Federal Election Commission

Office of Inspector General

Inspector General Statement on the Federal Election Commission's Management and Performance Challenges - 2014

Table of Contents Pg

Inspector General Statement on the FEC's Management and Performance Challenges 1-8

Attachment A: Response to OIG's Statement on the FEC's Management and Performance Challenges 9

FEDERAL ELECTION COMMISSION

WASHINGTON, D.C. 20463

Office of Inspector General

MEMORANDUM

TO: The Commission

FROM: Inspector General

SUBJECT: Inspector General Statement on the Federal Election Commission's Management and Performance Challenges

DATE: October 15, 2014

Each year, the Inspector General is required to provide a summary and assessment of the most serious management and performance challenges facing the Federal Election Commission (FEC). The requirement is contained in the *Reports Consolidation Act of 2000* (Public Law 106-531), an amendment to the *Chief Financial Officers (CFO) Act of 1990*. The attached document responds to the requirement, and provides the annual statement on Commission challenges to be included in the *Federal Election Commission Performance and Accountability Report (PAR) Fiscal Year (FY) 2014.*

The Inspector General has identified three management and performance challenges for inclusion in the FEC's FY 2014 PAR:

Information Technology Security
Governance Framework
Human Capital Management / Human Resources Operations

Since FY 2004, the Inspector General (IG) has identified information technology (IT) security as a challenge to the agency. The FEC has several IT security control related findings in the agency's annual financial statement audit[1] and other OIG audits and inspections that have been repeat findings for several years. Due to the agency's legal exemption from the *Federal Information Systems Management Act*, management has not formally adopted or implemented the applicable National Institute of Standards and Technology (NIST) IT security standards for the federal government. The current IT security program at the FEC is not structured to ensure that the IT controls identified as top priority government-wide, or those controls that are applicable to the FEC's business processes are implemented, or mitigated to the lowest possible risk.

Although IT security is considered a challenge at the FEC, the OIG notes that management has recently taken steps to address the on-going concerns of the IT security program.

[1] The FEC OIG has required a more in-depth review of IT security controls through the annual financial statement audits due to the agency's exemption from the Federal Information Systems Management Act.

As examples, the Office of the Chief Information Officer is working with the Department of Homeland Security on continuous monitoring efforts and has procured contract services to perform a full inventory review and gap analysis of FEC IT systems. The OIG looks forward to any improvements and enhancements to the agency's IT security program that will result from these efforts by management.

The agency's governance framework has also been a continued challenge for the FEC since FY 2008. Critical management positions that are directly linked to carrying out the agency's mission have remained vacant for more than a year. Stability and continuity in key leadership positions promotes an effective governance framework which improves the leadership and oversight of agency programs and functions, as these are key components to ensure that the agencies mission and objectives are achieved.

In addition, from FY 2005 to present, the IG has identified human capital management as another challenge for the agency. The OIG conducted an audit of the FEC's Office of Human Resources (OHR) in FY 2013. Several deficiencies related to leadership and critical human resource functions and processes were noted. The OIG notes that a new Director of OHR, who has extensive experience in HR management, was hired in May 2014. The OIG acknowledges that the new Director of OHR has already developed a roadmap to improve the OHR and has made customer service a top priority. As a result, OIG has removed leadership as a part of the OHR management challenges.

OHR has also begun to automate the hiring/selection process and personnel actions via the Federal Human Resources (FHR) system and Remedy (customer request tracking system). However, due to staff shortages and the number of corrective actions required, it will take time before additional improvements can be achieved with regards to key OHR functions.

The IG's annual assessment of management and performance challenges is based on information derived from a combination of several sources, including Office of Inspector General audit and inspection work, Commission reports, and a general knowledge of the Commission's programs and activities. The management and performance challenges are detailed in the attached report table. The *Reports Consolidation Act of 2000* permits agency comment on the IG's statements. Agency comments, if applicable, are due November 12, 2014.

