.



- The means by which the loss occurred, including whether the breach incident might be the result of criminal activity or is likely the result of criminal activity;
- The ability of the FEC to mitigate the identity theft; and
- Evidence that the compromised information is actually being used to commit identity theft.

## **VII. Analysis of Other Likely Harms**

Even if there is no risk of identity theft, consistent with the Privacy Act and the 2007 OMB Memo, in considering whether to notify consumers and others, the Breach Team shall consider a wide range of potential harms. These include risk of harm to reputation, embarrassment, inconvenience, unfairness, harassment, and prejudice, particularly when health or financial information is involved in the breach. Accordingly, the Breach Team will consider a wide variety of possible harms in determining whether external notification of a breach is necessary.

To determine the likely risk of harm caused by a breach when Covered Information is not involved and there is no risk of identity theft, the Breach Team will consider five factors as set forth in the 2007 OMB Memo:

- Nature and context of the data.<sup>6</sup>
- Number of individuals affected.
- Likelihood the information is accessible and usable.
- Likelihood the breach may lead to harm.
- Ability of the agency to mitigate the risk of harm.

## **VIII. Identity Theft Response**

If the Breach Team determines that there is a risk of identity theft from a breach of Covered Information, the Breach Team should develop a response plan to mitigate such risk. In developing such a plan, the Breach Team should consider the options available to agencies and individuals to protect potential victims of identity theft as set forth in the 2006 OMB Memo.

For individuals, these options include:

- Contacting financial institutions.
- Monitoring financial account activity.
- Requesting a free credit report.
- Placing an initial fraud alert on credit reports.

---

<sup>6</sup> For example, if an office Rolodex contained PII (name, address, telephone number, etc.), the information probably would not be considered sensitive and the breach of this information would not warrant further action. In contrast, if a list of retirees contained employee social security numbers and birth dates, the information likely would be considered sensitive and breach of this information would justify further action. In assessing the levels of risk of harm, the Breach Team therefore will consider the data elements in light of their context and the broad range of potential harms resulting from the disclosure to unauthorized individuals.

- For residents of states in which it is authorized under state law, considering placing a freeze on their credit file.
- For deployed members of the military, considering placing an active duty alert on their credit file.
- Reviewing resources at [www.idtheft.gov](http://www.idtheft.gov).

For the FEC, these options include:

- Engaging a third party to conduct a data breach analysis to determine whether a particular data loss appears to be resulting in identity theft<sup>7</sup>;
- Providing credit-monitoring services if the Breach Team has determined that such services are required to mitigate potential damage due to the breach.<sup>8</sup>

## **IX. Notification of Individuals**

If the Breach Team, applying the criteria set forth in the 2006 and 2007 OMB Memoranda, determines that (1) an unauthorized person has accessed Covered Information and that the information could be used for fraudulent purposes, or (2) an unauthorized person has accessed PII and its use is likely to lead to harm, then the affected individuals will be notified. This notice will be provided without unreasonable delay but no later than 45 days after the determination is made, except in extraordinary circumstances.

In determining the timing and content of the notice, the Breach Team will consult with the IG or other law enforcement officials investigating the breach incident before making any public disclosures about the breach incident.

The Breach Team will consider the following elements in the notification process:

- Timing of the notice.
- Source of the notice.
- Contents of the notice.
- Means of notification.
- Preparation needed for follow-on inquiries.

---

<sup>7</sup> One such third party conducted a data breach analysis for the Department of Veterans Affairs May 2006 data breach potentially involving 17.5 million veterans.

<sup>8</sup> The Breach Team should follow the recommendations set forth in the 2006 OMB Memo. If a decision is made to retain monitoring services, the Breach Team should consult the OMB Memorandum regarding “Use of Commercial Credit Monitoring Services Blanket Purchase Agreements,” issued on December 22, 2006, and available at <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-04.pdf>. A decision to retain credit-monitoring services will be made only after a careful balancing of likely harms and likely costs. Moreover, the Chief Financial Officer must be consulted before a decision to retain monitoring services is made.

These elements shall be analyzed in accordance with guidance set forth in the OMB Memoranda. In particular, the contents of any notice given by the agency to individuals shall include the following:

- A brief description of what happened;
- To the extent possible, a description of the types of information that were involved in the breach. A brief description of what the agency is doing to investigate the breach, mitigate losses, and protect against further breaches;
- Point-of-contact information for individuals who have questions or need more information, including a toll-free number, Web site, and/or postal address; and
- If the breach involved Covered Information, steps for individuals to undertake in order to protect themselves from the risk of identity theft, including how to take advantage of credit monitoring or other service(s) that the agency intends to offer, if any, and URL information for the Federal Election Commission's Web site, including specific relevant publications.

## **X. Notification to Third Parties**

Notice to individuals and notice to third parties, including the timing, order, and content of such notice, shall be carefully coordinated so that ongoing investigations are not compromised, the risk of harm to individuals is minimized, and the information provided is consistent and accurate. Notice to the following third parties may be considered depending on the nature of the breach:

**A. Law Enforcement.** Depending on the nature of the breach, it may be appropriate for the Breach Team, the FEC Information System Security Officer, FEC Physical Security Officer and/or the IG, to notify federal, state or local law enforcement, including local police departments, the Federal Protective Service and the Federal Bureau of Investigation.

**B. United States Computer Emergency Readiness Team (US-CERT).** OMB guidance requiring reporting to US-CERT is derived from FISMA from which the Commission is exempt. However, in the event of an actual breach, or strong suspicion of a breach, the DCIO and SAOP would report the breach incident to US-CERT as a matter of "best practice" and to facilitate our obtaining whatever law enforcement assistance might be necessary.

**C. Media and the Public.** The Press Officer, in coordination with the Breach Team, is responsible for conducting all meetings and discussions with the news media and public about a breach or suspected breach. This includes the issuance of press releases and related materials on the Commission's web site [www.FEC.gov](http://www.FEC.gov).

**D. Financial Institutions.** If the breach involves government-authorized credit cards, the FEC must notify the issuing bank promptly as set forth in the 2007 OMB Memo. The Chief Financial Officer or the Administrative Services Manager shall coordinate with the Breach Team regarding such notification and suspension of the account. If the breach involves individuals' bank account numbers that are used in employment-related transactions (e.g., payroll), the FEC will notify the bank or other entity that handles that particular transaction for the agency.

**E. Appropriate Members of Congress.** The Office of Communications, in consultation with the Breach Team, is responsible for coordinating all communications and meetings with members of Congress and their staff. The Breach Team will notify the Press Officer immediately when an issue arises that may require communications with members of Congress and their staff.

**F. Attorney General.** The IG shall promptly notify the Attorney General of any criminal violations relating to the disclosure or use of Covered Information or PII, as required by the Inspector General Act of 1978, as amended.

