Federal Election Commission

Office of Inspector General

Review of Outstanding Recommendations as of February 2017

March 2017

Assignment No. OIG-16-04

Office of Inspector General's Review of Outstanding Recommendations as of February 2017

The Office of Inspector General (OIG) semiannually provides to the Federal Election Commission (FEC) a report on the status of outstanding recommendations. The OIG provides these status reports as of February and August of each year. For this reporting period, we continued our review of the previous six audits and inspections that were outstanding as of August 2016, and added the *Audit of the FEC's Telework Programs,* as its recommendations have been outstanding for more than six months since the release date of the report. Based on the results of the audit follow-up review, the OIG was able to close 16 outstanding recommendations from three separate OIG reports.

As part of the OIG's follow-up review, a formal recommendation resolution process can be initiated at the discretion of the OIG if there are outstanding recommendations that management has not agreed to implement over a period of time. The resolution process can include:

a) management signing a *Risk Acceptance Memorandum*, or
b) the OIG presenting the issue(s) to the Commission to determine if management must comply with the OIG's recommendation, or corrective action is not required.

During this review period, the OIG concluded that a formal recommendation resolution was necessary for 13 recommendations collectively from the *Follow-up Audit of Privacy and Data Protection* (Privacy Audit) and the *Continuity of Operations Plan Inspection* (COOP Inspection) that management has not agreed to sufficiently implement since the release of both reports. The OIG provided a *Management Risk Acceptance Memorandum* dated December 19, 2016 to the Co-Senior Agency Officials for Privacy (Co-SAOP) and the Chief Information Officer (CIO) that included an assessment of the 13 recommendations and any potential risks to the agency if not sufficiently implemented. The OIG requested within the memorandum that management provide the OIG with:

1) an official signed memorandum accepting the identified risks if there were no planned corrective actions from management to address the recommendation;
2) an updated corrective action plan (CAP) if management has decided to implement any of the recommendations, or
3) supporting documentation if management believes corrective action has already been implemented to address the recommendation(s).

In response to the OIG's *Management Risk Acceptance Memorandum,* a signed memorandum was provided from the Co-SAOP on January 23, 2017, and a signed memorandum from the CIO on January 25, 2017. The OIG responded to the Co-SAOP and CIO in a memorandum dated March 21, 2017 confirming the resolution of the 13 recommendations based on the signed memorandums and follow-up discussions with management. *(See attachment).* In summary, the recommendation resolution process via the *Management Risk Acceptance Memorandum* closed 11 of the 13 assessed recommendations, as management agreed to implement 2 of the 13.

Therefore, the OIG's normal recommendation follow-up process for the seven OIG reports and the recommendations included in the *Management Risk Acceptance Memorandum* collectively had a total of 86 outstanding recommendations. Based on the two separate reviews and various assessments, a total of 27 recommendations were closed, leaving 59 recommendations open as of February 2017. (See table on page 3).

Noteworthy Accomplishments

In the short time the agency's new Chief Information Security Officer (CISO) has been onboard, the OIG has noted that progress is being made with the agency's information technology security program in areas that address the OIG's report containing the highest number of outstanding recommendations, the *COOP Inspection*. In the past, management has made very little progress in addressing these findings since the release date of the report. However, during this current review period, information has been readily provided by the CISO to the OIG to support corrective actions being made, and the CISO has shown a willingness to work with the OIG in resolving outstanding issues. The OIG greatly appreciates this open collaboration and hopes for a continued cooperative working relationship as the responsibilities of the agency's COOP is being transitioned to the Acting Chief Information Officer for Operations.

OIG Concerns

The overarching concern of the OIG is the lack of governance accountability for ensuring that outstanding recommendations that are intended to improve agency programs and prevent fraud, waste, and abuse are timely and sufficiently implemented by management. Many recommendations have been outstanding for five or more years, with no consistent progress or dedicated effort from management to implement corrective actions.

Based on past practices, the OIG is concerned that management does not use its resources efficiently by often addressing risks only after the agency's weaknesses have been exposed. The OIG believes management should have more preventive measures established within their business processes, as applicable, to adequately address the potential risk exposures to the agency. Governance must make management accountable for promptly addressing these outstanding recommendations to decrease the risk exposure, effectively manage resources, and control cost.

Table Summary of Results

The table below summarizes the progress made by FEC management since the OIG's last reporting period and the total outstanding recommendations as of February 2017.

