Federal Election Commission

Office of Inspector General

Final Report

Review of Outstanding Recommendations as of June 2014

July 2014

Assignment No. OIG-14-07

Office of Inspector General's Review of Outstanding Recommendations as of June 2014

The Office of Inspector General (OIG) semiannually provides to the Commission the status of outstanding recommendations. Since the December 2013 report was issued, we added the *Audit of the Federal Election Commission's Office of Human Resources* report (which was released in July 2013) to the audit follow-up process because the recommendations have been outstanding for more than six months. For this reporting period, we reviewed five audits and inspections that had a total of 102 recommendations outstanding. The OIG was able to collectively close fifteen (15) recommendations from three of the five audits and inspections. Three of the fifteen recommendations that were closed this period were closed due to management's decision to accept the risk of not implementing corrective actions for outstanding recommendations in the *Audit of the Commission Property Management Controls report*, see details on page 4.

Noteworthy Accomplishments

- The Office of Human Resources closed nine (9) of 26 audit recommendations from the *Audit of the Federal Election Commission's Office of Human Resources within the first six month follow-up period*.

OIG Concerns

- FEC needs to improve the accountability of management officials necessary to ensure compliance with all aspects of Directive 50: Audit Follow-up.

- FEC's IT inventory records are consistently inaccurate to include the recently purchased iPhones for FEC staff.

- OIG is concerned with the lack of progress in addressing the outstanding recommendations for the *Inspection of the FEC's Disaster Recovery Plan and Continuity of Operations Plan* report. Thirty recommendations were contained in the report, issued January 2013. Over eighteen months have passed and all thirty recommendations remain open. The lack of attention to these recommendations may put the agency at risk in the event of a local disaster.

Table Summary of Results

The table below summarizes the progress made by FEC management during the past six months and the outstanding recommendations as of June 2014.

Title & Report Date of OIG Audits/Inspection	***Total Outstanding Recommendations as of December 2013***	***Total Closed and Verified by OIG***	***[1]Total Open as of June 2014***
Audit of the Commission's Property Management Controls (3/2010)	7	5 [2]	2
2010 Follow-up Audit of Privacy and Data Protection (3/2011)	30	1	29
2010 Follow-up Audit of Procurement and Contract Management (6/2011)	9	0	9
Inspection of the FEC's Disaster Recovery Plan and Continuity of Operations Plans (1/2013)	30	0	30
Audit of the FEC's Office of Human Resources (7/2013)	26	9	17
Total Outstanding Recommendations			87

[1] "**Total Open as of June 2014**" column includes recommendations that management has disagreed with or has not adequately implemented, and the OIG concludes that these recommendations are still 'open'.
[2] Three (3) of the five (5) recommendations were closed based on management's decision to accept the risk of not implementing corrective action.

Audit Follow-up Meetings/Communications

Closed Audits

The Office of Inspector General did not close any audits for this review period.

Open Audits

A. Audit of the Commission's Property Management Controls

The Office of Inspector General (OIG) issued a memorandum to the Chief Information Officer (CIO) on February 10, 2014 (S*ee Appendix A*). The memorandum expressed the OIG's concern regarding the lack of progress in implementing the remaining seven open recommendations for the Audit of the FEC's Property Management Controls. The OIG's memo identified the potential risks to the agency and requested a written statement from the CIO accepting the risk of the outstanding recommendations in order for the OIG to officially close the recommendations.

In a memorandum dated March 4, 2014 (*See Appendix B),* the CIO provided a response to the OIG regarding the open recommendations. The OIG reviewed the responses and determined that:

- Three recommendations (1h, 3, 3e) will be closed based on management accepting the risk of not implementing corrective action to adequately address the recommendations
  - ***Recommendation 1h***: Document the ITD re-authorization process of PCD [personal communication device] users in ITD's Policy 58-4.4
  - ***Recommendation 3***: ITD should implement a form and process such as NIST Sample Sanitization Validation form, to record sanitization (wiping) of devices, disposal and/or destruction, as appropriate
  - ***Recommendation 3e***: Segregate the following program functions among three or more ITD staff: purchasing/ordering and recording assets; authorization for purchases, including devices received free under upgrade promotion; receipt. storage, and distributing of assets; and destruction or disposal of surplus PCDs;

