FEDERAL ELECTION COMMISSION

OFFICE OF INSPECTOR GENERAL

FINAL REPORT

Audit of the Federal Election Commission's Fiscal Year 2013 Financial Statements

December 2013

ASSIGNMENT No. OIG-13-02

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

MEMORANDUM

TO: The Commission

FROM: Inspector General

SUBJECT: Audit of the Federal Election Commission's Fiscal Year 2013 Financial Statements

DATE: December 13, 2013

Pursuant to the Chief Financial Officers Act of 1990, commonly referred to as the "CFO Act," as amended, this letter transmits the Independent Auditor's Report issued by Leon Snead & Company (LSC), P.C. for the fiscal year ending September 30, 2013. The audit was performed under a contract with, and monitored by, the Office of Inspector General (OIG), in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and applicable provisions of Office of Management and Budget (OMB) Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements*.

Opinion on the Financial Statements

LSC audited the balance sheet of the Federal Election Commission (FEC) as of September 30, 2013 and the related statements of net cost, changes in net position, budgetary resources, and custodial activity (the financial statements) for the year then ended. The objective of the audit was to express an opinion on the fair presentation of those financial statements. In connection with the audit, LSC also considered the FEC's internal control over financial reporting and tested the FEC's compliance with certain provisions of applicable laws and regulations that could have a direct and material effect on its financial statements. The financial statements of the FEC as of September 30, 2012, were also audited by LSC whose report dated November 14, 2012, expressed an unqualified opinion on those statements.

In LSC's opinion, the financial statements present fairly, in all material respects, the financial position, net cost, changes in net position, budgetary resources, and custodial activity of the FEC as of, and for the year ending September 30, 2013, in conformity with accounting principles generally accepted in the United States of America.

Report on Internal Control

In planning and performing the audit of the financial statements of the FEC, LSC considered the FEC's internal control over financial reporting (internal control) as a basis for designing auditing procedures for the purpose of expressing their opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the FEC's internal control. Accordingly, LSC did not express an opinion on the effectiveness of the FEC's internal control.

Because of inherent limitations in internal controls, including the possibility of management override of controls; misstatements, losses, or noncompliance may nevertheless occur and not be detected. According to the American Institute of Certified Public Accountants:

- A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.
- A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is a more than remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected by the entity's internal control.
- A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control.

LSC's consideration of internal control was for the limited purpose described in the first paragraph in this section and would not necessarily identify all deficiencies in internal control that might be significant deficiencies or material weaknesses. LSC did not identify any deficiencies in internal control that LSC would consider to be material weaknesses, as defined above. However, LSC did identify a significant deficiency in internal controls related to Information Technology security.

Report on Compliance with Laws and Regulations

FEC management is responsible for complying with laws and regulations applicable to the agency. To obtain reasonable assurance about whether FEC's financial statements are free of material misstatements, LSC performed tests of compliance with certain provisions of laws and regulations, noncompliance which could have a direct and material effect on the determination of financial statement amounts, and certain other laws and regulations specified in OMB Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements*. LSC did not test compliance with all laws and regulations applicable to FEC.

The results of LSC's tests of compliance with laws and regulations described in the audit report disclosed one instance of noncompliance with The Homeland Security Presidential Directive 23, and National Security Presidential Directive 54, *Cyber Security and*

Monitoring, establishing the Comprehensive National Cyber Security Initiative (the CNCI), and relating to Initiative No. 1, *Manage the Federal Enterprise Network as a Single Enterprise with a Trusted Internet Connection (TIC)*. Additional details can be found on page 25 of the audit report.

Audit Follow-up

The independent auditor's report contains recommendations to address deficiencies found by the auditors. Management was provided a draft copy of the audit report for comment and generally concurred with some of the findings and recommendations. In accordance with OMB Circular No. A-50, *Audit Follow-up*, revised, the FEC is to prepare a corrective action plan that will set forth the specific action planned to implement the agreed upon recommendations and the schedule for implementation. The Commission has designated the Chief Financial Officer to be the audit follow-up official for the financial statement audit.