Title & Report Date of OIG Audits/Inspection	*Total Outstanding Recommendations as of August 2016*	*Total Closed*	*Total Open as of February 2017*[1]
Audit of the Commission's Property Management Controls (3/2010)	1	0	1
2010 Follow-up Audit of Privacy and Data Protection (3/2011)	28	3[2]	25
2010 Follow-up Audit of Procurement and Contract Management (6/2011)	1	0	1
Inspection of the FEC's Disaster Recovery Plan and Continuity of Operations Plans (1/2013)	29	19[3]	10
Audit of the FEC's Office of Human Resources (7/2013)	8	0	8
Inspection of FEC's Compliance with FMFIA/OMB A-123 (6/2014)	8	3	5
Audit of the FEC Telework Programs (6/2016)	11	2	9
Total Outstanding Recommendations			59

[1] Column numbers may include recommendations that management has disagreed with or has not adequately implemented, and the OIG concludes that these recommendations are still open.

[2] All three recommendations were closed due to management's acceptance of risk and included in the *Management Risk Acceptance Memorandum*.

[3] The 19 recommendations reflect those closed from the audit follow-up review (11) and the *Management Risk Acceptance Memorandum* (8). The 19 closed recommendations include:

- 4 verified as sufficiently implemented by the OIG;
- 7 no longer applicable due to changes in business processes;
- 6 repeat findings from the annual financial statement audit where follow-up will be conducted, and
- 2 closed due to management's acceptance of risk.

Closed Audits/Inspections[4]

The OIG did not close any audits or inspections this review period.

Open Audits/Inspections

A. Audit of the Commission's Property Management Controls

The remaining outstanding recommendation for the *Audit of the Commission's Property Management Controls* is related to the Office of the Chief Information Officer's (OCIO) inventory records for cellular devices. For the past two review periods, the OIG deferred follow-up on this open item since management was in the process of providing staff with new devices. As OCIO completed the distribution of the new iPhone 6 devices to all appropriate employees prior to the start of this review period, the OIG commenced with a review of the OCIO's inventory records.

According to the Acting Deputy CIO of Operations, the agency is currently being enrolled in a new Apple program which requires AT&T to make changes to the agency's account. Therefore, the OIG planned to assess OCIO's records based on internal Office of Human Resources (OHR) records and physical verifications. The OIG reviewed agency records to ensure that no separated employees were still listed on the inventory list as having a device, and that the physical device was placed in storage or issued to another employee. This review noted two instances that separated employees were still listed on the inventory list. The OIG attempted to continue this review by conducting a physical test to verify that all devices listed as storage (devices on-hand), to include the devices listed to the separated employees, could be accounted for; however, the OIG was not able to complete this review due to the unavailability of the OCIO staff to produce the devices. Therefore, this recommendation remains open.

B. 2010 Follow-up Audit of Privacy and Data Protection

For the *2010 Follow-up Audit of Privacy and Data Protection*, the OIG's *Review of Outstanding Recommendations as of August 2016* report identified 28 open recommendations. The OIG followed up with the Privacy Team regarding 24 of the 28

[4] An audit or inspection is closed when the OIG determines that all applicable recommendations have been adequately addressed by management.

outstanding recommendations that management agreed to implement.[5] The Privacy Team responded to the OIG, noting that in accordance with their records, they "...have completed, and therefore consider no longer applicable, 15 of the 24 cited recommendations..." and at the discretion of the Co-Chief Privacy Officers, "...the Privacy Team does not intend to perform any additional work on the 15 recommendations... " In addition, the Privacy Team stated that they would assume the risk of not implementing five of the recommendations, but will implement the remaining four recommendations by May 2017.

The OIG responded to the Privacy Team, explaining that the 15 recommendations they consider closed will remain open, as management has not provided the OIG with sufficient evidence during our follow-up reviews that these recommendations have been implemented. The OIG clarified that the official resolution of recommendations (open/closed) is determined by the OIG. In addition, we clarified that the type of resolution for outstanding recommendations is also determined by the OIG. Therefore, management's notation of their risk acceptance for five of the outstanding recommendations is not applicable to this follow-up review process, and they will also remain open. For the four recommendations that management intends to implement by May 2017, the OIG will defer any follow-up until the next review period when these recommendations are anticipated to be closed. Thus, the 24 recommendations for review during this follow-up period remain open.