## **XI. Documentation of Breach Notification Response**

As appropriate, the Breach Team shall document responses to breaches for the purpose of tracking the Breach Team handling and disposition of specific breaches. The Breach Team, in coordination with any other appropriate officials and staff shall ensure that appropriate and adequate records are maintained to document the Breach Team response to all breaches reported under this plan. In accordance with the Privacy Act of 1974 and the Federal Records Act, such records shall be generated, compiled and maintained in a manner sufficient to safeguard the financial, legal or other rights of individuals, if any, affected by the breach, including any parallel law enforcement investigations, litigation, or other pending action. At the same time, such documentation shall be maintained no longer than required by applicable records retention schedules to ensure that any sensitive PII in such records is not unnecessarily retained or exposed to a risk of breach. Such records shall be destroyed only in accordance with approved and secure methods designed to ensure against inadvertent disclosure, theft or other compromise of personal or other nonpublic information.

## **XII. Evaluation of Breach Response**

The development and implementation of this plan for responding to breaches of personally identifiable information is an ongoing process, not a one-time exercise. Accordingly, following the handling and disposition of all suspected or actual breaches reported under this plan, the Breach Team will evaluate the Breach Team's response and identify tasks that could have been conducted more effectively and efficiently and make improvements or modifications to the plan as appropriate.



FEDERAL ELECTION COMMISSION  
WASHINGTON, D.C. 20463

November 14, 2014

The Honorable Shaun Donovan  
Director  
Office of Management and Budget  
725 17th Street, NW  
Washington, DC 20503

Dear Director Donovan:

I am transmitting herewith the Annual Privacy Management Report of the Federal Election Commission's Co-Senior Agency Officials for Privacy, Edward W. Holder, Acting Deputy Staff Director for Management and Administration, and Gregory R. Baker, Deputy General Counsel - Administration. The Privacy Management Report responds to OMB's memorandum M-15-01 to heads of executive departments and agencies entitled "Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices."

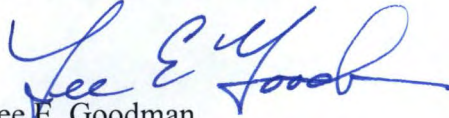
I am advised that because the FEC is not included in the applicable definition of "agency" under the Federal Information Security Management Act (FISMA) or the E-Government Act, the FEC historically has not responded to those parts of OMB's request for an annual report that derive from those statutes, and that the attached report follows that historic practice. Consequently, I am advised, the attached report contains only responses to those questions directed to the Senior Agency Officials for Privacy.

Also appended to this report is the FEC Co-SAOP's progress update on the FEC's plan for eliminating the unnecessary use of social security numbers and its review and reduction of its holdings of personally identifiable information (PII), a copy of the FEC's breach notification policy, and a description of the FEC's privacy training for employees and contractors.

The FEC is an independent regulatory commission charged with administering and enforcing federal campaign finance law. In the course of carrying out its responsibilities, the FEC has always taken very seriously the privacy of information it collects and maintains on individuals.

I trust this information is responsive. Should you have any questions, please contact Mr. Holder at (202) 694-1250 or Mr. Baker at (202) 694-1650.

On behalf of the Commission,



Lee E. Goodman  
Chairman

cc: Edward Holder  
Gregory Baker

Enclosure

2014 FEC Privacy Management Report (with attachments)

## **FEDERAL ELECTION COMMISSION PRIVACY TRAINING FOR EMPLOYEES AND CONTRACTORS**

As part of the FY 2014 Federal Information Security Management Act (FISMA) and Agency Privacy Management Report, OMB has instructed agencies to provide a description of their privacy training for employees and contractors. The Federal Election Commission (FEC) provides the following description of its privacy training policies and practices as part of the Agency's Privacy Management Report.

The FEC conducts privacy training for new employees and annual refresher training for existing employees through an electronic training management system, Skillport, which employees access through the Agency's intranet. The Skillport training consists of a two-part PowerPoint slideshow—Part 1 (Privacy Training 101) addresses protection of personally identifiable information (PII) and Part 2 (Privacy Training 102) addresses Privacy Act requirements.<sup>1</sup> Privacy Training 101 provides employees with information on how to identify PII, how to properly secure and transmit information containing PII, and the potential impacts of failing to properly secure PII. Privacy Training 102 explains the requirements of the Privacy Act, including Systems of Records Notices, Privacy Act Statements, and records requests, as well as penalties for violating the Privacy Act. The training materials also include relevant Agency privacy policies. Following both parts of the training, employees are required to complete short multiple-choice quizzes containing scenario-based questions to test employee comprehension of the material. Employees must successfully answer all test questions to complete the training. The training materials are annually reviewed by the FEC's Privacy Team and updated as necessary.

New employees typically complete privacy training on their first day at the Agency, as completion of the training is a requirement for accessing the FEC's computer network. Existing employees are generally provided with a two-week window of time each year within which they must complete the annual refresher training. By conducting privacy training through Skillport, the Agency is able to track employees' progress with respect to the training and verify that employees have successfully completed all portions of the training.

The Agency's contractors do not have access to the Skillport database. Therefore, the Agency provides its contractors with the privacy training materials in hard copy. Contractors are required on their first day at the Agency to review the training slides, quiz questions, and relevant Agency policies, and must sign and submit to the Office of the Chief Information Officer (OCIO) a certification form verifying they have completed the training. Contractors are not permitted access to the Agency's information technology network until they have completed the training and submitted their certification form to OCIO.

In addition to the new employee and annual refresher privacy training, the Agency's Privacy Team periodically conducts live job-specific training for different offices and divisions within the Agency. The training content is targeted to the specific needs of the employees working in that office or division, and provides an opportunity for employees to ask questions of

---

<sup>1</sup> Since the FEC is exempt from FISMA and the E-Government Act, the Agency's privacy training focuses on the requirements of the Privacy Act and does not address provisions of FISMA and the E-Government Act.

the Privacy Team and discuss with their colleagues common privacy-related issues within their office or division.



**FEDERAL ELECTION COMMISSION  
PRIVACY MANAGEMENT REPORT  
FISCAL YEAR 2014**



**PROGRESS UPDATE ON THE  
FEDERAL ELECTION COMMISSION'S  
REVIEW & REDUCTION OF  
PERSONALLY IDENTIFIABLE  
INFORMATION AND THE  
ELIMINATION OF THE  
UNNECESSARY USE OF SOCIAL  
SECURITY NUMBERS**



FEDERAL ELECTION COMMISSION  
Washington, DC 20463

November 14, 2014

The Honorable Shaun Donovan  
Director  
Office of Management and Budget  
725 17th Street, NW  
Washington, DC 20503

Dear Director Donovan:

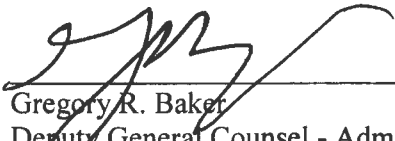
As part of the Fiscal Year 2014 Federal Information Security Management Act (FISMA) and Agency Privacy Management Report, the Office of Management and Budget has requested that agencies submit a progress update on their plans for eliminating the unnecessary use of social security numbers (SSNs) (hereinafter "SSN Reduction Initiative"), and their review and reduction of personally identifiable information (PII) holdings (hereinafter "PII Review Initiative"). The Federal Election Commission's (FEC) plan for eliminating SSNs and reducing its PII holdings has been solidified into one policy document entitled 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" (hereinafter FEC PII Plan). *See* FEC PII Plan, attached hereto as Appendix 1. Because the FEC's plans in this regard have been merged into one policy document, and its efforts for both initiatives are largely intertwined, this report provides a progress update on both initiatives.

