

Office of Inspector General



**Major Management and Performance
Challenges Facing the Federal Election
Commission for FY 2020**

October 2019

Federal Election Commission - Office of Inspector General
1050 First Street, N.E., Suite 1010, Washington, D.C. 20463



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

MEMORANDUM

TO: The Commission

FROM: Christopher Skinner
Inspector General 

SUBJECT: Inspector General (IG) Statement Summarizing the Major Management and Performance Challenges Facing the Federal Election Commission (FEC) for FY 2020

DATE: October 17, 2019

ENCLOSURE: (1) IG Statement Summarizing the Major Management and Performance Challenges Facing the FEC

In accordance with the Reports Consolidation Act of 2000,¹ the Inspector General (IG) is required to provide a summary and assessment of the most significant management and performance challenges facing the Federal Election Commission (FEC), for inclusion into the FEC's Fiscal Year (FY) 2019 Agency Financial Report (AFR). We believe that the challenges discussed herein, if not addressed, are most likely to impede the Commission's accomplishment of its mission objectives.

We identified the Commission's major management challenges by recognizing and assessing key themes from our audits, evaluations, special reviews, and investigative work, as well as reports published by oversight bodies such as the Office of Personnel Management (OPM) and the U.S. Government Accountability Office (GAO). Additionally, we reviewed previous management challenge reports to determine if those challenges remain significant for this submission. As a result, the major management challenges, in order of significance, are as follows:

1. The resignation of a Commissioner leaves Commission without a four-person quorum,
2. Improve Information Technology (IT) governance to prevent external threats into FEC systems,
3. The lack of a dedicated, full-time, Chief Information Officer (CIO) and vacancies to key leadership positions within the agency,
4. Address outstanding Office of Inspector General (OIG) audit recommendations to improve agency operations for compliance and effectiveness, and

¹ The Reports Consolidation Act of 2000 (amending 31 U.S.C. § 3516).

5. Address the results from the annual Federal Employee Viewpoint Survey (FEVS) and *2016 Root Causes of Low Employee Morale Study* to inform and guide management decisions to increase employee morale.

We hope that continued attention to the management challenges identified in this report will improve the Commission's ability to execute its mission objectives. The FEC OIG encourages the Commission to continue to focus on addressing the management challenges discussed herein. We hope that this report, accompanied by the oversight work we perform throughout the year, assists the Commission in its efforts to improve the effectiveness and efficiency of its programs and operations.

We appreciate the Commission's cooperation throughout the year in addressing the management challenges process. Please contact me if you have any concerns regarding the identified challenges.²

cc: Alec Palmer, Staff Director and Chief Information Officer
John Quinlan, Chief Financial Officer
Lisa Stevenson, Acting General Counsel

² The Reports Consolidation Act of 2000 permits agency comment on the IG's statements.

Table of Contents

Introduction	2
Management Challenge #1: Lack of a quorum	2
Management Challenge #2: Improve IT Governance to prevent external threats into FEC Systems	2
Management Challenge #3: Lack of full-time support to Chief Information Officer (CIO) position and vacancies to key leadership positions	4
Management Challenge #4: Address outstanding OIG audit recommendations	5
Management Challenge #5: Address results from the annual FEVS and <i>2016 Root Causes of Low Employee Morale Study</i>	6
Conclusion	6

Introduction

We identified the Commission’s major management challenges by recognizing and assessing key themes from our audits, evaluations, special reviews, and investigative work, as well as reports published by oversight bodies such as the Office of Personnel Management (OPM) and the U.S. Government Accountability Office (GAO). Additionally, we reviewed previous management challenge reports to determine if those challenges remain significant for this submission. As a result, we determined to identify and highlight five key challenges that the FEC currently faces, which are detailed herein.

Management Challenge #1: Lack of a quorum

The most significant management and performance challenge for FY 2020 resides with the announcement of the resignation of vice chairman, Matthew Petersen, in August 2019, leaving the Commission without a four-person quorum. The Commission is required to be composed of six commissioners, appointed by the President, with no more than three members affiliated with the same political party.¹ Furthermore, 52 U.S.C. § 30106 requires the affirmative vote of four members to take action on particular matters. As of September 2019, the FEC no longer has a quorum to carry out critical mission tasks for the first time in 11 years. The lack of a quorum prevents the agency from among other things, issuing decisions on pending enforcement actions, opening investigations, and issuing advisory opinions.