- Two recommendations (1k & 2g) will be closed due to recent changes (January 2014) to the agency's policy to include details on personal use using the new iPhone devices and the required training provided to FEC staff when issued a device
  - ***Recommendation Ik***: Provide the policies and procedures for the use of Blackberry devices to all users when issuing the Blackberry

- ***Recommendation 2g***: Management should educate Blackberry users of all features that incur additional cost to the agency, such as: roaming charges that result when employees place calls outside the AT&T service areas; texting; directory assistance; unauthorized software, and voice use over the pooled plan limits*;* and

- Two recommendations (2a &2f) required follow-up review as the CIO noted that corrective action had been taken and no further actions were necessary, and requested that the recommendations be closed
  - ***Recommendation 2a***: All unassigned Blackberry devices should be suspended or service should be terminated if the device can not be immediately transferred to another user (no active spares kept in ITD).
  - ***Recommendation 2f***: Blackberry user information should be kept up to date and adjusted in a timely manner on the ITD master Blackberry listing and the AT&T Premier website for employee separations and new assignment of devices.

The OIG conducted our follow-up review on recommendations 2a & 2f and found that both recommendations were not adequately implemented. To review the detailed results of the follow-up review for recommendations 2a & 2f, please see the **Audit of the FEC's Property Management Controls Testing Results** section of this report of page 9.

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

For the *2010 Follow-up Audit of Privacy and Data Protection*, the OIG's December 2013 report identified 30 open recommendations. At the start of this review period, the OIG contacted the Co-Chief Privacy Officers to identify if any corrective actions had been implemented to address the thirty (30) outstanding recommendations. The OIG received confirmation from the Co-Chief Privacy Officers that no progress had been made**.**

In May 2014, an updated CAP was submitted to the Commissioners noting that one recommendation, 6g, had been implemented. Recommendation 6g requires management to "*Implement an alternative to assigning a generic laptop encryption passphrase to contractors so that every contractor has a unique self selected passphrase*". In order to verify implementation of this recommendation, the OIG inquired with seven (7)[3] FEC contractors that they have a self selected passphrase for logging on to their FEC issued laptops. Six (6) of the seven contractors verified that they created their own passphrase. For the one contractor, hired in 2014, the OIG verified that the contractor was using an FEC issued laptop for official FEC business, but their laptop was not encrypted, which would not require them to input a passphrase for accessing the FEC's laptop. Based on the six contractors with encryption, the OIG closed recommendation 6g.

[3] Three of the seven contractors work for the OIG on the FEC's annual financial statement audit.

However, FEC's policy is that **all laptops** issued to FEC employees **and contractors** are to be encrypted, which is also an outstanding recommendation (6a: "…require all mobile devices to be encrypted") for this audit. Since the release of this audit report in 2010, management has failed to provide the documentation necessary to evidence that ITD has the capabilities to verify that every laptop issued to an FEC employee or contractor has been encrypted. During the OIG's follow-up review in December 2011, the Deputy CIO of Operations sent an email stating that all laptops are encrypted and considered the email to be sufficient evidence to close the recommendation. The OIG does not consider a statement contained in an email adequate evidence or evidence of appropriate controls and documentation being in place. In addition, management's CAPs sent to the Commission since December 2011, to include the most recent CAP in May 2014, identified recommendation 6a as closed. Based on this follow-up review regarding the one contractor recently hired without an encrypted laptop and ITD's inability to provide sufficient evidence since 2010 that all laptops are encrypted illustrates that FEC is not following their policy and that recommendation 6a will remain open.

All laptops issued to contractors have not been encrypted and appropriate documentation on encryption of FEC laptops has yet to be provided.

C. 2010 Follow-up of Procurement and Contract Management

The December *2013 Review of Outstanding Recommendations* report noted eight (8) of 17 audit recommendations from the *2010 Follow-up Audit of Procurement and Contract Management* had been closed during that reporting period. Per discussion with the Office of the Chief Financial Officer (OCFO) in May 2014, no additional progress has been made related to the remaining 9 outstanding audit recommendations. OIG notes that since the last follow-up work performed, the procurement office lost one full time employee (FTE) and has a new Procurement Officer. The OIG did not perform any follow-up work during the reporting period ending June 30, 2014.