In FY 2011, the Commission completed Phase 1 of its SSN Reduction Initiative (the collection and review of the agency's SSN holdings and Co-Chief Privacy Officer approval of recommendations for eliminating such holdings) and began Phase 2 of the initiative (collaborate with effected offices to develop feasible alternatives to SSN use). For two years the Privacy Team collected information from each of the Commission's offices and divisions regarding its SSN use. By using data from the Commission's PII inventory, as well as using information gained from interviews with FEC employees in each office, the team was able to determine which offices collected SSNs, the rationale for the collection, and whether there was a valid business justification for the collection. In FY 2012, the Privacy Team continued working with the affected offices to determine how best to address the recommendations, and reduce or diminish their SSN vulnerabilities, and also commenced a review of the Commission's PII holdings, which is following-up on the comprehensive inventory of the agency's PII holdings conducted by STSI during FY 2010.

During FY 2014, the Privacy Team continued to implement items in the *2010 Follow-Up Audit of Privacy and Data Protection Corrective Action Plan* finalized by the Agency's Co-Chief Privacy Officers to address the PII Assessment Report recommendations from the review conducted by STSI. In FY 2015, the Co-Chief Privacy Officers will work to complete Phase 2 of the PII Plan by again reaching out the heads of all Agency offices and divisions to provide assistance with implementing any outstanding recommendations from the Phase 1 report. The Privacy Team will also continue working with points-of-contact from each Agency office and division to obtain updated PII inventories, so that the Privacy Team can determine what changes to the Agency's PII holdings have occurred since the previous review.

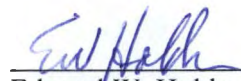
Should you have any questions, please contact the undersigned, Gregory Baker, Deputy General Counsel - Administration and Co-Senior Agency Official for Privacy, at (202) 694-1650, or Edward Holder, Acting Deputy Staff Director for Management and Administration, and Co-Senior Agency Official for Privacy, at (202) 694-1250.

Sincerely,



---

Gregory R. Baker  
Deputy General Counsel - Administration  
Co-Senior Agency Official for Privacy



---

Edward W. Holder  
Acting Deputy Staff Director for Management and Administration  
Co-Senior Agency Official for Privacy

#### Attachments

FY 2014 Progress Update Report  
FEC Plan (Appendix 1)



FEDERAL ELECTION COMMISSION  
Washington, DC 20463

## **PROGRESS UPDATE ON THE FEDERAL ELECTION COMMISSION'S REVIEW & REDUCTION OF PERSONALLY IDENTIFIABLE INFORMATION AND THE ELIMINATION OF THE UNNECESSARY USE OF SOCIAL SECURITY NUMBERS (SSNs)**

### **I. Introduction**

In December 2007, the Federal Election Commission ("Commission" or "Agency") issued 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 07-16 (OMB M-07-16), Safeguarding Against and Responding to the Breach of Personally Identifiable Information" [hereinafter "FEC PII Plan"], which outlined the Commission's plans for reducing personally identifiable information (PII) holdings and eliminating the use of social security numbers (SSNs). The FEC PII Plan comprehensively outlines the Agency's goals for reducing, and in some cases eliminating, the Commission's use of PII and SSNs, and also serves as a basic framework for how the Agency will monitor its use of, and properly safeguard, its PII for years to come. This report provides an update on how the Commission has met, or is meeting, the goals outlined in the FEC PII Plan to date.

### **II. Plan to Review and Reduce Holdings of PII**

In determining the best way to safeguard the Agency's PII holdings, and in accordance with OMB M-07-16, the Commission outlined the following steps in the FEC PII Plan for reviewing and reducing its PII holdings:

1. Publish a schedule for periodic review of its holdings on the FEC website;
2. Publish revised Systems of Records Notices (SORNs) to accurately reflect the number of Privacy Act systems of records held by the Agency, the information contained in those systems of records, routine uses for the information by Agency, the system's location and system manager/owner, and other information as required under the Privacy Act;
3. Conduct a biennial review of the Agency's system of records to ensure accuracy of the published SORNs; and

4. Conduct a biennial review of the Agency's overall PII holdings found in all Agency systems (paper and electronic), regardless of whether such PII is in a system of records.

This year, the FEC has continued to make progress on fulfilling many of the goals outlined in the Plan as explained below.

**a) Biennial Review of Agency Systems of Records & Publication of Revised Systems of Records Notices (SORNs)**

In FY 2011, the Privacy Team completed a review of the Agency's systems of records in an effort to publish new and updated SORNs by doing the following:

- Conducting follow-up interviews with FEC managers who reported new systems of records, or changes to existing systems of records, to determine whether new or revised SORNs were needed for those systems.
- Conducting follow-up interviews with various system administrators to determine how the reported systems worked, and whether they were structured in such a way as to make them Privacy Act systems of records.
- Attending presentations whereby system administrators demonstrated how the reported systems worked.
- Identifying new systems requiring SORNs and existing SORNs requiring updates/revisions.

The Privacy Team then drafted SORNs for five new systems at the Agency and revised three existing SORNs to reflect changes in the systems of records. In FYs 2012 and 2013, the Privacy Team completed drafting and revising the SORNs, which were reviewed and approved by the Co-Chief Privacy Officers.

**Next Steps:** The Privacy Team anticipates that the SORNs will be submitted to the Commission for approval in early calendar year 2015 and be published shortly thereafter. Simultaneously, the team will also be conducting another review of the Agency's systems of records to ensure the accuracy of the FEC's SORNs.

**b) Biennial Review of the Commission's PII Holdings ("PII Review Initiative")**

In FY 2012, the Privacy Team began its review of the Commission's PII holdings following-up on the comprehensive inventory of the agency's PII holdings conducted by STSI during FY 2010. The Privacy Team worked with points-of-contact (POCs) in each office and division in the Agency to obtain updated PII inventories. The Privacy Team provided the POCs with detailed instructions on how to update their inventories and the questionnaire forms, which included their respective office's PII inventories from the STSI review.

In FY 2013, the Privacy Team worked with POCs in various offices and divisions to obtain the outstanding updated PII inventories, which the Team has been reviewing to determine



what changes to the Agency's PII holdings have occurred since the prior PII review was conducted. The Privacy Team also continued working to implement the items in the 2010 Follow-Up Audit of Privacy and Data Protection Corrective Action Plan corrective action plan finalized by the Agency's Co-Chief Privacy Officers to address the PII Assessment Report recommendations from the review conducted by STSI. Due to the departure of several Privacy Team members, including the Chief Information Security Officer (CISO) [formerly the Information Systems Security Officer (ISSO)] and Assistant General Counsel for Administrative Law, the Agency's progress in completing the PII review was delayed; but the Agency anticipates that progress will be enhanced in FY 2015.