Lynne A. McFarland

Lynne A. McFarland
Inspector General

Attachment

cc: Judy Berning, Acting Chief Financial Officer
Alec Palmer, Staff Director and Chief Information Officer
Greg Baker, Deputy General Counsel-Administration
Lisa Stevenson, Deputy General Counsel-Law
Edward Holder, Acting Deputy Staff Director for Management and Administration
Roger Cotton, Director, Office of Human Resources

FEDERAL ELECTION COMMISSION (FEC)
MANAGEMENT and PERFORMANCE CHALLENGES
FY 2014

Information Technology Security

The FEC places significant reliance on information technology (IT) to fulfill the agency's mission. Therefore, an agency-wide security management program should be in place to establish a framework to manage security risks, develop security policies, assign responsibilities and monitor the adequacy of computer security related controls. The FEC is in need of a more robust security program that will ensure that the agency is always meeting the applicable government-wide IT security standards.

Challenge	OIG Assessment / Comment
1. Inadequate IT Security Program	
• The FEC has determined it is not subject to the Federal Information Systems Management Act (FISMA)[2] because FISMA uses the definition of agency found in the Paperwork Reduction Act, which specifically excludes the FEC. As a result, the agency has not implemented the applicable National Institute of Standards and Technology (NIST) IT controls that are used as best practice government wide.	• The agency has failed to adequately define the set of best practices used to secure the FEC's information technology. • The OIG believes that the IT security incidents that have occurred in recent years could possibly have been prevented or minimized if the agency had adopted and aligned with the government-wide security standards applicable to the FEC's business processes. Although IT risks can not be eliminated; having adequate controls in place can help reduce the risk and/or detect in a reasonable timeframe, standard security threats. • Management **must** perform risk assessments prior to declining to implement an IT control that is related to FISMA or NIST in order to determine what would be in the best interest of the agency, rather than opting not to implement the control because it is not legally required.
• Out of date IT security policies and procedures	• IT security policies and procedures are not updated in a timely manner or followed by the Information Technology Division (ITD). In addition, audits have revealed that FEC IT management and staff are not aware of their own policies in order to ensure compliance.

[2] Federal Information Systems Management Act is the law that requires federal agencies to follow government-wide IT security standards.

2. Disaster Recovery Plan (DRP) Continuity of Operations Plans (COOP)	
• Management has yet to fully implement a plan for ensuring the agency can continue to carry out its mission in the event of a local disaster or temporary disruption (i.e. flooding, fire, etc.) to the FEC's headquarters.	• Management has not properly planned or provided the necessary resources to the COOP project. FEC procured contract services in 2008 to assist in developing the DRP and COOPs, however, the work and resources put into developing these plans has diminished in the past six (6) years because testing, training, and updates have not been thoroughly conducted and completed. Thus, the agency is planning to spend additional funding on similar contract services to implement a COOP for the agency. • The OIG initiated an inspection of the FEC's DRP/COOP implementation, and released the report in January 2013 identifying 30 recommendations for improvement. All 30 recommendations remain open, and management has consistently stated that no progress has been made in this area since the release of the report. These recommendations are critical to the agency's ability to effectively respond, recover, and continue agency business in the event of a disaster or disruption to business operations.

Governance Framework

A governance framework consists of the structure and stability of an organization's senior leadership that are accountable for the organization's mission and objectives. The absence or weaknesses in a proper governance framework hinders the organization from efficiently and effectively carrying out the mission of the organization.

Challenge	OIG Assessment / Comment
1. Vacant Key Leadership Positions	
• The agency experiences frequent turnover in key positions. Currently, there are three key positions that are vacant: **a)** General Counsel **b)** Chief Financial Officer **c)** Deputy Staff Director for Management and Administration	• **General Counsel (GC) -** this position has been vacant for over a year. The former GC was employed at the FEC for less than two (2) years. The GC has the responsibility of ensuring that the Office of General Counsel properly administers and enforces campaign finance laws, among other duties. This position is critical to the agency's mission • **Chief Financial Officer (CFO) -** this position has been vacant for two (2) years (since October 2012). The CFO is responsible for the agency's budget and for ensuring that the agency's funds are accounted for and accurately reported. The FEC has had an Acting CFO since the vacancy in October 2012. However, with the current budget constraints in the government, the FEC should make filling this position with a permanent CFO a priority to ensure that the FEC's appropriated funds are appropriately spent and accurately recorded. • **Deputy Staff Director for Management and Administration (Deputy Staff Director) -** the Deputy Staff Director is the direct supervisor over many of the program offices of the agency. This position has only been vacant since August 2014, and an Acting Deputy Staff Director has been appointed; however, the FEC is in the process of fully implementing their new Strategic Plan, and it is imperative that the Deputy Staff Director's position is filled with a qualified candidate to ensure the proper oversight.