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 Inspection*) was released in January 2013. The OIG contacted the Deputy Chief Information Officer (CIO) of Operations to provide a status of the open recommendations. The Deputy CIO notified the OIG that there has been no change to the status of the thirty (30) outstanding recommendations.

The OIG reviewed management's May 2014 corrective action plan submitted to the Commission for the COOP Inspection and management stated that "*Due dates have been revised to coincide with the COOP plan update this year*." However, based on outstanding recommendations related to the COOP from the FEC's annual financial

statement audit, management currently does not have a project plan[4] in place to address the COOP findings and their updated due date of October 2014 for implementing corrective actions for the CAP is not reasonable and should be updated once a plan has been developed.

The OIG is concerned with the lack of progress and commitment by the Information Technology Division to address the numerous problems found during the COOP Inspection. In FY 2008, the agency procured contractors to develop the agency's COOPs and DRP. The OIG is aware that ITD is planning to **procure contract services for a second time** because ITD did not follow through with conducting proper testing and monitoring of the plans when they were completed by the contractors in FY 2010.

The agency spent $277,506 from 2008 to 2010 on ITD's COOP project which was never fully implemented. The agency is again spending funds to procure almost identical contract services while procuring more computer hardware to replace the previous Netbooks that were used for contingency planning. Although ITD is spending money towards developing the agency's COOP, ITD does not have a project plan in place to ensure key tasks and milestones to implement corrective actions for findings identified in the COOP Inspection will be achieved. In addition, without a project plan in place, management cannot properly manage the time, resources, and project cost to fully execute the COOP project. The OIG strongly believes without a proper COOP project plan, the agency is at risk for spending money on an IT project that will fail to achieve the project objective as in FY 2010.

FEC is at risk for spending contract money on COOP for the 2nd time and not completing the project objective.

Currently, the FEC is not in compliance with a required Presidential Directive: *Homeland Security Presidential Directive (HSPD-20), section 19(d)*[5]. In the event of a localized emergency or disaster to the FEC building (i.e. fire, flooding, etc.) the agency does not have an adequate plan in place or the necessary tools to ensure the agency can continue to carry out its mission.

FEC would be challenged in administering and enforcing **FECA** in the event of a local disaster.

[4] ***Project Plan***: a documented plan used to guide both project execution and project control; documents how and when a project's objectives are to be achieved by showing the major deliverables, milestones, activities and resources required on the project.

[5] "Heads of executive departments and agencies shall execute their respective department or agency COOP plans in response to a localized emergency and shall: (d) "Plan, conduct and support annual tests and training…"

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

The *Audit of the Federal Election Commission's Office of Human Resources* (OHR) *report* was issued in July 2013. The OHR audit report identified 26 audit recommendations to improve OHR operations. In March 2014, the OIG followed-up with the Acting Director of Human Resources to discuss corrective actions taken to address the recommendations. Then, the OIG reviewed the updated OHR CAP and requested supporting documentation required to close certain recommendations. Based on the OIG's review of documentation to support corrective actions by OHR, the OIG closed nine (9) of the 26 outstanding recommendations.

In June 2014, the OIG followed up with one of the OHR follow-up officials (OHR Supervisor) to determine if any additional progress has been made on OHR's outstanding audit recommendations. OIG was informed that due to the OHR work load, staff shortage, and the hiring of the new Director of OHR, no additional progress has been made since March 2014. Therefore, no additional follow-up work was performed by OIG. As of June 30, 2014 the OHR audit has 17 open audit recommendations.

Audit of the FEC's Property Management Controls Testing Results

The Chief Information Officer's (CIO) March 4, 2014 memorandum states that management now has direct access to the AT&T system to ensure changes to inventory records are accurate and made in a timely manner. Based on the OIG's review results, the inventory list for the new iPhones is not accurate and the AT&T system is still not properly managed to reflect an accurate record of assigned iPhones, even with the new direct access permitted to management. The lack of adequate internal controls found during the OIG's 2010 audit for the Blackberry devices still exists as a result of the OIG's recent review of iPhone records. The risk of fraud is heightened as the agency has moved to the new iPhone devices that have a greater market value than the prior Blackberry devices. It is concerning that the inventory list for iPhones is not accurate as this is a relatively new acquisition. The OIG has expressed concerns over the lack of appropriate inventory control in ITD for many years.