**Next Steps:** The Agency's CISO will be conducting informal risk assessments on the systems containing PII to determine whether there any deficiencies in the systems. Based on the results of these risk assessments the Privacy Team will prepare a report to the Co-Chief Privacy Officers' approval that will propose corrective actions, if necessary, to address any deficiencies discovered through the assessments.

### **III. Plan to Eliminate Unnecessary SSNs**

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 07-16 (OMB M-07-16), Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (hereinafter "FEC PII Plan") outlines three phases for the Agency's elimination of unnecessary SSN use:

1. Phase 1: The FEC's CISO and the Office of General Counsel, Administrative Law Team (OGC-ALT) will collect information from each of the FEC offices to determine which offices collect and use SSNs; the rationale for its collection and use; the SSNs' necessity; and whether alternative identifying information may be used instead of SSNs.
2. Phase 2: The Co-Chief Privacy Officers will work with affected offices to explore alternatives to the collection and use of SSNs.
3. Phase 3: The FEC will implement decisions regarding the collection and use of SSNs and alternative identifiers. The CISO and OGC-ALT will also monitor the impact of the implemented decisions to determine their effectiveness, and to make modifications if necessary. The Co-Chief Privacy Officers will review the Agency's collection and use of SSNs biennially.

To prevent the duplication of efforts for SSN information gathering, the Privacy Team rolled Phase 1 of the SSN Reduction Initiative into the PII Review Initiative. Following the PII Review Initiative, the Privacy Team analyzed the SSN information collected during, and prior to, the Initiative.<sup>1</sup> Using this information, the Privacy Team produced a "Social Security Numbers

---

<sup>1</sup> Prior to the PII Review Initiative, the Privacy Team conducted an initial presentation on the SSN elimination project with support staff from every division and office in the agency. The Team conducted follow-up interviews with the support staff, who acted as points-of-contact in identifying documents containing PII within their respective work units. Information collected during this process was incorporated into the PII Review Initiative.

(SSNs) Reduction Plan Phase 1 Report Recommendations for Reducing Agency SSN Use.” This report, provided to the Co-Chief Privacy Officers, suggests alternatives for eliminating the unnecessary SSN use found throughout the agency. It signifies the completion of Phase 1 of the Agency’s FEC PII Plan.

Beginning in FY 2013, the Co-Chief Privacy Officers moved forward with Phase 2 of the PII plan by recirculating the Phase 1 report to the heads of each office and division in the Agency and offering support to those offices that need assistance in addressing any unresolved issues concerning the recommendations in the report. Although the Agency’s PII Plan is not yet complete, several FEC Offices have found alternatives to using SSNs. For example, the Office of General Counsel regularly instructs employees not to place their SSNs on training forms, even if the training form requests such information.

**Next Steps:** The Co-Chief Privacy Officers will continue implementing Phases 2 and 3 of the PII Plan. The Privacy Team will also continue to work with specific agency offices to address any identified SSN handling and/or use weaknesses noted in the Phase 1 Report. The Privacy Team will monitor the impact of those alternatives on work processes to determine their effectiveness and to make adjustments as necessary to promote the goal of reducing and eliminating to the extent feasible, SSN use throughout the agency.

We hope that this information is helpful to you. If you have any questions regarding the contents of this report, please contact Gregory Baker, Deputy General Counsel - Administration and Co-Chief Privacy Officer, at (202) 694-1650, or Edward Holder, Acting Deputy Staff Director for Management and Administration and Co-Chief Privacy Officer, at (202) 694-1250.

## APPENDIX 1



**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**

**Introduction**

Safeguarding personally identifiable information<sup>1</sup> in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. The Social Security Number (SSN) is a powerful piece of personally identifiable information, which has come to be used for numerous purposes other than those required by law or Social Security. The widespread use of SSNs beyond their intended purpose raises privacy concerns and enables the continued rise in identity theft.

In accordance with the Privacy Act and related laws, on May 22, 2007, OMB issued Memorandum M-07-16, Safeguarding and Responding to the Breach of Personally Identifiable Information. M-07-16 requires agencies to, among other things, review their current holdings of personally identifiable information and to ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete and reduce such holdings to the minimum necessary for the proper performance of a documented agency function. Additionally, agencies are required to review their use of SSNs and establish a plan to eliminate the unnecessary collection and use of SSNs<sup>2</sup>. M-07-16 also requires that agencies participate in government-wide efforts to explore alternatives to agency use of SSNs as a personal identifier for both Federal employees and in Federal programs (e.g., surveys, data calls, etc.).

In our ongoing effort to comply with the Privacy Act and applicable OMB guidelines, the FEC supports the goals of M-07-16, and has developed this plan to review and reduce the holdings of personally identifiable information and to eliminate its unnecessary use of SSNs by mid-November 2008.

---

<sup>1</sup> The term “personally identifiable information” refers to information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.

<sup>2</sup> There are two requirements to any agency’s collection, use, maintenance, or dissemination of an SSN. Section 7(a)(1) of the Privacy Act provides that it shall be unlawful for any Federal, State, or local government agency to deny any individual any right, benefit, or privilege provided by law because of the individual’s refusal to disclose his social security account number unless required by Federal statute or pursuant to a preexisting statute or regulation. If an agency requests an individual to disclose his SSN, it shall inform that person whether that disclosure is mandatory or voluntary; the statutory or other authority under which the number is solicited; and what uses will be made of it. See 5 U.S.C. § 552a note.

#### **A. Plan to Review and Reduce Holdings of Personally Identifiable Information**

M-07-16 requires agencies to develop and make public a schedule for periodic review of holdings of personally identifiable information. The FEC has published the schedule on its website at [http://www.fec.gov/law/privacy\\_act\\_notices.shtml](http://www.fec.gov/law/privacy_act_notices.shtml). The schedule states that the Federal Election Commission will be publishing revised systems of records notices (SORNs) in 2007 and will conduct periodic reviews of its holdings of personally identifiable information on a biennial (two-year) basis. In connection with publishing revised SORNs, the General Law and Advice Division of the Office of General Counsel (OGC GLA) reviewed the FEC's holdings of personally identifiable information to ensure that they are accurate, relevant, timely, and complete. As a result of that review, OGC GLA revised the agency's SORNs, deleted two systems of records, and added new systems of records. The plan to ensure that the FEC maintains its holdings of personally identifiable information to the minimum necessary for agency function is to continue to review the holdings on a biennial basis in connection with the biennial review of agency systems of records. The PII review, however, will include PII contained in all records, and will not be limited to the review of agency systems of records that are subject to the Privacy Act's notice requirements.