As additional information, the OIG suggested that a meeting be scheduled with the OIG, Co-Chief Privacy Officers, and the Privacy Team to address the current status of the Privacy Audit's recommendations and to ensure that all parties are clear on the OIG's follow-up process. Management has agreed to this meeting suggestion and the meeting is tentatively scheduled for March 2017.

C. 2010 Follow-up Audit of Procurement and Contract Management

The *2010 Follow-up Audit of Procurement and Contract Management* was issued in June 2011. The OIG's *Review of Outstanding Recommendations as of August 2016* report identified only one open recommendation related to the updated Directive 66, which is the overarching agency-wide policy for procurement and acquisitions. This one recommendation is still open for this follow-up review period.

[5] The remaining four recommendations were included in the OIG's *Management Acceptance Risk Memorandum* as recommendations that management has not agreed to implement. The detailed assessment of those four recommendations are included in the memorandum attached with this report, and the numbers in the *Table Summary of Results* on page 3 of this report are reflective of this assessment.

D. Inspection of the FEC's Disaster Recovery Plan and Continuity of Operations Plans

The *Inspection of the FEC's Disaster Recovery Plan and Continuity of Operations Plans* (COOP) report was released in January 2013. The OIG's *Review of Outstanding Recommendations as of August 2016* report identified 29 outstanding recommendations, and for this review period, the OIG conducted follow-up on 20 of the 29 recommendations.[6]

The OIG and OCIO staff held a meeting on February 9, 2017, to discuss the status of the open COOP Inspection recommendations. During this meeting, the CISO provided the OIG with documents in support of actions that have been completed by management and noted instances where progress is being made to sufficiently close the open recommendations related to the IT security portions of the COOP. In addition, the Acting Deputy CIO of Operations noted tasks and plans of actions to address recommendations related directly to the agency's COOP process. Management also provided an updated CAP to the OIG with updates and revised implementation dates. Based on this meeting, the documentation provided, and the updated CAP, the OIG was able to close 11 outstanding recommendations:

- 4 recommendations were closed based on evidence reviewed that corrective actions had been successfully implemented;
- 3 recommendations management previously agreed to implement are no longer applicable due to process changes; and
- 4 recommendations were closed and forwarded to be included in the annual financial statement audit, where similar recommendations are reported.

The remaining nine recommendations are still open. However, management has noted in their CAP an intended plan of action to implement these recommendations with many completion dates estimated for the 3rd quarter of 2017.

E. Audit of the FEC's Office of Human Resources

The *Audit of the Federal Election Commission's Office of Human Resources* report was issued in July 2013. The OIG's *Review of Outstanding Recommendations as of August 2016* report identified eight open recommendations for the OHR audit report.

In February 2017, the OIG met with the Director of OHR to discuss the status of the eight outstanding audit recommendations as well as review corrective actions since the last

[6] The remaining nine recommendations were included in the OIG's *Management Acceptance Risk Memorandum* as recommendations that management has not agreed to implement. The detailed assessment of those nine recommendations are included in the memorandum attached with this report, and the numbers in the *Table Summary of Results* on page 3 of this report are reflective of this assessment.

follow-up review was conducted in August 2016. Based on follow-up work performed, no open recommendations can be closed at this time. However, OIG notes that progress was made on Recommendation 16 related to the electronic fingerprinting scheduling process. The OHR informed the OIG that it has completed a pilot of an on-line electronic scheduling system (Timetrade). OHR is currently working with the procurement office to purchase the Timetrade web-based software, which will be used to electronically schedule both fingerprinting and badging appointments. Also, the OIG was informed that OCIO is looking into an on-line correspondence tracking system called Service Now which could potentially replace HR On Demand, which is currently used to track and monitor HR inquiries.

Once these systems have been fully implemented, the OIG will confirm if they are operating effectively before the related recommendations can be closed. As a result, the OHR audit still has eight open audit recommendations for this follow-up review period.

F. Inspection of FEC's Compliance with FMFIA/OMB Circular A-123

The *Inspection of FEC's Compliance with FMFIA/OMB Circular A-123* (A-123 Inspection*)* was released in June 2014. The OIG's *Review of Outstanding Recommendations as of August 2016* report identified eight open recommendations for the A-123 Inspection report. Since the August 2016 follow-up review period, the Office of the Chief Financial Officer (OCFO) in cooperation with the FEC A-123, Task Force finalized and rolled out the new annual internal control review (ICR) procedures and template to comply with the new OMB A-123 guidance. All of the designated program managers for FY 2016 have been trained, and all program offices completed the new ICR documentation.