> FEC IT inventory records are consistently incomplete and/or contain inaccurate data.

Detailed Testing Results

To verify corrective action for recommendations 2a & 2f from the *Audit of the Commission's Property Management Controls*, the OIG reviewed ITD's master inventory list provided on April 24, 2014 by the Deputy CIO of Operations and FEC's AT&T Wireless phone bill for billing cycles February 28 – March 27, 2014 & March 28, 2014 – April 27, 2015. The OIG reviewed the documentation for accuracy of phone assignments between the master inventory list and the AT&T bill information to ensure corrective action has been adequately implemented to support the CIO's response that "*Spares are…accounted for, properly tracked and managed…PCDs record keeping has never been in any risk of fraud…any risk attached to the audit finding has been mitigated…*"

- iPhone #XXX-3281 is assigned as a phone in storage on the inventory list; however, the AT&T bill has the device listed as assigned to an Enforcement Division attorney.

- iPhone #XXX-4874 is assigned to an Administrative Law Division attorney on the inventory list; however, the AT&T bill has the device listed as assigned to an Enforcement Division attorney.
    - According to the inventory list **and** the AT&T bill, the Enforcement Division attorney is assigned two iPhones (#XXX-2790 and #XXX-4874).

- iPhone #XXX-0439 is assigned as a iPhone in storage on the inventory list; however, the AT&T bill shows the iPhone assigned to an Executive Assistant in a Commission Office.

- iPhone #XXX-4659 is assigned to a Program Support Officer on the inventory list; however, the AT&T bill shows the iPhone assigned to an Enforcement Division attorney.

- iPhone #XXX-8324 is assigned twice to a Reports Analysis Division employee and an Office of Administrative Review employee on the inventory list; however, the AT&T bill shows the iPhone assigned to the Office of Administrative Review employee.
    - iPhone #XXX-6690 is assigned to the Reports Analysis Division employee on the AT&T bill; this iPhone is not listed on the inventory list.

- iPhone #XXX-2318 is assigned to a Litigation Division attorney on the inventory list; however, the AT&T bill has the device assigned to a Policy Division attorney[6].

- iPhone #XXX-0890 is assigned as the "Federal Election Commission" and not an individual employee on the AT&T bill; however, the inventory list shows the iPhone assigned to a Special Counsel attorney in the Commission Office.

- iPhone #XXX-6447 is assigned to a former[7] Executive Assistant in a Commission Office on the AT&T bill; however, the inventory list does not have this iPhone listed.

[6] As of June 8th, 2014 employee is on temporary assignment as an Executive Assistant in a Commission Office.
[7] Employee separated from the FEC on March 22, 2014.

OIG Concerns

FEC needs to improve the accountability of management officials necessary to ensure compliance with all aspects of Directive 50: Audit Follow-up. It is essential that the Commission not only requires management to report on semi-annual basis the status of outstanding recommendations, but also develops a process to ensure the Audit Follow-up Officials are being held accountable for implementing outstanding recommendations in a timely manner that are beneficial to the agency's' mission and will improve agency programs. The Office of Management and Budget (OMB) Circular No. A-50 states:

> *"Agency heads are responsible for (2) Assuring that management officials throughout the agency understand the value of the audit process and are responsive to audit recommendations.*

Without accountability necessary to ensure corrective actions are taken by management, the mission of the agency is consistently operating under weaker controls that can increase cost, expose the agency to risks, and increase the potential of fraud waste, and abuse to agency programs.

In addition, the OIG is concerned with the lack of progress in addressing the outstanding recommendations for the *Inspection of the FEC's Disaster Recovery Plan and Continuity of Operations Plan.* The original 30 recommendations have been outstanding since the release date of the report, January 2013.

Report Review

This report provides the Commission and management the results of the Office of Inspector General's (OIG) review of outstanding OIG recommendations as of June 2014.

As required by the Inspector General Act of 1978, as amended, the Office of Inspector General (OIG) is responsible for conducting audits of the Federal Election Commission's (FEC) 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, to include 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.*

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 actions, 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).