#### **B. Plan to Eliminate Unnecessary Use of SSNs**

The FEC plan to eliminate unnecessary use of SSNs is composed of three main phases. During the first phase, the FEC's Information Systems Security Officer (ISSO) and OGC GLA will collect information from each of the FEC offices to determine which ones collect and use SSNs; the rationale for the collection and use; and whether the collection and use is necessary, or whether alternative identifying information may be used. During the second phase, the Co-Chief Privacy Officers will work with affected offices to explore alternatives to the collection and use of SSNs. During the third phase, the FEC will implement decisions regarding collection, use, and alternative identifiers. At the midpoint of the third phase, the ISSO and OGC GLA will monitor the impact that our decisions have had, to determine whether the plan is working as envisioned and to make adjustments as necessary. Thereafter, the Co-Chief Privacy Officers will review the agency's collection and use of SSNs on a biennial (two year) basis.

##### **Phase 1: Review (May 2007 through January 2008)**

In Phase 1, the ISSO will collect information from all offices within the FEC documenting whether the office collects or uses SSNs, why, and whether there are alternatives to the use of SSNs. This work is already underway; the ISSO has requested this information, several offices have responded, and the ISSO and OGC GLA will soon follow-up to obtain missing responses. Once the survey is complete, OGC GLA will review each collection to ensure that it is required by statute or regulation and authorized for the specific purpose for which it is actually used. The ISSO and OGC GLA will also interview appropriate personnel to confirm and clarify such responses.

### **Phase 2: Explore Options (January 2008 through May 2008)**

During this phase the Co-Chief Privacy Officers and their staffs will work with affected offices, the Staff Director, or her designee, and the Chief Financial Officer to explore feasible alternatives to the collection and use of SSNs. There may be instances where the collection and use of SSNs is justified, necessary, and unavoidable and where no satisfactory alternative is available. In those instances, the Co-Chief Privacy Officers will approve the collection and use of SSNs.

### **Phase 3: Implement Options and Assess (June, 2008 through November 2008)**

During this phase the decisions made during Phase 2 will be implemented. During August 2008, the ISSO will contact the offices whose practices regarding SSNs have changed to confirm that the practices have in fact changed, that the practices are in compliance with the plan, and to determine the effect of the change in practices on the functioning of the department. This will provide the Co-Chief Privacy Officers with an opportunity to assess the plan and to make any additional changes before November, 2008.

### **Biennial Review**

A review of the FEC's collection and use of SSNs will be conducted on a biennial basis in conjunction with our review of our systems of records and personally identifiable information holdings. Every two years, the ISSO will send a memorandum to each office asking whether it continues to collect and use SSNs, whether it has begun any new collections or uses of SSNs in the previous two years, why it collects and uses SSNs and whether alternatives are feasible. The Co-Chief Privacy Officers will then undertake a process similar to Phases 2 and 3 of this plan. The agency's efforts in this regard should be described in our Privacy Reports to OMB, Congress, and the FEC Office of Inspector General.

**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**

**Introduction**

Safeguarding personally identifiable information<sup>1</sup> in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. The Social Security Number (SSN) is a powerful piece of personally identifiable information, which has come to be used for numerous purposes other than those required by law or Social Security. The widespread use of SSNs beyond their intended purpose raises privacy concerns and enables the continued rise in identity theft.

In accordance with the Privacy Act and related laws, on May 22, 2007, OMB issued Memorandum M-07-16, Safeguarding and Responding to the Breach of Personally Identifiable Information. M-07-16 requires agencies to, among other things, review their current holdings of personally identifiable information and to ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete and reduce such holdings to the minimum necessary for the proper performance of a documented agency function. Additionally, agencies are required to review their use of SSNs and establish a plan to eliminate the unnecessary collection and use of SSNs<sup>2</sup>. M-07-16 also requires that agencies participate in government-wide efforts to explore alternatives to agency use of SSNs as a personal identifier for both Federal employees and in Federal programs (e.g., surveys, data calls, etc.).

In our ongoing effort to comply with the Privacy Act and applicable OMB guidelines, the FEC supports the goals of M-07-16, and has developed this plan to review and reduce the holdings of personally identifiable information and to eliminate its unnecessary use of SSNs by mid-November 2008.

---

<sup>1</sup> The term “personally identifiable information” refers to information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.

<sup>2</sup> There are two requirements to any agency’s collection, use, maintenance, or dissemination of an SSN. Section 7(a)(1) of the Privacy Act provides that it shall be unlawful for any Federal, State, or local government agency to deny any individual any right, benefit, or privilege provided by law because of the individual’s refusal to disclose his social security account number unless required by Federal statute or pursuant to a preexisting statute or regulation. If an agency requests an individual to disclose his SSN, it shall inform that person whether that disclosure is mandatory or voluntary; the statutory or other authority under which the number is solicited; and what uses will be made of it. See 5 U.S.C. § 552a note.

#### **A. Plan to Review and Reduce Holdings of Personally Identifiable Information**

M-07-16 requires agencies to develop and make public a schedule for periodic review of holdings of personally identifiable information. The FEC has published the schedule on its website at [http://www.fec.gov/law/privacy\\_act\\_notices.shtml](http://www.fec.gov/law/privacy_act_notices.shtml). The schedule states that the Federal Election Commission will be publishing revised systems of records notices (SORNs) in 2007 and will conduct periodic reviews of its holdings of personally identifiable information on a biennial (two-year) basis. In connection with publishing revised SORNs, the General Law and Advice Division of the Office of General Counsel (OGC GLA) reviewed the FEC's holdings of personally identifiable information to ensure that they are accurate, relevant, timely, and complete. As a result of that review, OGC GLA revised the agency's SORNs, deleted two systems of records, and added new systems of records. The plan to ensure that the FEC maintains its holdings of personally identifiable information to the minimum necessary for agency function is to continue to review the holdings on a biennial basis in connection with the biennial review of agency systems of records. The PII review, however, will include PII contained in all records, and will not be limited to the review of agency systems of records that are subject to the Privacy Act's notice requirements.

#### **B. Plan to Eliminate Unnecessary Use of SSNs**

The FEC plan to eliminate unnecessary use of SSNs is composed of three main phases. During the first phase, the FEC's Information Systems Security Officer (ISSO) and OGC GLA will collect information from each of the FEC offices to determine which ones collect and use SSNs; the rationale for the collection and use; and whether the collection and use is necessary, or whether alternative identifying information may be used. During the second phase, the Co-Chief Privacy Officers will work with affected offices to explore alternatives to the collection and use of SSNs. During the third phase, the FEC will implement decisions regarding collection, use, and alternative identifiers. At the midpoint of the third phase, the ISSO and OGC GLA will monitor the impact that our decisions have had, to determine whether the plan is working as envisioned and to make adjustments as necessary. Thereafter, the Co-Chief Privacy Officers will review the agency's collection and use of SSNs on a biennial (two year) basis.