OIG Evaluation of Leon Snead & Company's Audit Performance

We reviewed LSC's report and related documentation and made necessary inquiries of its representatives. Our review was not intended to enable the OIG to express, and we do not express an opinion on the FEC's financial statements; nor do we provide conclusions about the effectiveness of internal control or conclusions on FEC's compliance with laws and regulations. However, the OIG review disclosed no instances where LSC did not comply, in all material respects, with *Government Auditing Standards.*

We appreciate the courtesies and cooperation extended to LSC and the OIG staff during the audit. If you should have any questions concerning this report, please contact my office on (202) 694-1015.

Lynne A. McFarland
Inspector General

Attachment

Cc: Judy Berning, Acting Chief Financial Officer
Alec Palmer, Staff Director/Chief Information Officer
Gregory Baker, Deputy General Counsel for Administration
Lisa Stevenson, Deputy General Counsel for Law

Federal Election Commission

Audit of Financial Statements

As of and for the Years Ended September 30, 2013 and 2012

Submitted By

Leon Snead & Company, P.C.
Certified Public Accountants & Management Consultants

TABLE OF CONTENTS

Page

Independent Auditor's Report.....1

Report on Internal Control.....3

Report on Compliance.....25

Attachment 1, Status of Prior Year Recommendations.....29

Attachment 2, Agency Response to Report.....32

LEON SNEAD
& COMPANY, P.C.

Certified Public Accountants
& Management Consultants

416 Hungerford Drive, Suite 400
Rockville, Maryland 20850
301-738-8190
Fax: 301-738-8210
leonsnead.companypc@erols.com

Independent Auditor's Report

THE COMMISSION, FEDERAL ELECTION COMMISSION
INSPECTOR GENERAL, FEDERAL ELECTION COMMISSION

We have audited the accompanying financial statements of Federal Election Commission (FEC), which comprise the balance sheet as of September 30, 2013 and 2012, and the related statements of net cost, changes in net position, budgetary resources, and custodial activity for the years then ended. The objective of our audit was to express an opinion on the fair presentation of those financial statements. In connection with our audit, we also considered the FEC's internal control over financial reporting and tested the FEC's compliance with certain provisions of applicable laws, regulations, and certain provisions of contracts.

SUMMARY

As stated in our opinion on the financial statements, we found that the FEC's financial statements as of and for the years ended September 30, 2013 and 2012, are presented fairly, in all material respects, in conformity with accounting principles generally accepted in the United States of America.

Our consideration of internal control would not necessarily disclose all deficiencies in internal control over financial reporting that might be material weaknesses under standards issued by the American Institute of Certified Public Accountants. Our testing of internal control identified no material weaknesses in financial reporting.

However, we identified significant deficiencies related to the IT security program established by the FEC. We also noted one other control issue that did not rise to the level of a reportable condition in a separate letter dated December 12, 2013, for management's consideration.

Our tests of compliance with certain provisions of laws, regulations, and contracts disclosed one instance of noncompliance that is required to be reported under *Government Auditing Standards* and the OMB Bulletin 14-02, *Audit Requirements for Federal Financial Statements*. The issue deals with noncompliance with The Homeland Security Presidential Directive 23 and National Security Presidential Directive 54, *Cyber Security and Monitoring*, establishing the Comprehensive National Cyber Security Initiative (the CNCI), and relating to Initiative No. 1, *Manage the Federal Enterprise Network as a Single Enterprise with a Trusted Internet Connection (TIC).*

The following sections discuss in more detail our opinion on FEC's financial statements, our consideration of FEC's internal control over financial reporting, our tests of the FEC's compliance with certain provisions of applicable laws and regulations, and management's and our responsibilities.