2. Adequate Management Accountability & Oversight	
• Currently, the FEC lacks the accountability necessary to ensure compliance with all aspects of the agency's Audit Follow-Up process.	• The agency currently has eighty-seven (87) outstanding OIG recommendations. Some of these recommendations have been outstanding since 2010. OIG concludes that senior leaders should be held accountable for minimal progress on implementing outstanding recommendations. Without sufficient accountability to ensure corrective actions are taken by management, the mission of the agency is potentially 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 and operations.
• FEC needs a Chief Information Officer who is solely dedicated to the agency's Information Technology Division.	• The Staff Director and Chief Information Officer (CIO) positions at the FEC are filled by one FEC employee. At the FEC, information technology (IT) is: **a)** a critical part of the agency's mission in disclosing campaign finance information to the public; **b)** an area of concern regarding IT security; **c)** not aligned with government-wide IT control standards; and **d)** an area that consistently has open and repeat recommendations from OIG audits and inspections. Currently, the Information Technology Division (ITD) is making strides to improve their security postures and resolve IT vulnerabilities, which requires adequate oversight and leadership. Therefore, the OIG believes that the area of IT requires a CIO that can be fully dedicated to ensuring that ITD is able to adequately fulfill the agency's mission of disclosure, while ensuring that the agency's IT security program is adequately designed to comply with government-wide IT standards and ensure continuous monitoring to remain current on IT risks and controls.

Human Capital Management / Human Resources Operations

The Office of Human Resources (OHR) and Labor Relations is vital to ensuring a human capital management framework is developed and implemented at the Commission, and that the framework supports the agency's overall goals and objectives. The OHR is also responsible (either directly or indirectly) for all FEC personnel related activities including hiring, benefits, and personnel actions (pay raises, status changes), among other activities. The numerous responsibilities of the OHR results in the office being one of the most important administrative functions of the FEC. The OIG has been reporting on FEC's human capital management and other OHR operational performance challenges (specifically customer service and updated policies and procedures) since FY 2010 and completed an audit of OHR in FY 2013. *The Audit of the FEC's Office of Human Resources* (OHR Audit) audit report was issued in July 2013. The OIG acknowledges that FEC has made progress with respect to human capital management that includes a final Strategic Human Capital Management Plan (HCMP) and standard performance management plans which are now aligned with FEC strategic goals for all employees with the exception of the Office of Inspector General (OIG). OIG also notes that the FEC hired a new Director of OHR in May 2014 who has extensive human resource management experience. The Director of OHR is making progress to implement corrective actions and is committed to improving customer service. However, based on the number of findings and recommendations (26) included in the OHR audit, it will take additional time and resources to address them all. The OIG has identified the major challenges that still face OHR as described below:

Challenges	**OIG Assessment / Comment**
1. Customer Service	
• Customer service has been reported as a management challenge since FY 2011. In FY 2014, OHR implemented an automated customer request tracking system (Remedy) and has partially automated the selection/hiring process and personnel actions via the FHR system. However, per discussion with the Director of OHR, the Remedy system was not customized to meet the specific needs of the OHR environment. Therefore, the system may not be robust enough to optimize the tracking and reporting needed to improve OHR response time to inquiries. Also, it is going to take time for employees to get acclimated to using the new automated systems. OIG also notes that OHR lost another full time employee in January 2014 who has not been replaced. In order to make significant improvements in customer service, other factors that impact customer service including but not limited to proper staffing, implementation of streamlined operating procedures and creating an organizational structure that promotes efficiency need to be in place.	• Based on initial follow-up work on recommendations included in the OHR audit, OIG concludes that OHR is making progress with implementing corrective actions which should help improve customer service. Once corrective actions have been fully implemented, OIG will assess whether the efforts by OHR has resulted in significant improvements in customer service. .