##### **Phase 1: Review (May 2007 through January 2008)**

In Phase 1, the ISSO will collect information from all offices within the FEC documenting whether the office collects or uses SSNs, why, and whether there are alternatives to the use of SSNs. This work is already underway; the ISSO has requested this information, several offices have responded, and the ISSO and OGC GLA will soon follow-up to obtain missing responses. Once the survey is complete, OGC GLA will review each collection to ensure that it is required by statute or regulation and authorized for the specific purpose for which it is actually used. The ISSO and OGC GLA will also interview appropriate personnel to confirm and clarify such responses.

### **Phase 2: Explore Options (January 2008 through May 2008)**

During this phase the Co-Chief Privacy Officers and their staffs will work with affected offices, the Staff Director, or her designee, and the Chief Financial Officer to explore feasible alternatives to the collection and use of SSNs. There may be instances where the collection and use of SSNs is justified, necessary, and unavoidable and where no satisfactory alternative is available. In those instances, the Co-Chief Privacy Officers will approve the collection and use of SSNs.

### **Phase 3: Implement Options and Assess (June, 2008 through November 2008)**

During this phase the decisions made during Phase 2 will be implemented. During August 2008, the ISSO will contact the offices whose practices regarding SSNs have changed to confirm that the practices have in fact changed, that the practices are in compliance with the plan, and to determine the effect of the change in practices on the functioning of the department. This will provide the Co-Chief Privacy Officers with an opportunity to assess the plan and to make any additional changes before November, 2008.

### **Biennial Review**

A review of the FEC's collection and use of SSNs will be conducted on a biennial basis in conjunction with our review of our systems of records and personally identifiable information holdings. Every two years, the ISSO will send a memorandum to each office asking whether it continues to collect and use SSNs, whether it has begun any new collections or uses of SSNs in the previous two years, why it collects and uses SSNs and whether alternatives are feasible. The Co-Chief Privacy Officers will then undertake a process similar to Phases 2 and 3 of this plan. The agency's efforts in this regard should be described in our Privacy Reports to OMB, Congress, and the FEC Office of Inspector General.

# **Federal Election Commission**

## **Policy and Plan for Responding to Breaches of Personally Identifiable Information**

### **I. Introduction and Overview**

The Federal Election Commission (FEC) developed this policy and plan for responding to breaches of personally identifiable information in response to memoranda that the Office of Management and Budget (OMB) issued in 2006<sup>1</sup> and 2007<sup>2</sup>. To mitigate the risk of harm (including identity theft) should a data breach occur, the OMB Memoranda recommend that agencies establish a core management group to respond to the loss of certain categories of sensitive personal information.<sup>3</sup>

This core management team will be convened and conduct an initial evaluation of any potential breach to help guide the Commission's further response. OMB's experience suggests that such a core group should include, at minimum, an agency's chief information officer, chief legal officer, Inspector General and a senior management official (or their designees). The group should ensure that the agency has brought together staff with expertise in information technology, legal authorities, the Privacy Act and law enforcement, as necessary, to respond to a data breach.

This breach plan identifies appropriate senior agency management officials within the FEC and provides a high-level strategy to handle data security breaches, including those incidents posing a potential risk of identity theft. The breach plan also specifies the responsibilities of the FEC Breach Notification and Response Team (Breach Team), whose mission is to provide advance planning, guidance, an initial analysis and a recommended course of action in response to a breach. In the event of a breach, the Breach Team will be convened promptly, conduct a risk analysis to determine whether the breach poses risks related to identity theft or other harms,<sup>4</sup> and timely implement a risk-based, tailored response to each breach.

---

<sup>1</sup> OMB Memorandum regarding "Recommendations for Identity Theft Related Data Breach Notification," issued on September 20, 2006 (hereafter "2006 OMB Memo," attached at Tab A). The 2006 OMB Memo also is available at [http://www.whitehouse.gov/omb/memoranda/fy2006/task\\_force\\_theft\\_memo.pdf](http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf).

<sup>2</sup> OMB Memorandum 07-16 regarding "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," issued on May 22, 2007 (hereafter "2007 OMB Memo," attached at Tab B). The 2007 OMB Memo also is available at <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf>.

<sup>3</sup> Although the 2007 OMB memo specifically references the Federal Information Security Management Act of 2002 (FISMA) and its associated requirements from which the FEC is exempt, the Commission has nevertheless developed this breach plan. In addition, the Commission has implemented the following steps to minimize its risk of a breach of Personally Identifiable Information (PII):

- Whole drive encryption of all FEC laptops.
- 30 minute time out for inactivity of all mobile devices.
- Password protection of all mobile devices.
- Two factor authentication for all FEC laptops.
- Issuance of Guidelines to Protect Sensitive Information.

<sup>4</sup> In this context, when assessing the risk of potential harms, consistent with the Privacy Act of 1974, agencies are expected to consider a wide range of harms, including embarrassment, inconvenience, or unfairness to any

## **A. Definitions for Purposes of the Breach Plan**

- 1. Personally Identifiable Information (PII)** — As set forth in the 2007 OMB Memo, PII refers to information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. (See 2007 OMB Memo footnote (1)).
- 2. Covered Information** — As set forth in the 2006 OMB Memo, Covered Information refers to PII posing a risk of identity theft. Covered Information shall include, at minimum, the following information, whether in paper, in electronic form, or communicated orally:
  - (1) An individual's Social Security number alone; or
  - (2) An individual's name or address or phone number in combination with one or more of the following: date of birth; Social Security number; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; credit or debit card number.
- 3. Breach and/or breach incident** — The terms "breach" and/or "breach incident" include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII or Covered Information, whether physical or electronic.

## **II. Breach Notification Response Team Membership and Roles**

Consistent with the OMB Memoranda, the Breach Team will consist of the following members:

- Staff Director or Deputy Staff Director.
- Deputy Chief Information Officer (DCIO).
- Inspector General (IG) or Deputy IG.
- General Counsel (GC) or Deputy GC.
- Deputy General Counsel - Administration.
- Information Systems Security Officer (ISSO).

The Deputy General Counsel - Administration and Deputy Chief Information Officer (DCIO) currently share the roles of Chief Privacy Officer and Senior Agency Official for Privacy (SAOP) at the FEC.

---

individual on whom information is maintained. Accordingly, the Breach Team will consider in its analysis a wide range of harms such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial information is involved in the breach.



The DCIO will serve as the Chair of the Breach Team, preside over meetings and initiate responses to breaches as appropriate. The Deputy General Counsel - Administration will serve as the Co-Chair of the Breach Team.

The IG may play a central role in the investigation of any breach. The IG shall be consulted in any determination of the risk of harm and the need for providing individuals with notice. In addition, in accordance with the Inspector General Act and other applicable laws, the IG may conduct an investigation to determine, among other things: (1) if the theft of PII or Covered Information was intentional; (2) if employee misconduct was involved; (3) if the theft or compromise was a one-time breach incident or the subject of a broad based criminal effort; (4) if the breach incident is the subject of an ongoing investigation by the FBI, Secret Service, or other federal, state, or local law enforcement; or (5) if notice to individuals or third parties would compromise an ongoing law enforcement investigation. In addition, in accordance with the IG Act, the IG has a responsibility to report to the Attorney General whenever the IG has reasonable grounds to believe there has been a violation of Federal criminal law.