REPORT ON THE FINANCIAL STATEMENTS

We have audited the accompanying financial statements of FEC, which comprise the balance sheets as of September 30, 2013 and 2012, and the related statements of net cost, statements of changes in net position, statements of budgetary resources, and statements of custodial activity for the years then ended, and the related notes to the financial statements.

Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of FEC as of September 30, 2013 and 2012, and the related net cost, changes in net position, budgetary resources, and custodial activity for the years then ended in accordance with accounting principles generally accepted in the United States of America.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America. Such responsibility includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to error or fraud.

Auditor's Responsibility

Our responsibility is to express an opinion on the financial statements based on our audit. We conducted our audit in accordance with auditing standards generally accepted in the United States of America; standards applicable to financial statement audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and OMB Bulletin 14-02, *Audit Requirements for Federal Financial Statements* (the OMB audit bulletin). Those standards and the OMB audit bulletin require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments in a Federal agency, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing opinions on the

effectiveness of the FEC's internal control or its compliance with laws, regulations, and significant provisions of contracts. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

REQUIRED SUPPLEMENTARY INFORMATION

Accounting principles generally accepted in the U.S. require that Management's Discussion and Analysis be presented to supplement the basic financial statements. Such information, although not a part of the basic financial statements, is required by the Federal Accounting Standards Advisory Board (FASAB) who considers it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic, or historical context. We have applied certain limited procedures to the required supplementary information in accordance with auditing standards generally accepted in the United States of America, which consisted of inquiries of management about the methods of preparing the information and comparing the information for consistency with management's responses to our inquiries, the basic financial statements, and other knowledge we obtained during our audit of the basic financial statements. We do not express an opinion or provide any assurance on the information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

OTHER ACCOMPANYING INFORMATION

Our audit was conducted for the purpose of forming an opinion on the basic financial statements taken as a whole. The performance measures and other accompanying information are presented for the purposes of additional analysis and are not required parts of the basic financial statements. Such information has not been subjected to the auditing procedures applied in the audit of the basic financial statements, and accordingly, we do not express an opinion or provide any assurance on it.

OTHER AUDITOR REPORTING REQUIREMENTS

Report on Internal Control

In planning and performing our audit of the financial statements of FEC as of and for the years ended September 30, 2013 and 2012, in accordance with auditing standards generally accepted in the United States of America, we considered the FEC's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the FEC's internal control. Accordingly, we do not express an opinion on the effectiveness of the FEC's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies, and therefore material weaknesses or significant deficiencies may exist that were not identified. However, given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be a material weakness. As discussed below, we identified certain deficiencies in internal control that we consider to be significant deficiencies.

Because of inherent limitations in internal controls, including the possibility of management override of controls, misstatements, losses, or noncompliance may nevertheless occur and not be detected. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Findings and Recommendations

1. **Failure to Develop a Strong IT Security Program Places FEC at High Risk of Continued Network Intrusions**

   FEC's IT security program does not meet government-wide best practice minimum security requirements in many areas. We attributed this serious internal control vulnerability to FEC's officials failure to establish a process that would ensure that Office of the Chief Information Officer (OCIO) exercise due diligence with regard to the establishment of information security and risk management[1] controls within the agency. As a result, FEC's information and information systems have serious internal control vulnerabilities and have been penetrated at the highest levels of the agency, while FEC continues to remain at high risk for future network intrusions.

[1] Information security due diligence includes using all appropriate information as part of an organization-wide risk management program. Using the risk management tools and techniques that are available to organizations is essential in developing, implementing, and maintaining the safeguards and countermeasures with the necessary and sufficient strength of mechanism to address the current threats to organizational operations and assets, individuals, other organizations, and the Nation. Employing effective risk-based processes, procedures, and technologies will help ensure that all federal information systems and organizations have the necessary resilience to support ongoing federal responsibilities, critical infrastructure applications, and continuity of government.