The OIG reviewed the FY 2016 ICR documentation submitted to the OCFO and concludes that the control assessment template was completed for all program offices. However, the OIG notes that several program offices' ICR documentation did not contain adequate information to comply with the new A-123 requirements, specifically as it relates to risk associated with potential and/or known control issues. The OIG acknowledges that this is a new process and believes that additional training may be needed especially since there are additional A-123 requirements that go into effect in FY 2017, which are discussed in more detail below.

The final A-123 guidance (*Management's Responsibility for Enterprise Risk Management and Internal Control*),which was released on July 15, 2016, requires all executive branch agencies to adopt an Enterprise Risk Management (ERM) approach as well as a plan for complying with *the Fraud Reduction and Data Analytics Act of 2015* (the Fraud Reduction Act of 2015).

According to the final A-123 guidance, all executive branch agencies are required to:

- develop ERM and Fraud Reduction implementation plans by June 4, 2017;
- create a formal risk profile; and
- perform periodic risk assessments in order to properly manage risk.

Per discussion with OCFO, Management plans to implement and leverage the work done by the A-123 Task Force which includes finalizing and formally adopting the Senior Management Council charter which will be the designated oversight body responsible for the FEC's internal control and ERM programs.

Although major progress was made during this review period, the OIG was only able to close three of the eight recommendations. In light of the additional A-123 requirements that go into effect in FY 2017, the OIG cannot close the remaining five recommendations until the FEC incorporates ERM and fraud risk assessments into the ICR process and the OIG can verify that the new processes are operating effectively. Therefore, five recommendations remain open for this follow-up review period.

G. Audit of the FEC's Telework Programs

The *Audit of the FEC's Telework Programs* (Telework Audit) was released in June 2016. The Telework Audit report identified eleven recommendations. This is the first follow-up for the Telework Audit. In February 2017, the OIG met with the Telework Management Official (TMO) to discuss the updated CAP and the OIG's request for supporting documentation needed to close some of the recommendations. Based on our follow-up work and review of documentation submitted, the OIG closed two recommendations. The other nine outstanding recommendations will remain open until the annual telework monitoring procedures have been fully implemented, related policies and procedures have been revised/created, and the requirements of the telework programs have been reinforced. Therefore, nine recommendations remain open for this follow-up review period.

Background

As required by the Inspector General Act of 1978, as amended, the OIG is responsible for conducting audits of the FEC's programs and operations. In addition to conducting and supervising audits, the OIG also has the responsibility to conduct audit follow-ups to ensure that management has effectively implemented OIG recommendations. Audit follow-up, including the timely implementation of audit recommendations by FEC management, is required by Office of Management and Budget Circular A-50, *Audit Follow-up*, as revised, and FEC Directive 50: *Audit Follow-up.*

At the conclusion of each OIG audit and inspection, it is management's responsibility to develop a corrective action plan (CAP). The CAP identifies the plan management has developed to address the OIG's findings and recommendations. The CAP should detail the following:

1. assignment of Audit Follow-up Official, who is responsible for overseeing the corrective action;
2. OIG finding(s);
3. OIG recommendation(s);
4. detailed corrective action to implement the OIG's recommendation(s);
5. FEC staff person with responsibility to implement each task; and
6. expected completion dates.

Once management drafts the CAP, the OIG then reviews the CAP and provides comments to management regarding the sufficiency of their planned corrective actions to address the OIG's findings. Management reviews the OIG's comments, finalizes the CAP, and then provides the final CAP to the Commission with a courtesy copy to the OIG.

FEC Directive 50 requires management to:

> *(3) Conduct regular meetings with the Inspector General throughout the year to follow-up on outstanding findings and recommendations, and include reports of these meetings in the written corrective action plan and semi-annual reports required to be presented to the Commission...;*

In order to work effectively with FEC management in adhering to FEC Directive 50, and to ensure continuous monitoring and adequate and timely audit resolution, the OIG communicates with management at least semiannually to discuss the status of outstanding OIG recommendations. If management has implemented any corrective action(s), the OIG schedules a meeting with management to discuss the implementation of the corrective action(s), and the OIG then reviews evidence of the corrective action (i.e., new/updated policies, procedures, and processes to improve internal controls).