The GC shall be responsible generally for providing legal support and guidance in responding to a suspected or actual breach. The GC's responsibilities, for example, include:

(1) Preparing new or revised Privacy Act system of records notices or other notices or routine uses or implementing other requirements of the Privacy Act of 1974 relating to the collection, maintenance, use or disclosure of Agency systems of records subject to that Act; (2) identifying and providing legal opinions on other applicable requirements of statutes, rules, orders or policies, including those relating to personnel, acquisitions, computer security, access and disclosure, etc.; (3) coordinating with the IG and other appropriate agency officials and staff, whether referral of a matter to other authorities is warranted as a matter of law; and (4) serving as the Agency's official legal representative in any formal administrative or judicial proceedings that might arise as a result of a suspected or actual breach.

Once it has been determined that a breach has occurred, the Staff Director will immediately inform all Commissioners and provide all relevant known details. The Staff Director will provide to all Commissioners as soon as it is available the Breach Team's proposed response plan and ensure the Commissioners are kept informed of the progress of the Breach Team's decision-making about further actions to be taken under this Breach Plan.

The ISSO will participate in all phases of the agency's planning, preparation, management reviews and response to breaches involving PII and Covered Information. The ISSO also will provide support to the Breach Team by ensuring that it receives information in a timely manner, subject matter expertise and operational support in analyzing and responding to a suspected or actual breach.

Other FEC divisions/offices that the Breach Team may ask to assist in responding to a breach include representatives from the Information Technology Division (ITD) and Office of General Counsel (OGC), the Office of Human Resources and the Press Officer. In addition, responding to a particular breach likely will require assistance from the managers and employees of the Office that experienced the breach.

The Breach Team also will coordinate with other FEC offices to ensure that appropriate risk-based, tailored responses to data breaches are developed and implemented. In addition, the Breach Team will work closely with other Federal agencies, offices, and teams as deemed appropriate.

### **III. Taking Steps to Contain and Control the Breach**

The DCIO, in coordination with the ITD Computer Incident Response Team, will take all necessary steps to contain, control and mitigate the risks from the breach and prevent further unauthorized access to or use of individual information, including: (1) monitoring, freezing, or closing affected accounts; (2) modifying computer access codes or physical access controls; and (3) taking other necessary and appropriate action.

In addition, for paper records and physical security incidents generally that may affect privacy, the FEC Physical Security Officer shall ensure that necessary steps are taken to contain and control a breach and prevent further unauthorized access to or use of individual information. Such steps may include changing locks or key codes, deactivating ID cards, adding further physical security to entrances/exits, alerting the Federal Protective Service, development or implementation of special instructions, reminders, or training, etc. The FEC Physical Security Officer shall take these steps without undue delay and do so in coordination with the Breach Team, ITD, Office of the Inspector General (OIG), OGC and other appropriate offices.

### **IV. Reporting of Incidents**

Pursuant to FEC internal policy, all agency officials, employees and contractors are directed to immediately report any suspected computer security incidents (whether involving a paper or electronic format) to their managers and to the ITD HelpDesk, 202-694-1255. Such incident reports shall be initially forwarded to and reviewed by the ISSO to determine whether they merit notification of United States Computer Emergency Response Team (US-CERT). The IG shall be provided a copy of all breach incident reports. These reports also shall be immediately forwarded to the DCIO and the SAOP, who shall determine whether the Breach Team should review the reported breach incident to determine any other appropriate agency response. The Breach Team, in coordination with the representatives from OGC and ITD, will ensure that employees are trained how to respond to and report any confirmed or potential breach. Formal incident response requirements shall be part of the FEC's mandatory Security Awareness and Privacy Training.

### **V. Initial Response to Breaches**

#### **A. Initial Assessment**

Within 24 hours of being notified of an incident involving or potentially involving Covered Information or PII, the DCIO (or SAOP if the DCIO is not available) will notify all members of the Breach Team. The ISSO will brief the Breach Team of the initial assessment of the situation and if possible at that time provide a report on whether an actual breach occurred and the probability of a loss of PII or Covered Information.

The Breach Team will, as appropriate, evaluate the ISSO's report and any other pertinent data and decide whether further response is required.

Determining what data have been compromised or potentially compromised is vital to making an accurate risk assessment and charting an appropriate course of action.

As part of the initial evaluation, the following issues should be addressed:

- Date of breach incident.
- Nature of breach incident and the means by which the breach occurred:
  - Unauthorized access to information.
  - Unauthorized use of information.
  - Lost computer, storage device, or portable media.
  - System or network intrusion.
  - Loss of control of paper documents containing sensitive information.
- Person who reported breach incident.
- Person who discovered breach incident.
- Number of individuals potentially affected.
- The accessibility of the information.<sup>5</sup>

## **B. Management Review and Investigative Responsibilities**

- If an incident appears to involve the unintentional or negligent loss of control or disclosure of PII or Covered Information, the DCIO may have primary responsibility for undertaking a review. The DCIO shall promptly notify the IG if additional information becomes available that indicates the intentional loss of control or disclosure of PII or Covered Information.
- If an incident appears to involve the intentional or grossly negligent disclosure of PII or Covered Information or possible criminal activity, the IG will have responsibility for undertaking an investigation.
- If intent cannot be ascertained as part of the initial evaluation, the DCIO may have initial responsibility, in consultation with the IG, until intent can be determined.

## **VI. Identity Theft Risk Analysis**

To determine if a breach causes identity theft risks, the Breach Team should evaluate the factors identified in the 2006 OMB Memo. These factors include not only the type of Covered Information that was compromised, but also:

- How easy or difficult it would be for an unauthorized person to access the information given how it was protected;

---

<sup>5</sup> For example, the Breach Team will determine whether the information was properly encrypted or otherwise rendered unusable. The fact that information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals.

- The means by which the loss occurred, including whether the breach incident might be the result of criminal activity or is likely the result of criminal activity;
- The ability of the FEC to mitigate the identity theft; and
- Evidence that the compromised information is actually being used to commit identity theft.

## **VII. Analysis of Other Likely Harms**

Even if there is no risk of identity theft, consistent with the Privacy Act and the 2007 OMB Memo, in considering whether to notify consumers and others, the Breach Team shall consider a wide range of potential harms. These include risk of harm to reputation, embarrassment, inconvenience, unfairness, harassment, and prejudice, particularly when health or financial information is involved in the breach. Accordingly, the Breach Team will consider a wide variety of possible harms in determining whether external notification of a breach is necessary.

To determine the likely risk of harm caused by a breach when Covered Information is not involved and there is no risk of identity theft, the Breach Team will consider five factors as set forth in the 2007 OMB Memo:

- Nature and context of the data.<sup>6</sup>
- Number of individuals affected.
- Likelihood the information is accessible and usable.
- Likelihood the breach may lead to harm.
- Ability of the agency to mitigate the risk of harm.