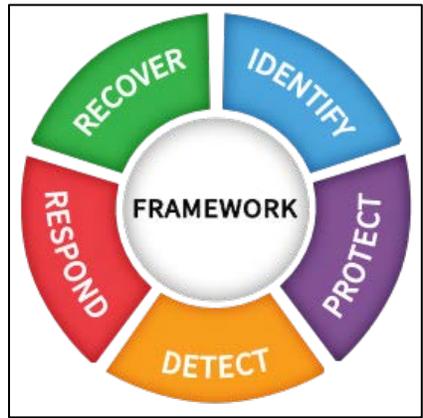
The lack of a quorum prominently directly and indirectly impacts agency programs and procedures. The OIG understands that this management challenge is beyond the control of the agency; but the OIG would be remiss if it failed to identify the lack of a quorum as the most significant management challenge facing the Commission in FY 2020. Furthermore, this challenge has potential to directly impact the subsequent management concerns.

Management Challenge #2: Improve IT Governance to prevent external threats into FEC Systems

The FEC has struggled to implement an IT governance approach that establishes effective oversight to meet security standards in efforts to prevent external and internal threats into FEC systems. The National Institute of Standards and Technology (NIST) developed the minimum security standards for Federal information systems. Since the release of those standards in 2014, technology has become increasingly multifaceted, with cybersecurity and privacy continuing to be key areas of nationwide importance. As a result, NIST published an updated version in 2018.² The updated version identifies among other things, a five core function framework, as illustrated below, that “should be performed concurrently and continuously to form an operational culture to address the dynamic cybersecurity risk.”

¹ See 52 U.S.C. § 30106.

² Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.



The FEC is in need of an adequate government-wide framework to support the agency's information security program. The agency has determined that it is legally exempt from the *Federal Information Systems Management Act (FISMA)*, an applicable framework for information security. The OIG has recommended that the FEC formally adopt the standards of the NIST as its framework, but the agency has not implemented this recommendation.

We acknowledge that the agency has made significant improvements by updating many policies and procedures to address identified control weaknesses, reducing the number of outstanding vulnerabilities, and most notably, assessing and authorizing the operations of major agency systems. In order to continue addressing outstanding information security control issues and ensure the agency is compliant with applicable security requirements, the agency should develop a plan to fully implement an acceptable government-wide security framework, and work to develop a sufficiently mature FEC information security program.

Furthermore, a recent vulnerability report of FECs internal and external networks concludes that FEC is at risk of an internal user visiting a malicious website or clicking on a link in a phishing attack that would allow an external attacker to gain access to the FEC internal network. Consequently, the agency recently encountered a similar issue where an employee was terminated for downloading prohibitive software on their FEC issued laptop. This unforeseen event elevated the risk for malware or viruses to be injected into FEC networks which prompted FEC management to partner with the Cybersecurity and Infrastructure Security Agency (CISA) to provide an assessment to determine if an intrusion occurred within the FEC's network environment. As a result, the CISA team found no threat actor activity but recommended, among other things, that the FEC implement strict Network Access Control policies and review its Trusted Internet Connection data flow architecture.

The OIG supports the requirement for management to focus attention to these types of issues and improve the agencies IT cybersecurity framework and strengthen internal controls to mitigate external threats from entering the network. In addition to the need to prioritize cybersecurity, the OIG identifies an opportunity to restructure the agencies Information Security Office to ensure the agency meets its mission requirements efficiently and effectively.

³ Image generated from <https://www.nist.gov/cyberframework>.

Management Challenge #3: Lack of full-time support to Chief Information Officer (CIO) position and vacancies to key leadership positions

Currently, the senior leadership roles of the Staff Director and CIO are occupied by the same individual. As a result, there are several reported control weaknesses within the FEC's information security program that have been identified and reported in several OIG reports, with a few recommendations remaining outstanding. Information technology is ever-evolving, which affects all government agencies and without a fully dedicated CIO to focus on these issues to ensure resources are properly allocated, and adequate processes are in place for the protection and safety of the agency, the agency will remain at high risk for fraud, waste, and abuse. Based on the foregoing, we encourage the agency to hire or appoint someone to carry out the agency CIO duties on a full-time basis.

While we acknowledge that the FEC has filled several key leadership positions (Chief Financial Officer, IG, and Deputy CIO), the agency continues to operate with vacancies to essential senior leader and management positions. Many of these positions are staffed with personnel in an acting capacity, which creates an unstable environment which increases the risk for noncompliance and creates inconsistency within the department. This has potential to put the agency at risk and inhibit the agency to efficiently meet its mission requirements.