To provide management with timely feedback and the results of our review prior to management's reporting deadlines to the Commission in May and November, the OIG reports on our review of outstanding recommendations as of February and August of each year. The semiannual meetings are also intended to assist the audit follow-up official in following provisions 4 through 6 of Directive 50, which are listed as follows:

> *(4) Respond in a timely manner to all audit reports;*
> *(5) Engage in a good faith effort to resolve all disagreements; and*
> *(6) Produce semi-annual reports that are submitted to the agency head.*

The official status (open/closed) of OIG recommendations is determined by the OIG once the OIG has verified that management has adequately implemented the corrective actions. The Inspector General can also make a decision to close recommendations or seek resolution from the Commission for recommendations where the OIG and management disagree. Lastly, the number of outstanding recommendations is also reported to the Commission and Congress in the OIG's Semiannual Reports to Congress.

ATTACHMENT

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

MEMORANDUM

TO: Alec Palmer
Staff Director\Chief Information Officer

Gregory Baker
Deputy General Counsel\Co-Chief Privacy Officer

Edward Holder
Deputy Staff Director Office for Management and
Administration\Co-Chief Privacy Officer

FROM: J. Cameron Thurber
Deputy Inspector General

SUBJECT: Management Risk Acceptance and Recommendations Resolution

DATE: March 21, 2017

In a memorandum dated December 19, 2016, the Office of Inspector General (OIG) identified 13 open recommendations collectively from the *2010 Follow-up Audit of Privacy and Data Protection* (Privacy Audit) and the *Inspection of the Federal Election Commission's Disaster Recovery Plan and Continuity of Operations Plans* (COOP Inspection) that management has neither concurred with nor agreed to implement. The memorandum also noted that:

(a) 4 of the 13 recommendations were no longer applicable due to a change in agency processes and
(b) 2 of the 13 recommendations are repeat recommendations from the agency's annual financial statement audit.

These six recommendations were all from the COOP Inspection and were closed by the OIG in accordance with the December 19th memorandum. The seven remaining recommendations required confirmation of risk acceptance from management.

The OIG requested that management provide a memorandum signed by the Co-Chief Privacy Officers for the four Privacy Audit recommendations and a memorandum from the Chief Information Officer (CIO) for the (3) COOP Inspection recommendations accepting the risk of not implementing the unresolved IG recommendations. Upon receipt of the signed memorandums, the OIG agreed to close the recommendations, noting that management has accepted the potential risks.

In addition, the OIG also noted that if management decided to implement any or all of the seven recommendations after review, or management believes actions have already been implemented to address a recommendation, to provide the OIG with an updated corrective action plan (CAP) containing the intended or implemented plan of action for the OIG's review.

Based on the signed memorandums and follow-up discussions with management, the OIG has resolved the seven audit recommendations as detailed below:

<u>Privacy Audit Recommendations</u>

1. Record all mobile computing devices in inventory when received.

   - **Risk:** *Fraud- Theft of agency IT equipment*

     - ➢ If devices are not logged into inventory until distributed, rather than when received, there is a high likelihood that theft could occur without detection from management because there is no official system record of the purchased inventory until the equipment has been distributed to staff. Management's process to hand-count the equipment when received would not prevent this risk of fraud from occurring.

   - **OIG Resolution** (Closed – *Management accepts risk*)

     - ➢ The Acting Deputy CIO of Operations noted that the Office of the Chief Information Officer's (OCIO) process for recording inventory when received is to keep a scanned copy of the packing slip on the server that includes the detailed information of each computer device purchased and shipped after the OCIO staff member completes a physical inventory count of the shipment. The OIG verified that packing slips were maintained by the OCIO; however, there were no signatures or sign-off indications from the person who conducted the physical inventory count to affirm all devices purchased were received. Although we acknowledge that a process is in place, the OIG does not feel the OCIO's process is the most efficient. In an effort to enhance the OICO's process for internal control purposes, the OIG suggested that the OCIO require its staff member conducting the physical inventory count to sign the packing slip they are maintaining as their official record of devices received to strengthen this verification process. OCIO management did not concur with the suggested added control procedure. Based on the OIG's assessment of OCIO's overall process for recording inventory, the OIG will defer to management's response in the CIO's memo and close this item based on management accepting the stated risks.