Based on management's availability, the OIG strives to schedule these meetings to provide management with the results of our review prior to management's reporting deadlines to the Commission in May and November. These meetings can provide management with timely OIG feedback for their semiannual reports to the Commission and enables the OIG to keep abreast of management's progress. 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."*

FEC management is required by FEC Directive 50 to provide semiannual status reports (May and November) to the Commission of their progress concerning outstanding OIG recommendations. 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 reported to the Commission and Congress in the OIG's Semiannual Reports to Congress.

Background

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 (AFO), 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 their 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…;"

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

MEMORANDUM

TO: Alec Palmer
Staff Director/Chief Information Officer

FROM: Lynne A. McFarland
Inspector General

SUBJECT: Risk Acceptance Statement: *December 2013 Review of Outstanding Recommendations Report*

DATE: February 10, 2014

The Office of Inspector General (OIG) is finalizing the *December 2013 Review of Outstanding Recommendations Report* to be released February 2014. As you know, the OIG's outstanding recommendations report details the results of the OIG's follow-up reviews for audit and inspections that have outstanding recommendations for six months or more.

As of December 2013, the *Audit of the FEC's Property Management Controls* has several recommendations that have been outstanding for over three years. The OIG has reported on our concern with the lack of progress from ITD management since June 2012, and our soon to be released report on outstanding recommendations reiterates the OIG's concern. The audit follow-up official has stated during OIG follow-up reviews that no further corrective actions will be implemented to address the remaining recommendations and management considers the recommendations closed. Therefore, the OIG's *December 2013 Review of Outstanding Recommendations Report* is requesting a written statement from the Staff Director accepting the risk of the outstanding recommendations in order for the OIG to officially close the open recommendations. A list of the outstanding recommendations, and the risks associated with not implementing the recommendations, is attached with this memo and will also be included in the final report.

In addition, the OIG is aware that ITD is in the process of replacing the Blackberry devices with iPhones. The OIG would like to note that the outstanding recommendations are applicable to the iPhone and any other cellular phone device the agency may procure. Based on the OIG's knowledge of the agency's lack of controls in this area, the OIG believes the roll-out of the new iPhone devices would be the opportune time for management to implement the remaining outstanding recommendations to improve the agency's controls.

The OIG is requesting a written statement from the Staff Director by **March 3, 2014** in response to accepting the risk of the outstanding recommendations for the *Audit of the Property Management Controls* in order for the OIG to properly plan for the next audit follow-up review period. If you decide to implement one or more of the outstanding recommendations, based on the risks outlined in this memorandum, please let me know by March 3, 2014 so that I can schedule a review of the corrective action(s) at a future date.

Thank you.

Attachment

Management's Acceptance of Risk for the *Audit of the FEC's Property Management Controls* Outstanding Recommendations

The Office of Inspector General is requesting a written statement from the Staff Director in regards to the remaining open recommendations from the *Audit of the FEC's Property Management Controls* that are listed below. In order to close these recommendations and conclude the follow-up process, the Staff Director should state that management will accept the risk of not implementing the outstanding recommendations. Below are the outstanding recommendations and their associated risks.

1. *Recommendation 1h*: Document the ITD re-authorization process of PCD [personal communication device/Blackberry] users in ITD's Policy 58-4.4
    - **Risk:** *Waste of agency funding*.
        - The re-authorization of PCD users is an internal control to help ensure that staff provided a Blackberry continue to have a need for the device. Staffs' job responsibilities change over time, and their need for a Blackberry can change. Therefore, it is important to periodically review the staff assigned a Blackberry to make sure the expenditure of funds for the Blackberry service is still required. As ITD is the office with oversight of the Blackberry devices, ITD's refusal to periodically re-authorize the users means ITD may be unaware if the agency is wasting funds on FEC personnel or contractors who no longer have a business need for an FEC issued Blackberry.

2. *Recommendation 1k*: Provide the policies and procedures for the use of Blackberry devices to all users when issuing the Blackberry.
    - **Risk:** *Abuse of government property.*
        - Blackberry devices issued to authorized users have the potential to be misused (excessive personal use, downloading of unauthorized applications, viewing prohibited information on a government issued device, etc.) if users are not aware of polices and procedures for using an FEC issued Blackberry.