2. Policies and Procedures	
• As reported since the 2011 OIG management challenges, there are many OHR policies (Directives) and/or standard operating procedures (SOPs) that are either outdated, do not exist, inadequate, or do not reflect current business practices. OIG notes that some of OHR related Directives have been updated over a year ago but have not yet been approved by the Commission. Timely updating and distribution of current policies and procedures are essential to ensure compliance, and to promote an effective and efficient workforce.	• OIG notes that updating and/or creating OHR Policies and SOPs is a priority of the new Director of OHR. However, due to the volume of documents to be updated/created, and the number of other priorities facing OHR, this will continue to be a challenge in FY 2015.

ATTACHMENT A

Management’s Response
(2014 Management’s Challenges)

Response to the OIG’s Statement on the Federal Election Commission's Management and Performance Challenges – Nov. 12, 2014

Although management generally agrees with the summary assessment contained in the body of OIG’s memo, we do not concur with many of OIG’s Assessment/Comments contained in the report table included with the memo. Most of management’s disagreements with OIG’s assessment are reported on in the semi-annual corrective action plans (CAP) for each OIG audit. The following addresses each instance where management disagrees with OIG’s Assessment/Comment, as detailed in the table.

Information Technology Security:

1. **Inadequate IT Security Program**

OIG Assessment / Comment:

- The agency has failed to adequately define the set of best practices used to secure the FEC’s information technology.

Management Response:

- The Commission is undertaking a thoughtful evaluation of the applicable NIST IT controls to define those that best apply to an agency of our size and mission. As OIG acknowledges, the FEC is legally exempt from FISMA and, therefore, is not required to implement the NIST IT controls. Nevertheless, to date, 32 NIST standards have been adopted by the agency. These standards, listed below, have been formalized as policies and enacted as part of Directive 58.

    - 58.1.1: Personnel Security Policy
    - 58.1.2: Security Training and Awareness Policy
    - 58.1.3: Information Classification Policy
    - 58-1.4: Hardware and Software Acquisition Security Policy
    - 58.1.5: Third Party Services Policy
    - 58.2.1: Risk Management Policy
    - 58.2.2: Account Management Policy
    - 58.2.3: Change Management Policy
    - 58.2.4: Certification and Accreditation Policy
    - 58.2.6: User Security Support Policy
    - 58.2.7: Segregation of Duties Policy
    - 58.2.8: Backup and Recovery Policy
    - 58.2.9: Continuity of Operations and Disaster Recovery Policy
    - 58.2.10: Security Incident Response Policy
    - 58.2.ll: Security Review (Continuous Monitoring) Policy
    - 58.3.1: Logical Access Policy
    - 58.3.2: Application and Operating System Policy

- 58.3.3: Auditing and Monitoring Policy
- 58.3.5: Electronic Mail and Internet Security Policy
- 58.3.6: Malicious Code Policy
- 58.3.7: Personally Owned Wireless Connectivity Security Policy
- 58.3.7: Wireless Security Policy
- 58.4.1: Physical Access Security Policy
- 58.4.2: Media Management Security Policy
- 58.4.3: Mobile Computing Security Policy
- 58.4.4: Personal Communication Devices Security Policy
- 58.4.5: Virtual Private Network (VPN) Policy
- 58.4.6: System Integrity Policy
- 58.4.7: Physical & Environmental Security Policy
- 58.4.8: Maintenance Security Policy
- 58.4.9: Systems & Communications Protection Security Policy
- 58A: FEC Information System Security Policy
- FEC Directive 58: Electronic Records, Software and Computer Usage
- IT Systems Security Program Policy Cover Letter

Additionally, the agency continues to review the applicable NIST IT controls. In FY2014, the agency contracted with an IT security consultant to perform a comprehensive review of implementing further NIST guidelines at the FEC. This study will evaluate any potential gaps in the agency's security controls, analyze which NIST standards are most applicable to the work of our agency, and determine the costs of implementing these recommended controls. Furthermore, the agency continues to evaluate the NIST study provided by the OIG to the Commission on October 7, 2014. This study includes recommendations for implementing differing levels of NIST controls, ranging from $451,375 (Small Firm, Primary Controls) to $1,291,075 (Large Firm, Moderate Controls). Upon the completion of these reviews, the Commission will evaluate the recommended policies and the cost analysis of implementing any additional security controls.