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

- **Risk:** *Unauthorized access to PII and/or agency confidential information*

  - If management has no physical system record of what devices are encrypted, there is a high likelihood that employees could have laptops/tablets that are exposed to hackers when connected to networks outside of the agency via Wi-Fi connections used for business travel and/or home networks used for Telework purposes. In addition, if a device is lost or stolen, agency information would be easily accessible to the public. During deployment of new laptops, OCIO consistently experienced instances where the encryption may not work/install properly on a device while in use by the employee, leaving the device vulnerable while still in the employee's possession.

  - In past audit follow-up reviews, management has attempted to use their written policy that all devices must be encrypted to satisfy this recommendation; however, a written policy alone cannot provide management with confirmation that all devices distributed to staff have been properly encrypted, or ensure that instances of encryption failure have been properly and timely resolved.

- **OIG Resolution:** (Open – *pending further documentation*)

  - The OIG verified that OCIO now has the capability to capture the data to verify that computer devices are encrypted, and the OIG reviewed the SQL database report for encrypted computer devices. The OIG noted that all computer devices distributed to FEC staff are not included in the report, as many of the FEC staff have not been issued new computers with the new encryption software. The CIO initially disagreed with the portion of the recommendation which recommends that the verification of encryption should be included on the inventory list. Although the OCIO disagrees with keeping the encryption data in the inventory list, the fact that OCIO now has the capability to capture this pertinent information, even as a separate report, is sufficient to resolve the OIG's audit finding. The OCIO anticipates all staff will be provided with new laptops by the next OIG follow-up review; therefore, the OIG will defer closing this recommendation until a full encryption report can be produced for verification that all laptops are properly encrypted.

3. Assign privacy roles and responsibilities to one individual Chief Privacy Officer (CPO) with high level sponsorship in the Commission. If the Commission decides to continue with two CPOs and SAOPs [Senior Agency Officials for Privacy], roles and responsibilities under these titles should be clearly delineated between individuals sharing the positions.

   - **Risk:** *Non-compliance with the Privacy Act of 1974*

     ➢ The agency lacks sufficient accountability over the Privacy Program to ensure that the agency is continuously in compliance with federal requirements regarding privacy laws. The established oversight structure of the program is ineffective as privacy issues and weaknesses identified approximately nine years ago are still outstanding.[1] Without one person being solely responsible for the overall compliance of the Privacy Program, the shared responsibilities of oversight and execution of privacy tasks will continue to cause the agency to be delayed in meeting federal requirements, deadlines, and keeping up to date with the changes to privacy laws.

   - **OIG Resolution:** (Closed – *Management accepts risk*)

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

   - **Risk:** *Unauthorized access to confidential information*

     ➢ Detailed procedures for classifying and labeling sensitive information (paper and electronic formats) has not been formally established at the agency. Without a clear established policy, the agency's and employees' confidential information has the potential to be mishandled within and outside the agency.

     ➢ In addition, according to management's current status for the Privacy Audit CAP, management has yet to complete all phases of

[1] The OIG's 2007 Performance Audit of Privacy and Data Protection was released December 2007 and all open recommendations were reported again in the OIG's follow-up audit (Privacy Audit) in 2010.

an assessment resulting from a May 2009 contract[2] to comply with OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information.*

Thus, the agency has not been fully compliant with this requirement for approximately seven years.

- ➢ OIG has noted instances where Office of Human Resources documents have been provided to our office during the hiring process with applicants Social Security Numbers visible although not needed for the evaluation and interview process.

- **OIG Resolution:** (Closed – *Management accepts risk*)

COOP Inspection Recommendations

5. We recommend that COOP/DRP training is provided at least annually. Personnel newly appointed to COOP roles should receive training shortly thereafter joining the FEC if training has already been conducted for the year.

   - **Risk:** *Non-compliance with Department of Homeland Security, Federal Continuity Directive 1, Federal Executive Branch National Continuity Program and Requirements*

     - ➢ The OIG notes that the agency's COOP process has changed since the release of the report; however, adequate agency training still must be conducted on an annual basis regardless of the agency's process. Since management has decided to use Telework for their COOP program, the Telework policy can be executed differently within the different offices and divisions, and noting that all mission essential personnel may not be participating in a regular telework schedule, the COOP Coordinator should conduct annual mandatory training for all designated mission essential personnel to ensure they are able to carry-out their mission duties in the event of a local disaster. Annual training would ensure that the correct

[2] OCIO contracted with Solutions Technology Systems, Inc., to conduct an inventory of FEC systems that contain personally identifiable information and provide a report with recommendations to enhance the protection of PII in both paper and electronic form.

mission essential personnel are identified; they are aware of their responsibilities; computer equipment is working properly; and the necessary software, applications, etc., to conduct agency business has been provided.