a. Risk Analysis Not Completed Before Rejection of Minimum IT Security Controls

The FEC, unlike other federal agencies that are exempt from the Federal Information Security Management Act (FISMA)[2], has refused to adopt as the agency's IT security standard the IT security controls and techniques released by the National Institute of Standards and Technology (NIST). For instance, the Government Accountability Office (GAO), like FEC, is exempt from FISMA compliance, but has adopted the NIST security requirements. GAO stated[3] that it "adheres to federal information security governance, such as OMB and National Institute of Standards and Technology guidance." While FEC officials have advised that the agency follows NIST best practices "where applicable to their operations," independent evaluations performed since fiscal year 2004 have continually reported significant weaknesses and noncompliance with IT best practice standards within FEC's IT security program areas reviewed.

FEC will remain at high risk for intrusions and data breaches unless it fundamentally changes its governance and management approach, and adopts a risk-based IT security program that is based upon the federal government's IT security control standard – National Institute of Standards and Technology (NIST) best practices, to include:

- Federal Information Processing Standards (FIPS) 199, *Standards for the Security Categorization of Federal Information and Information Systems*,
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*,
- Special Publication (SP) 800-53, *Recommended Security Controls for Federal Systems and Organizations*, and
- Related Federal Information System Management Act (FISMA) security documents.

FEC officials have indicated that the agency makes informed decisions when deciding whether to adopt government-wide IT security requirements. However, our audits have shown that FEC does not have a policy document that requires a risk-based analysis to support the agency's decision to not adopt a minimum government-wide IT security requirement, and we were unable to find any evidence that such reviews were, in fact, performed prior to the agency refusing to adopt the IT security requirement. As further support, we identified other

[2] The E-Government Act (P.L. 107-347) recognizes the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets.

[3] GAO Performance and Accountability Report – 2011, page 58.

independent evaluations[4] performed since fiscal year 2004 that have reported significant deviations in FEC's IT security program from minimum accepted best practice IT security controls.

Without a risk-based analysis and supporting evidence, FEC's critical IT security decisions are based upon whether the agency is exempt from the legislative requirement, rather than assessing if the control would provide an effective reduction of risks to the FEC's information and information systems.

For example, while FEC is required to follow the Federal Acquisition Regulations (FAR), the FEC refuses to adopt FAR requirements relating to requiring specific IT security controls and processes to be included in government contracts. FEC has exempted itself from compliance with the FAR sections requiring specific (FISMA based) IT security standards for contractors. The NIST best practice requirements are meant to provide the federal government with uniform and cost-effective IT security controls that contractors must meet to ensure that an agency's information systems and information are appropriately secured.

This significant deficiency places FEC's information and information systems that are operated, and/or accessible by contractors at significant unnecessary risk, and greatly increases the potential for data intrusions and loss or manipulation of sensitive information.

Recommendations

1. Formally adopt as a model for FEC, the NIST IT security controls established in FIPS 199, FIPS 200, SP 800-53, and other applicable guidance that provides best practice IT security control requirements

   FEC Response

   OCIO officials advised that, even though the FEC is exempt from FISMA, the OCIO partially agrees with this recommendation, and noted that the IT Security Officer will review NIST 800-53 for implementation in FY 2014. The OCIO officials advised that they do not agree to formally adopt NIST guidelines.

   Auditor Comments

   While OCIO officials have advised that they will "review" the NIST minimum control requirements, they have again stated that they will not adopt the federal government's minimum IT security controls best practices. Until FEC adopts these minimum controls, as other federal agencies have done that are also exempt, FEC will remain at high risk.

[4] A security control assessment report, issued to FEC by an independent contractor in December 2008 found that 40 percent of the IT security controls applicable to FEC's IT environment had been only partially implemented, or not implemented at all. The Office of Inspector General (OIG) in 2004 as part of reporting required by the *Chief Financial Officers (CFO) Act of 1990* first identified information technology security as a challenge that has raised serious concerns about the effectiveness of FEC's IT security program.