OIG Assessment / Comment:

- The OIG believes that the IT security incidents that have occurred in recent years could possibly have been prevented or minimized if the agency had adopted and aligned with the government-wide security standards applicable to the FEC's business processes. Although IT risks cannot be eliminated; having adequate controls in place can help reduce the risk and/or detect in a reasonable timeframe, standard security threats.

Management Response:

- The security of our systems is taken seriously by the agency. We have maintained network scanning processes to prevent and detect intrusions and, in recent years, enhanced and intensified the level of network scanning. The FEC servers are located in three redundant data centers under the control of a 24-hour a day contractor for FEC systems. This redundancy allows the agency to continue to carry out its mission even if we experience an IT security breach.

Despite our IT security controls, we have unfortunately experienced minor IT security breaches, which are similar to the incidents that other government agencies, large and small, have experienced, including agencies that have fully implemented and complied with FISMA and NIST. The most recent security incident occurred during the 2013 government shutdown, which impaired staff's ability to respond by manually applying patches and precautionary fixes to systems that require human intervention.

Following the shutdown, the agency made strides in mitigating our vulnerabilities during periods of non-human monitoring. We have strengthened firewalls and installed protective IT "moats" and alerts to mitigate our vulnerabilities.

As OIG acknowledges, IT risks cannot be eliminated even with full NIST and FISMA implementation. There is no guarantee that the FEC would avoid all future security incidents through full NIST and FISMA implementation as is evident by those agencies that have fully implemented FISMA and NIST requirements, but have still experienced IT security breaches. Nevertheless, because the agency is committed to protecting the FEC's infrastructure, we have made significant strides in enhancing IT controls to reduce the risk of and detect standard security threats.

OIG Assessment / Comment:

- Management **must** perform risk assessments prior to declining to implement an IT control that is related to FISMA or NIST in order to determine what would be in the best interest of the agency, rather than opting not to implement the control because it is not legally required.

Management Response:

- As acknowledged in OIG's memo, the Commission is undertaking a thoughtful evaluation of the applicable NIST IT controls in order to determine what would be in the best interest of the agency. In FY2014, we contracted with an IT security consultant to perform a comprehensive review of how the FEC should implement NIST policies. This review will include a recommendation of which policies are applicable to and should be adopted by the FEC. This review will take into consideration the agency's risk of not implementing any particular NIST standard and the cost analysis of implementing these recommended security controls. The agency's evaluation will take into consideration the NIST study provided by OIG to the Commission on October 7, 2014. OIG's study includes cost estimates that range from $451,375 (Small Firm, Primary Controls) to $1,291,075 (Large Firm, Moderate Controls).

OIG Assessment / Comment:

- IT security policies and procedures are not updated in a timely manner or followed by the Information Technology Division (ITD). In addition, audits have revealed that FEC IT management and staff are not aware of their own policies in order to ensure compliance.

Management Response:

- All current IT security policies and procedures are part of Directive 58. The IT Division's Security Officer is responsible for updating the policies as required or as changes occur. For example, due to recent changes and necessary updates, Policy 58-4.4 was updated in January 2014, and Policy 58-3.6 was updated in September 2014.

  FEC IT management and staff are aware of IT security policies and make every effort to ensure compliance. IT security is an agenda topic of the weekly IT Staff Meetings, which are attended by all IT supervisors. Security threat detection and protection techniques are discussed, as well as the weekly status of IT security systems. These weekly meetings are led by the IT security officer, and IT management is intimately involved in and aware of the IT security program. Additionally, all new employees are directed to familiarize themselves with all of the Commission's directives as a component of HR training. Furthermore, all employees and contractors are required to participate in IT security training each year. This training entails a recap of vital security polices, and, where appropriate, references the policies themselves.

  Upon completion of the training, employees certify that they have reviewed the appropriate policies.

2. Disaster Recovery Plan (DRP) Continuity of Operations Plan (COOP)

OIG Assessment / Comment:

- Management has not properly planned or provided the necessary resources to the COOP project. FEC procured contract services in 2008 to assist in developing the DRP and COOPs, however, the work and resources put into developing these plans has diminished in the past six (6) years because testing, training, and updates have not been thoroughly conducted and completed. Thus, the agency is planning to spend additional funding on similar contract services to implement a COOP for the agency.