Additionally, failure to fulfill these key leadership positions in a timely manner creates resource constraints. As a result, position voids are created with those in long-term acting positions which limits the management and oversight of personnel and operations.

The following critical FEC senior leadership and key management level positions are currently vacant or occupied by staff in an acting capacity:

- General Counsel
- Director of Human Resources (vacancy announced September 2019)
- Accounting Director
- Deputy General Counsel for Law
- Deputy Chief Information Officer of Operations
- Assistant Staff Director for the Audit Division
- Secretary and Clerk of the Commission

As many of these positions require specialized knowledge and skills to ensure office operations are effectively and efficiently supporting the overall mission of the agency, assigning acting personnel to many of these vacant positions on a long term basis is not an efficient solution. It is imperative that the agency Personnel Committee elevate the importance of fulfilling these vacant senior leader and management positions as a priority to ensure consistency and clear direction in the leadership of the agency.

Management Challenge #4: Address outstanding OIG audit recommendations

As depicted in the image below, the OIG currently has 40 outstanding audit recommendations dating back to 2010. FEC management has worked towards addressing and completing 11 recommendations since April 2019 but key recommendations continue to remain open.

OIG Audits/Inspections	Total Outstanding Recommendations as of March 31, 2019	Total Closed Recommendations (Apr 1 - Sep 2019)	Total Open as of September 2019 ⁴
2010 Follow-up Audit of Privacy and Data Protection <i>8 years outstanding⁵</i>	20	3	17
2010 Follow-up Audit of Procurement and Contract Management <i>7 years outstanding</i>	1	1	0
Inspection of the FEC's Disaster Recovery Plan and Continuity of Operations Plans <i>6 years outstanding</i>	7	0	7
Audit of the FEC's Office of Human Resources <i>5 years outstanding</i>	3	1	2
Inspection of FEC's Compliance with FMFIA/OMB A-123 <i>4 years outstanding</i>	2	1	1
Audit of the FEC Telework Programs <i>2 years outstanding</i>	7	5	2
Required Review Under the DATA Act <i>1.5 years outstanding</i>	3	0	3
Outstanding Recommendations from prior Annual Financial Statement Audits ⁶ <i>At least 1 year outstanding</i>	8	0	8
Totals	51	11	40
Total Outstanding Recommendations			<u>40</u>

⁴ FEC management has not adequately implemented the remaining recommendations and therefore, continue to remain open.

⁵ Timelines are calculated based on the final report issuance date.

⁶ OIG recommendations are tracked, reviewed, and updated during the annual financial statement audit. 33 (65%) of the recommendations have been outstanding for at least 4 years.

For example, currently the FEC's annual financial statement audit includes eight outstanding recommendations attributed to prior financial statement audits, of which several relate to the security of FEC information, that were reported since FY 2004. In addition, follow-up to the 2013 OIG audit report, *Inspection of the FEC's Disaster Recovery Plan and Continuity of Operations Plan*, and the 2010 *Follow-up Audit of Privacy and Data Protection* continue to note outstanding recommendations that identify areas of high risk to agency information and the continuity of operations. It is essential that all federal agencies protect personal identifiable information (PII) and restrict access to data in accordance with applicable guidance. The agency should devote attention to address the outstanding recommendations in efforts to ensure adequate internal controls are identified, documented, and implemented.

Management Challenge #5: Address results from the annual FEVS and 2016 Root Causes of Low Employee Morale Study

In the OPM Human Capital Management Evaluation report of the FEC dated August 13, 2019, OPM identified that FEC lacks a formal process for using FEVS results to inform management decisions and focus improvement efforts. As a result of the *2016 Root Causes of low Employee Morale Study*, the agency continues to make strides in improving agency morale through the improvements in management training, professional development, and increased communications. However, the OIG believes that implementing a formal process to address employee concerns would further benefit the agency and increase employee morale. Specifically, management should focus on FEC FEVS satisfaction scores that were significantly less than similarly sized agencies. Management should continue to develop and implement action plans to address these concerns which have potential to hinder efficiency and effectiveness.

Conclusion

The OIG presents these challenges as previous and evolving issues facing the FEC in FY 2019 and FY 2020. This report echoes previous management challenges reported over the last few years. However, the lack of a quorum is a new challenge facing the agency and has potential to further impact, among other things, the key challenges identified in this report. The challenges serve as impending barriers to promote efficiency and effectiveness in the management of FEC operations and procedures. The OIG remains dedicated to provide independent oversight to ensure accountability of the mission of the FEC.

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 1050 First Street, N.E., Suite 1010, 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.