3. *Recommendation 2a*: All unassigned Blackberry devices should be suspended or service should be terminated if the device can not be immediately transferred to another user (no active spares kept in ITD). At the time of our inspection, ITD retained a minimum of 10 inactive spare devices (many of the spares were left active incurring monthly charges) and a spare Subscriber Identity Module (SIM) card (portable memory chip). If required, a device could be activated within 24 hours.
    - **Risk:** *Fraud and no internal control.*
        - In a prior audit follow-up, management stated that they have decreased the number of spare devices on hand to three. Although the OIG agrees that three spare devices is more reasonable than the previous 10 spares, the OIG reviewed devices listed as unassigned (spare) on the agency's AT&T monthly bill and they showed activity (in use) and were listed as assigned to FEC personnel on

the inventory list. As a result, ITD is not maintaining accurate records of the unassigned Blackberry devices. Because these devices are not properly tracked, management runs the risk of potential fraud (stolen devices, unauthorized activity) because ITD does not maintain proper records of spare devices.

4. *Recommendation 2f*: Blackberry user information should be kept up to date and adjusted in a timely manner on the ITD master Blackberry listing and the AT&T Premier website for employee separations and new assignment of devices.
    - **Risk**: *Fraud and no internal control.*
        - Because these devices are not properly tracked, management runs the risk of potential fraud (stolen devices) because ITD does not maintain proper inventory records, and it's likely these devices would not be detected as missing.

5. *Recommendation 2g:* Management should educate Blackberry users of all features that incur additional cost to the agency, such as: roaming charges that result when employees place calls outside AT&T service areas; texting; directory assistance; unauthorized software, and voice use over the pooled plan limits.
    - **Risk:** *Waste of agency funding and abuse of government property.*
        - The agency is at risk of wasting funds on unauthorized device features that cost additional money beyond the agency's plan. There is also potential for abuse by users in using their agency issued devices for excessive personal use. Both instances have been identified by the OIG and reported to management during the initial audit and in prior follow-up reviews.

6. *Recommendation 3:* ITD should implement a form and process such as the NIST Sample Sanitization Validation form, to record sanitization (wiping) of devices, disposal and/or destruction, as appropriate.
    - **Risk:** *Data breaches and fraud.*
        - Old devices that are no longer in use run the risk of containing sensitive information from emails/attachments if management has no record that the device has been properly sanitized prior to transferring the device as surplus to the General Services Administration. In addition, if the device is to be destroyed and there is no record of the destruction, there is a risk that the device can be removed from the agency and used for personal use or prohibited activity (selling an agency issued device).

7. *Recommendation 3e:* Segregate the following program functions among three or more ITD staff: Purchasing/ordering and recording assets; Authorization for purchases, including devices received free under upgrade promotion; Receipt, storage, and distributing of assets; and Destruction or disposal of surplus PCDs.
    - **Risk***: Waste of agency funds and fraud***.**
        - Having one person to oversee all purchasing, recording, and storage responsibilities for Blackberry devices presents the risk of a) wasting agency funds on additional devices that are purchased for prohibited activity; b) abuse of agency devices being used as personal use; and c) creating fraudulent documentation and records to prevent the detection of prohibited activity of agency issued devices.

FEDERAL ELECTION COMMISSION
WASHINGTON, D.C. 20463

MEMORANDUM

To: Lynne A. McFarland
Inspector General

FROM: Alec Palmer
Staff Director/Chief Information Officer

SUBJECT: Response to the Inspector General's February 10, 2014 Memorandum of the Outstanding Recommendations of the Audit of the *Property Management Controls*

DATE: March 4, 2014

Per your request, the attached document contains the OCIO responses to the Inspector General's outstanding recommendations of the Audit of the *Property Management Controls*. The attachment contains the response to each recommendation cited in the subject memo and the progress we have made in each category. We look forward to your feedback as we continue to improve upon our security posture here at the FEC. I have copied the Commissioners and as always seek their collective advice to ensure we are following the proper steps in mitigating any risks associated with the findings of the property risk assessment.

Thank you.

cc: Commissioners

RESPONSE TO THE INSPECTOR GENERAL'S OUTSTANDING RECOMMENDATIONS OF THE AUDIT OF THE FEC'S *PROPERTY MANAGEMENT CONTROLS*

1. ***Recommendation 1h*:** Document the ITD re-authorization process of PCD [personal communication device/Blackberry] users in ITD's Policy 58-4.4
    - **Risk:** *Waste of agency funding.*

      The re-authorization of PCD users is an internal control to help ensure that staff provided a Blackberry continue to have a need for the device. Staffs' job responsibilities change over time, and their need for a Blackberry can change. Therefore, it is important to periodically review the staff assigned a Blackberry to make sure the expenditure of funds for the Blackberry service is still required. As ITD is the office with oversight of the Blackberry devices, ITD's refusal to periodically re-authorize the users means ITD may be unaware if the agency is wasting funds on FEC personnel or contractors who no longer have a business need for an FEC issued Blackberry.