## **VIII. Identity Theft Response**

If the Breach Team determines that there is a risk of identity theft from a breach of Covered Information, the Breach Team should develop a response plan to mitigate such risk. In developing such a plan, the Breach Team should consider the options available to agencies and individuals to protect potential victims of identity theft as set forth in the 2006 OMB Memo.

For individuals, these options include:

- Contacting financial institutions.
- Monitoring financial account activity.
- Requesting a free credit report.
- Placing an initial fraud alert on credit reports.

---

<sup>6</sup> For example, if an office Rolodex contained PII (name, address, telephone number, etc.), the information probably would not be considered sensitive and the breach of this information would not warrant further action. In contrast, if a list of retirees contained employee social security numbers and birth dates, the information likely would be considered sensitive and breach of this information would justify further action. In assessing the levels of risk of harm, the Breach Team therefore will consider the data elements in light of their context and the broad range of potential harms resulting from the disclosure to unauthorized individuals.

- For residents of states in which it is authorized under state law, considering placing a freeze on their credit file.
- For deployed members of the military, considering placing an active duty alert on their credit file.
- Reviewing resources at [www.idtheft.gov](http://www.idtheft.gov).

For the FEC, these options include:

- Engaging a third party to conduct a data breach analysis to determine whether a particular data loss appears to be resulting in identity theft<sup>7</sup>;
- Providing credit-monitoring services if the Breach Team has determined that such services are required to mitigate potential damage due to the breach.<sup>8</sup>

## **IX. Notification of Individuals**

If the Breach Team, applying the criteria set forth in the 2006 and 2007 OMB Memoranda, determines that (1) an unauthorized person has accessed Covered Information and that the information could be used for fraudulent purposes, or (2) an unauthorized person has accessed PII and its use is likely to lead to harm, then the affected individuals will be notified. This notice will be provided without unreasonable delay but no later than 45 days after the determination is made, except in extraordinary circumstances.

In determining the timing and content of the notice, the Breach Team will consult with the IG or other law enforcement officials investigating the breach incident before making any public disclosures about the breach incident.

The Breach Team will consider the following elements in the notification process:

- Timing of the notice.
- Source of the notice.
- Contents of the notice.
- Means of notification.
- Preparation needed for follow-on inquiries.

---

<sup>7</sup> One such third party conducted a data breach analysis for the Department of Veterans Affairs May 2006 data breach potentially involving 17.5 million veterans.

<sup>8</sup> The Breach Team should follow the recommendations set forth in the 2006 OMB Memo. If a decision is made to retain monitoring services, the Breach Team should consult the OMB Memorandum regarding “Use of Commercial Credit Monitoring Services Blanket Purchase Agreements,” issued on December 22, 2006, and available at <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-04.pdf>. A decision to retain credit-monitoring services will be made only after a careful balancing of likely harms and likely costs. Moreover, the Chief Financial Officer must be consulted before a decision to retain monitoring services is made.

These elements shall be analyzed in accordance with guidance set forth in the OMB Memoranda. In particular, the contents of any notice given by the agency to individuals shall include the following:

- A brief description of what happened;
- To the extent possible, a description of the types of information that were involved in the breach. A brief description of what the agency is doing to investigate the breach, mitigate losses, and protect against further breaches;
- Point-of-contact information for individuals who have questions or need more information, including a toll-free number, Web site, and/or postal address; and
- If the breach involved Covered Information, steps for individuals to undertake in order to protect themselves from the risk of identity theft, including how to take advantage of credit monitoring or other service(s) that the agency intends to offer, if any, and URL information for the Federal Election Commission's Web site, including specific relevant publications.

## **X. Notification to Third Parties**

Notice to individuals and notice to third parties, including the timing, order, and content of such notice, shall be carefully coordinated so that ongoing investigations are not compromised, the risk of harm to individuals is minimized, and the information provided is consistent and accurate. Notice to the following third parties may be considered depending on the nature of the breach:

**A. Law Enforcement.** Depending on the nature of the breach, it may be appropriate for the Breach Team, the FEC Information System Security Officer, FEC Physical Security Officer and/or the IG, to notify federal, state or local law enforcement, including local police departments, the Federal Protective Service and the Federal Bureau of Investigation.

**B. United States Computer Emergency Readiness Team (US-CERT).** OMB guidance requiring reporting to US-CERT is derived from FISMA from which the Commission is exempt. However, in the event of an actual breach, or strong suspicion of a breach, the DCIO and SAOP would report the breach incident to US-CERT as a matter of "best practice" and to facilitate our obtaining whatever law enforcement assistance might be necessary.

**C. Media and the Public.** The Press Officer, in coordination with the Breach Team, is responsible for conducting all meetings and discussions with the news media and public about a breach or suspected breach. This includes the issuance of press releases and related materials on the Commission's web site [www.FEC.gov](http://www.FEC.gov).

**D. Financial Institutions.** If the breach involves government-authorized credit cards, the FEC must notify the issuing bank promptly as set forth in the 2007 OMB Memo. The Chief Financial Officer or the Administrative Services Manager shall coordinate with the Breach Team regarding such notification and suspension of the account. If the breach involves individuals' bank account numbers that are used in employment-related transactions (e.g., payroll), the FEC will notify the bank or other entity that handles that particular transaction for the agency.

**E. Appropriate Members of Congress.** The Office of Communications, in consultation with the Breach Team, is responsible for coordinating all communications and meetings with members of Congress and their staff. The Breach Team will notify the Press Officer immediately when an issue arises that may require communications with members of Congress and their staff.

**F. Attorney General.** The IG shall promptly notify the Attorney General of any criminal violations relating to the disclosure or use of Covered Information or PII, as required by the Inspector General Act of 1978, as amended.

## **XI. Documentation of Breach Notification Response**

As appropriate, the Breach Team shall document responses to breaches for the purpose of tracking the Breach Team handling and disposition of specific breaches. The Breach Team, in coordination with any other appropriate officials and staff shall ensure that appropriate and adequate records are maintained to document the Breach Team response to all breaches reported under this plan. In accordance with the Privacy Act of 1974 and the Federal Records Act, such records shall be generated, compiled and maintained in a manner sufficient to safeguard the financial, legal or other rights of individuals, if any, affected by the breach, including any parallel law enforcement investigations, litigation, or other pending action. At the same time, such documentation shall be maintained no longer than required by applicable records retention schedules to ensure that any sensitive PII in such records is not unnecessarily retained or exposed to a risk of breach. Such records shall be destroyed only in accordance with approved and secure methods designed to ensure against inadvertent disclosure, theft or other compromise of personal or other nonpublic information.

## **XII. Evaluation of Breach Response**

The development and implementation of this plan for responding to breaches of personally identifiable information is an ongoing process, not a one-time exercise. Accordingly, following the handling and disposition of all suspected or actual breaches reported under this plan, the Breach Team will evaluate the Breach Team's response and identify tasks that could have been conducted more effectively and efficiently and make improvements or modifications to the plan as appropriate.