2. Revise FEC policies to require that FEC contractors adhere to the FAR requirements which adopt FISMA and NIST IT security controls that contractors must follow when providing services to the federal government.

FEC Response

OCIO officials advised that they "do not understand the actual purpose of this finding. Auditors have not demonstrated how including a FAR statement will help improve the security posture of FEC. OCIO disagrees with this recommendation. As a FISMA exempt agency, the FEC incorporates language and is supported by FAR clauses that address the level of security necessary to safeguard agency security in all of its contracts. This language was agreed to by the agency contracting officer and ISSO. Contractors are required to adhere to the same level of security as FEC employees."

Auditor Comments

FEC is required to follow the FAR. However, OCIO officials cite the agency's FISMA exemption as the reason for not implementing IT security controls. It appears that regardless of the regulation or the control, if the matter relates to the FISMA, FEC officials exempt the agency. The decision to exempt the agency from required IT security controls appears to be made without any analysis of the costs, or the actual or potential harm to FEC by not implementing the security control or process.

In addition, as discussed in this report, FEC's IT security policies do not meet the minimum federal government's "best practice" IT security controls. Therefore, we continue to believe that the FEC should follow FAR requirements that mandate use of applicable "best practice" IT security controls in all contracts.

3. Revise FEC policies and procedures to require a documented, fact-based, risk assessment prior to declining adoption of any government-wide IT security best practice, or IT security requirement, including those that FEC may be legally exempt. Require the Chief Information Officer (CIO) to approve, and accept the risk of any deviation from government-wide IT security best practices that are applicable to the FEC business operations. Retain documentation of these decisions.

FEC Response

OCIO officials advised that they partially agree with this recommendation, and will review applicable NIST 800-53 for possible implementation in FY 2014. The FEC advised that any actions taken will be based on obtaining additional personnel resources. Further, all FISMA implementation must be approved by the commission since the FEC is legally exempt from FISMA.

Auditor Comments

We continue to believe that FEC's information systems and information would be significantly more secure if the agency adopted the federal government's

minimum IT security controls best practices, Presidential Directives on IT security, and OMB directives that provide guidance on strengthening the federal government's IT security posture. We disagree that adoption of the IT security controls best practices would require Commission approval because the FEC is legally exempt. In fact, in a June 1, 2011, memorandum to the Acting Staff Director, the FEC Office of General Counsel noted that the FEC could voluntarily adopt an IT operational policy issued by the federal government's Chief Information Officer as a best practice even though the FEC is specifically exempt from the guidance. Further, the CIO has a responsibility to ensure the FEC's information and information systems are properly protected, and thus implementation of the best practices would be in line with this responsibility. Until FEC fully adopts best practice IT controls, the agency will remain at high risk of further intrusions and data breaches.

b. Refusal to Adopt Government-wide IT Controls Increased Risks of Intrusions

FEC has experienced several serious data intrusions and information breaches in the last few years. During our audit, we obtained information on two intrusions and information data breaches that are briefly discussed below. Our analysis indicates that if FEC had implemented government-wide minimum best practice IT security controls, these intrusions and breaches may have prevented and/or more timely detected. Details of the two most serious matters follow:

Intrusion No. 1

In May 2012, the FEC was a victim of a network intrusion by an Advanced Persistent Threat (APT)[5]. Several FEC systems and a Commissioner's user account were compromised by this specific threat. For approximately eight months, the Commissioner's computer contained malware with the potential for a computer hacker to access and obtain copies of:

- Matters Under Review by the agency, and not made public until final decisions are made, and would include such sensitive information as General Counsel's reports and briefs, subpoenas, and other similar items;
- Specific details on the agency review processes, such as specifics on the criteria used for a committee to be referred to the Alternative Dispute Resolution (ADR); and specific dollar value variances of violations that result in inclusion in public audit reports; and

[5]According to NIST SP 800-39, an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of obtaining information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives. The contractor also identified two additional systems that were infected, but were not shown as APT type threats.