    - **Response:**

      Since the audit was conducted, OCIO has completed and documented 2 reauthorizations, the first one in September of 2009, as an immediate response to the initial audit, and again in August of 2013 as part of the latest CAP update. The results of the last re-authorization are attached. The conduct of these two re-authorizations in conjunction with the annual inventory, satisfies the IG recommendation that ITD conduct "periodic" re-authorizations. We believe any risk attached to this audit finding has been mitigated to the minimum and any perceived risk is at an acceptable level. We are requesting that this finding should be considered closed.

2. ***Recommendation 1k*:** Provide the policies and procedures for the use of Blackberry devices to all users when issuing the Blackberry.
    - **Risk:** *Abuse of government property.*

      Blackberry devices issued to authorized users have the potential to be misused (excessive personal use, downloading of unauthorized applications, viewing prohibited information on a government issued device, etc.) if users are not aware of polices and procedures for using an FEC issued Blackberry.

    - **Response:**

      Newly assigned users are made aware of the provisions of the PCD Policy, provided the link to the location of the policy, and are informed as to the basic services offered by the agency's provider. Additionally we have worked closely with OGC to establish a new and required Skillport training course which addresses abuse of government property, prior to issuance of such device. We believe any risk attached to this audit finding has been mitigated to the minimum and any perceived risk is at an acceptable level. We are requesting that this finding should be considered closed.

3. ***Recommendation 2a*:** All unassigned Blackberry devices should be suspended or service should be terminated if the device can not be immediately transferred to another user (no active spares kept in ITD). At the time of our inspection, ITD retained a minimum of 10 inactive spare devices (many of the spares were left active incurring monthly charges) and a spare Subscriber Identity Module (SIM) card (portable memory chip). If required, a device could be activated within 24 hours.

   - **Risk:** *Fraud and no internal control.*

     In a prior audit follow-up, management stated that they have decreased the number of spare devices on hand to three. Although the OIG agrees that three spare devices is more reasonable than the previous 10 spares, the OIG reviewed devices listed as unassigned (spare) on the agency's AT&T monthly bill and they showed activity (in use) and were listed as assigned to FEC personnel on the inventory list. As a result, ITD is not maintaining accurate records of the unassigned Blackberry devices. Because these devices are not properly tracked, management runs the risk of potential fraud (stolen devices, unauthorized activity) because ITD does not maintain proper records of spare devices.

   - **Response:**

     OCIO has instituted the IG recommendation that PCD's be included in the agency's overall IT inventory complete with barcode. The annual inventory conducted includes PCD's. Spare devices are necessary to be able to support the turnover of personnel, new hires, and other contingencies in support of the agency's mission. The number of spare devices varies with the fluctuation of staffing. The number is also a factor of the quantity discounts offered by providers at the time of device purchase or upgrades provided by the vendor. Spares are kept secure, inventoried, accounted for, properly tracked and managed. In the past access to the AT&T monthly bill was through the AT&T billing office and name changes to the bill were made through an AT&T agent. Subsequently, requested changes were not completed in a timely manner, and we had little, if any control over the assigned user names that appeared on the AT&T bill. AT&T has since upgraded their billing system to a dashboard configuration, allowing us to directly input the billing system, to add, delete and change users. PCD record keeping has never been in any risk of fraud, however the record keeping has been more automated than in the past. We believe any risk attached to this audit finding has been mitigated to the minimum and any perceived risk is at an acceptable level. We are requesting that this finding should be considered closed.

4. ***Recommendation 2f*:** Blackberry user information should be kept up to date and adjusted in a timely manner on the ITD master Blackberry listing and the AT&T Premier website for employee separations and new assignment of devices.

   - **Risk**: *Fraud and no internal control.*

     Because these devices are not properly tracked, management runs the risk of potential fraud (stolen devices) because ITD does not maintain proper inventory records, and it's likely these devices would not be detected as missing.