Management Response:

- At this time, the agency is not planning to spend additional funds to procure additional services, similar to those contract services used in 2008 to implement a COOP for the agency. After management procured services in 2008 to develop a COOP, the COOP was adopted and approved by the Commission in 2009, and revised in November of 2010.

Due to a lack of resources during sequestration, the agency was required to delay several projects. Because the FEC is a category four agency as defined by Annex A of HSPD-20, full-scale testing of the COOP was deemed to be a lower priority and was among the FEC projects delayed. Currently, management is revising the COOP to specifically address the types of emergencies that would impact the FEC's mission. Due to the FEC's category four designation for continuity of operations, the necessary revisions to the COOP will be aligned accordingly.

OIG Assessment / Comment:

- OIG initiated an inspection of the FEC's DRP/COOP implementation, and released the report in January 2013 identifying 30 recommendations for improvement. All 30 recommendations remain open, and management has consistently stated that no progress has been made in this area since the release of the report. These recommendations are critical to the agency's ability to effectively respond, recover, and continue agency business in the event of a disaster or disruption to business operations.

Management Response:

- Currently, management is revising the COOP in an effort to respond to OIG's 2013 recommendations. To the extent that any outstanding recommendations remain, these on-going revisions to the COOP will close any remaining recommendations. Management, however, does not agree with some of OIG's COOP findings and has responded to those concerns in the response to OIG's January 2013 report.

Governance Framework:

1. Vacant Key Leadership Positions:

- The agency experiences frequent turnover in key positions. Currently, there are three key positions that are vacant:
  - **a)** General Counsel
  - **b)** Chief Financial Officer
  - **c)** Deputy Staff Director for Management and Administration

Management Response:

- Management understands the importance of filling these key, vacant positions. It remains a challenge, however, to permanently fill these high-level positions. It should be noted that in the interim, the responsibilities of these positions are being fulfilled by qualified, capable, hardworking individuals. Management is assisting the Commission in its recruitment, screening, and selection process.

2. Adequate Management Accountability and Oversight:

OIG Assessment / Comment:

- The agency currently has eighty-seven (87) outstanding OIG recommendations. Some of these recommendations have been outstanding since 2010. OIG concludes that senior leaders should be held accountable for minimal progress on implementing outstanding recommendations. Without sufficient accountability to ensure corrective actions are taken by management, the mission of the agency is potentially 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 and operations.

Management Response:

- Although management is appreciative of OIG's recommendations, management is committed to prudent management, the strategic distribution of resources, and minimal acceptance of risk. The proper emphasis and attention has been afforded to all areas of management. Accountability is essential to ensuring progress in completing OIG's recommendations where management and OIG agree, and will continue to take action to ensure such progress. Management has appropriately responded to the applicable recommendations across functional areas within the agency and will continue to do so.

OIG Assessment / Comment:

- The Staff Director and Chief Information Officer (CIO) positions at the FEC are filled by one FEC employee. At the FEC, information technology (IT) is:

  a) a critical part of the agency's mission in disclosing campaign finance information to the public;
  b) an area of concern regarding IT security;
  c) not aligned with government-wide IT control standards; and
  d) an area that consistently has open and repeat recommendations from OIG audits and inspections.

  Currently, the Information Technology Division (ITD) is making strides to improve their security postures and resolve IT vulnerabilities, which requires adequate oversight and leadership. Therefore, the OIG believes that the area of IT requires a CIO that can be fully dedicated to ensuring that ITD is able to adequately fulfill the agency's mission of disclosure, while ensuring that the agency's IT security program is adequately designed to comply with government-wide IT standards and ensure continuous monitoring to remain current on IT risks and controls.

Management Response:

- In 2011, the Commission approved, that the Staff Director and Chief Information Officer (CIO) positions would be filled by one FEC employee. IT is a critical part of the agency's mission in disclosing campaign finance information to the public and an area of concern regarding IT security and the current employee who fulfills both the Staff Director and CIO position is fulfilling his obligations as directed by the Commission.

  As OIG acknowledged, ITD has "ma[de] strides to improve their security postures and resolve IT vulnerabilities." These strides have been made under the current leadership.

Human Capital Management / Human Resources Operations:

- The FEC has recently hired a new Director of Human Resources, and the areas of Human Capital, Customer Service, and Policies and Procedures are his top priority to improve HR performance.

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.