- Any sensitive FEC documentation and sensitive personal identifiable information.

Although the contractor was unable to identify if the above sensitive information was actually accessed by the intrusion, the opportunity did exist. The agency hired a contractor to analyze this serious intrusion on FEC's IT systems, and to provide recommended solutions to eliminating any threat discovered by the contractor. The contractor completed the analysis, and provided a report to FEC on October 5, 2012. The contractor made a significant number of recommendations, including that FEC should complete the actions by the end of October 2012. However, when we requested documentation of the actions taken by FEC to implement the report's recommendations, almost one year after the report was issued, we were advised by FEC officials that the agency had not yet implemented any significant portion of the contractor's recommendations.

Intrusion No. 2

In August 2013, the FEC was notified of an intrusion to the FEC's website (FEC.gov). The FEC had to disable use of certain features of the website to conduct an analysis of the intrusion. FEC is currently receiving technical expertise to analyze the extent of the breach and its impact. As FEC was working on remediating the August 2013 intrusion, another intrusion was detected on the agency's website in early fiscal year 2014.

Recommendations

4. Using the initial Corrective Action Plan (CAP) developed by the Chief Information Security Officer as a base, implement each of the contractor's recommendations in the October 2012 *Threat Assessment Program* report, and complete all remedial actions (i.e. changing of all user passwords) within the next 60 days, and all other tasks by February 2014. Provide sufficient budgetary and personnel resources to this project to ensure that actions are properly accomplished.

FEC Response

OCIO officials advised that they are moving as quickly as possible on the recommendations made by the contractor. OCIO has stated that several of the recommendations have been implemented and they are working diligently to implement the others as necessary.

Auditor Comments

The current FEC remediation plan, provided to us in late October 2013, shows that FEC has now begun to address recommendations in the contractor's report. We continue to believe that the FEC's IT security program would be significantly strengthened by implementing all of the report's recommendations as soon as possible.

5. Provide biweekly updates to the CIO on the status of the implementation of the October 2012 *Threat Assessment Program* report recommendations to ensure that it continues on track, and issues that arise are addressed as soon as possible.

   FEC Response
   OCIO officials advised that they agree with this recommendation, and have assigned a staff person to provide a biweekly status update to the CIO.

   Auditor Comments
   Since OCIO officials have agreed to implement this recommendation, we have no additional comments.

6. Provide semiannual corrective action plan (CAP) updates to the Commission on the status of the implementation of the October 2012 Threat Assessment Program report recommendations in accordance with Commission Directive 50.

   FEC Response
   OCIO officials advised that they will continue to update the Commission concerning CAPs on a semi-annual basis through the Commission Secretary's Office.

   Auditor Comments
   We believe that the importance of implementing the recommendations in the contractor's report should be discussed with the Commission on a regular basis. Therefore, not only should management continue to provide the Commission with updates for the financial statement audit CAP, but the CAP developed by the CISO regarding the October 2012 *Threat Assessment Program* report should also be provided.

7. Revise all pertinent FEC policies and procedures to ensure that they address proper prevention and detection controls, and provide a current and authoritative control structure for addressing APT, and other types of intrusions. Ensure that this review is completed, and policies and procedures are issued by March 2014.

   FEC Response
   OCIO officials agree with this recommendation. OCIO officials stated that they will review FEC policies and procedures to ensure they are aligned with the agency's current practices. OCIO officials further noted that FEC is working with the Department of Homeland Security (DHS), and is also purchasing additional tools and capabilities to address possible vulnerabilities and strengthen the FEC infrastructure.

   Auditor Comments
   Since OCIO officials agreed to implement this recommendation, we have no additional comments.