- **Response:**

  See the response to 3 above. We believe any risk attached to this audit finding has been mitigated to the minimum and any perceived risk is at an acceptable level. We are requesting that this finding should be considered closed.

5. ***Recommendation 2g:*** Management should educate Blackberry users of all features that incur additional cost to the agency, such as: roaming charges that result when employees place calls outside AT&T service areas; texting; directory assistance; unauthorized software, and voice use over the pooled plan limits.

   - **Risk:** *Waste of agency funding and abuse of government property.*

     The agency is at risk of wasting funds on unauthorized device features that cost additional money beyond the agency's plan. There is also potential for abuse by users in using their agency issued devices for excessive personal use. Both instances have been identified by the OIG and reported to management during the initial audit and in prior follow-up reviews.

   - **Response:**

     All users are informed of the features of the agency's plan when issued a device. Any updates to the plan are communicated at the time of update. The agency is in the process of transitioning to iPhone from Blackberry devices and features of the new technology and plan are being communicated in training conducted. The current plan has been simplified to greatly reduce any instance off over use or unauthorized use and any potential for fraud. The plan currently covers unlimited text and data and 300 voice minutes per month pooled over all users. This amount has proved adequate to prevent over usage charges. We believe any risk attached to this audit finding has been mitigated to the minimum and any perceived risk is at an acceptable level. We are requesting that this finding should be considered closed.

6. ***Recommendation 3:*** ITD should implement a form and process such as the NIST Sample Sanitization Validation form, to record sanitization (wiping) of devices, disposal and/or destruction, as appropriate.

   - **Risk:** *Data breaches and fraud.*

     Old devices that are no longer in use run the risk of containing sensitive information from emails/attachments if management has no record that the device has been properly sanitized prior to transferring the device as surplus to the General Services Administration. In addition, if the device is to be destroyed and there is no record of the destruction, there is a risk that the device can be removed from the agency and used for personal use or prohibited activity (selling an agency issued device).

   - **Response:**

     GSA does not accept any devices whose memory/storage components have not been erased. The FEC sanitizes all data storages devices that are disposed of through GSA facilities in accordance with DOD standards as a matter of policy.

The FEC has suspended it's practice of destroying devices in lieu of disposal at a GSA facility. All FEC computer / communication devices are disposed of through GSA facilities, or through other authorized disposal methods. Documentation of all devices turned into GSA is maintained on file. We believe any risk attached to this audit finding has been mitigated to the minimum and any perceived risk is at an acceptable level. We are requesting that this finding should be considered closed.

7. ***Recommendation 3e:*** Segregate the following program functions among three or more ITD staff: Purchasing/ordering and recording assets; Authorization for purchases, including devices received free under upgrade promotion; Receipt, storage, and distributing of assets; and Destruction or disposal of surplus PCDs.

   - **Risk**: *Waste of agency funds and fraud.*
     Having one person to oversee all purchasing, recording, and storage responsibilities for Blackberry devices presents the risk of a) wasting agency funds on additional devices that are purchased for prohibited activity; b) abuse of agency devices being used as personal use; and c) creating fraudulent documentation and records to prevent the detection of prohibited activity of agency issued devices.

   - **Response:**
     The responsibility for the administration of the PCD program of the agency rests with the Office of the CIO, and more specifically within the IT Operations Division. IT procurement initiation also is the responsibility of the IT Operations Division. Purchase Requests (PR) are prepared by one employee, the PR is approved or denied by the DCIO, and then forwarded to the procurement division. The IT inventory is maintained by the desktop support branch, as well as the distribution and maintenance of all IT desktop and PCD equipment. The responsibility for the actual procurement and expenditure of funds rests within the procurement division, not IT. Since the entire budget for PCD's is within the simplified acquisition procedures threshold, it is our objective to streamline and keep the process as simple as necessary, and OCIO in conjunction with OCFO accomplishes this objective and still maintains adequate controls for a project that is under $150K. We believe any risk attached to this audit finding has been mitigated to the minimum and any perceived risk is at an acceptable level. We are requesting that this finding should be considered closed.

Federal Election Commission
Office of Inspector General

Fraud Hotline
202-694-1015

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

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

Together we can make a difference.