- ➢ Thus far, management has only conducted COOP testing which was initiated in September 2015. Upon review, the testing was found inadequate to comply with federal requirements. The COOP testing conducted was voluntary rather than mandatory, and all mission essential personnel were not equipped with the proper computer equipment to validate they were able to conduct normal business functions as designed. In addition, this testing did not include the transition from the production servers to the disaster recovery servers to ensure the recovery of server data in the event of a disaster. In order to conduct annual COOP training for mission essential personnel, the COOP must first be sufficiently tested to ensure it's working as intended prior to training.

- **OIG Resolution:** (Open – *Management has concurred with the recommendation*)

  - ➢ Per management's signed memorandum: *Management concurs and will provide online Skillport training to staff designated as COOP personnel to identify expectations and procedures. Current COOP personnel will be required to complete said training course by 3rd quarter 2017 and annually thereafter.*

  - ➢ OIG will follow-up on this recommendation after the anticipated completion date of training.

6. Develop and implement a COOP exercise plan. The functional exercise should include all COOP points of contact and be facilitated by the system owner or responsible authority. Exercise procedures should be developed to include an element of system recovery from backup media.

   - **Risk:** *Non-compliance with Department of Homeland Security, Federal Continuity Directive 1, Federal Executive Branch National Continuity Program and Requirements*

     - ➢ The OIG notes that the agency's COOP process has changed since the release of the report; however, the requirement of an exercise plan to be performed is still applicable to the FEC's process. If an exercise plan is not executed at least annually to test the continued capability of system recovery, the agency is at risk of not being able to recover the necessary data from the primary site to the alternate work site in the event of a local disaster. In addition, as personnel and responsibilities often change, the COOP coordinator should conduct testing to ensure that all responsible parties are aware of their duties and responsibilities during such an event.

- **OIG Resolution:** (Closed – *Management accepts risk)*

  - ➢ After receipt of management's signed memo that concurred with this recommendation, the OIG met with the OCIO staff on February 9, 2017, to discuss outstanding recommendations for the

    COOP Inspection follow-up. During this meeting, management noted that they disagreed with this recommendation, and the Deputy CIO for Operations followed up with the OIG in an email stating, "Management does not believe a yearly test of the COOP is required."

  - ➢ The OIG believes a COOP exercise plan is still relevant as everyone who is a point of contact for COOP is not necessarily a participant in the telework program (which is used as the agency's COOP process), or has a normal telework schedule based on different office or division implementation of the program. In addition, not everyone who participates in the telework program uses their tablet (which was purchased for COOP purposes) when working from home, which means their laptop is not always at their telework location for immediate use in the event of a COOP situation. An annual test exercise for COOP participants would ensure that all participants can access the necessary software, applications, etc. needed for regular business operations (as these change, update, or increase over time) and ensure all tablets are working properly for those who don't use them on a regular basis in the event of an emergency where we would need to follow the COOP process. Based on this assessment, the OIG will close this recommendation based on management's acceptance of the risk.

7. Review and obtain another alternative for the disaster recovery site or primary data site to ensure that the new facility is located in a geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure).

- **Risk:** *Non-compliance with Department of Homeland Security, Federal Continuity Directive 1, Federal Executive Branch National Continuity Program and Requirements*

  - Federal requirements applicable to the FEC state: "*Alternate operating facilities must be located in an area where disruption to the agency's ability to initiate, maintain, and terminate operations is minimized.*" However, the agency is not in full compliance with this requirement, as the primary data site (production site) and the alternate disaster recovery site that houses the backup servers are in the same geographical location.

  - In the event of a disaster (power outages, flooding etc.) effecting the agency's primary data site, there is a high likelihood that the agency's alternate disaster recovery site will be effected as well.

    This risk would prevent the agency from utilizing the alternate data site for its intended purpose; to avoid an interruption in executing the agency's day to day operations when there has been a disruption to the primary data site.

- **OIG Resolution:** (Closed – *Management accepts risk*)

If you should have any questions regarding this memorandum, please feel free to contact Mia Forgy at extension 1317. Thank you.

cc: The Commission