2. Oversight and Monitoring of IT Corrective Actions are Ineffective

FEC has failed to implement agreed upon corrective actions to address IT security vulnerabilities that have, in some cases, been outstanding for approximately five years. We attributed this significant internal control weakness to the lack of emphasis placed on the audit corrective action process by FEC officials; the need for more effective oversight and monitoring of IT operations by FEC officials; and the need for updated IT policies relating to this area. As a result, FEC's information and information systems continue to be at high risk for further intrusions and data breaches.

The OIG has expressed similar concerns about the lack of prompt and effective corrective actions in several reports. For example, the OIG in a June 2013, report advised:

> "Currently, the FEC lacks the accountability necessary to ensure compliance with all aspects of (FEC) Directive 50: Audit Follow-Up. It is essential that the Commission not only requires management to report on a semi-annual basis the status of outstanding recommendations, but also develop 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. Without the 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."

Audit follow-up, to include the timely implementation of audit recommendations, is required by Office of Management and Budget Circular A-50, *Audit Follow-up*, as revised, and FEC Directive 50. The FEC directive requires FEC officials 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;
> (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…."

OMB Circular A-50, paragraph 10 requires agencies to "Assure that performance appraisals of appropriate officials reflect effectiveness in resolving and implementing audit recommendations."

Finally, OMB Circular A-123, *Management's Responsibility for Internal Control*, Section V. provides that agency managers are responsible for taking timely and effective action to correct deficiencies; correcting deficiencies is an integral part of

management accountability and must be considered a priority by the agency; corrective action plans should be developed for all material weaknesses, and progress against plans should be periodically assessed and reported to agency management. Management should track progress to ensure timely and effective results. A-123 also provides that "As managers consider IG and GAO audit reports in identifying and correcting internal control deficiencies, they must be mindful of the statutory requirements for audit follow-up included in the IG Act, as amended and OMB Circular A-50, Audit Followup. Management has a responsibility to complete action, in a timely manner, on audit recommendations on which agreement with the IG has been reached."

Due to the lack of emphasis placed on the audit corrective action process, OCIO has not implemented agreed upon corrective actions to address IT security vulnerabilities. During our FY 2013 Financial Statement Audit, we found that OCIO officials have not taken action on most of the audit recommendations contained in the 2012 and prior years' FEC financial statement audit reports, nor have they implemented corrective actions on critical issues identified in an independent contractor's internal control report.

Recommendations

8. Assure that the annual performance plans of all appropriate audit follow-up officials reflect their responsibility to monitor and ensure the timely implementation of audit recommendations, as required by OMB Circular A-50.

   FEC Response
   OCIO officials advised that because performance plans for FY 2014 have already been developed and implemented, the OCIO will revisit this recommendation in FY 2015.

   Auditor Comments
   We believe that the issues noted in this report, and in OIG's management challenges included in FEC's 2012 Performance and Accountability Report (PAR), and other OIG reports, show that FEC has not placed sufficient emphasis on implementing corrective actions to address reported internal control weaknesses. This problem can be best illustrated by the failure to take any actions on a critical contractor's report that addressed a serious intrusion into FEC's information systems at the highest levels of governance within the agency. Appropriate FEC officials, as required by OMB A-50, should be evaluated on implementation of corrective actions in a timely manner. We believe this recommendation should be implemented immediately.

9. Require the audit follow-up official to develop a tracking process that would include monthly reports to the CIO, and highlight key tasks, progress, and missed target dates, when applicable.

FEC Response

OCIO advised that they agree with this recommendation and have assigned an individual to track audit follow-up actions, that the status meetings will be recorded to show the progress of this recommendation.

Auditor Comments

Since OCIO officials agreed to implement this recommendation, we have no additional comments.

During this year's audit, we conducted follow-up testing to determine the status of prior years' reported significant deficiencies, and the status of these significant deficiencies are outlined below.

a. After Five Years, FEC Has Made No Progress in Implementing a System to Recertify Users' Access Authorities

While FEC agreed in 2009 to implement an annual recertification of users' access authorities to the FEC network and applications, as we disclosed in each subsequent audit, including our 2013 follow-up testing, FEC has made no progress implementing a process for recertifying users' access authorities. During our 2013 audit, we were advised by the Deputy Chief Information Officer (DCIO) for Operations that the agency no longer agrees to periodically review users' access authorities. We noted that this decision conflicts with FEC IT policy and prior management responses.

IT policy 58-2.2, *Account Management Policy*, states "All user account access rights and privileges will be periodically reviewed and validated in accordance with General Support System...system security plans..." The security plan for the General Support System, dated 2009, contains a control requirement that the users' accounts will be reviewed every six months.

Subsequently, we met with the Chief Information Officer (CIO) in mid-August 2013, to discuss the lack of corrective actions taken by the agency on this and other problem areas. We were advised by the CIO that subsequent to our meeting with the Deputy CIO for Operations, the FEC was taking a new look at the prior year's audit recommendations. Information was then provided that indicated that the Office of the CIO may begin to send information to users' supervisors to review access authorities; however, this review has not yet been implemented and there were no details provided on how the system would work or when the control would be implemented. Currently, FEC is not compliant with best practices, and officials do not have assurance that users only have access to information and information systems that are necessary to accomplish job responsibilities. The importance of this control process can be illustrated by recent data breaches of FEC information and information systems, as follows:

- In July 2012, an FEC employee discovered that they had unauthorized access to personnel-related files, labor management files, and Administrative Law files.
- In November 2012, it was determined that an FEC employee retained access to OGC files for two years after being transferred from OGC to another office within FEC.

Had FEC implemented the audit recommendation as it agreed to do in 2009, an effective review of user access authorities could have detected these problems.

Recommendations

10. Establish a project with the project manager reporting to the CIO to help ensure that this long-delayed project will be implemented within the next three months. Require the project director to provide biweekly updates to the CIO. Provide necessary budgetary and personnel resources to ensure that this project is completed timely.

    FEC Response
    OCIO officials advised that they have assigned an individual as the Project Coordinator for this recommendation. This individual will work with the IT Security Officer to report biweekly status updates to the CIO. Review of users' access will be implemented at the end of November.

    Auditor Comments
    Since OCIO officials agreed to this recommendation, we have no additional comments.

11. Reissue FEC Policy 58-2.2 to require annual recertification of users' access authorities by supervisory personnel who would have knowledge of the users' requirements for accessing FEC information and information systems. Ensure that the policy contains sufficient operational details to enable an effective review and update process.

    FEC Response
    OCIO advised that they concur with this recommendation. OCIO officials noted that the agency will send a report to data owners to verify user access authorities in mid-December; however, managers and data owners are accountable to report access changes to OCIO.

    Auditor Comments
    OCIO officials agreed to this recommendation. However, before the recommendation can be closed, additional information is needed concerning the process that will be used in ensuring that this control is effectively implemented with the agency.

b. Access Control Weaknesses Pose a Risk to FEC's Information and Information Systems

Access controls established by FEC are weak, and provide vulnerabilities that could be exploited. We have reported significant user control weaknesses within FEC's IT security program since 2009. The problems we reported with FEC's access controls, and the actions taken by FEC to remediate the problem, if any, are discussed in the following paragraphs.

- **Accounts with Passwords that Never Expire:** FEC officials had not taken action to address the issues we noted in our prior audit dealing with approximately 140 accounts that did not have a password expiration date; a large percentage of these accounts have not had their password changed for years, and contained some form of administrator[6] authority.

  In response to our 2012 audit report, the Deputy CIO for Operations advised that the OCIO agreed in part with these recommendations, and that the FEC would complete a review of those accounts by July 2013. However, when we requested documentation to support the corrective actions taken on these problems in August 2013, we found that no actions had yet been taken by OCIO officials.

- **Processes for Assigning Replacement and Initial Passwords[7]:** During our audit, we requested all FEC policies and operating procedures relating to the assignment of replacement and initial passwords for testing. We were advised by OCIO officials that the FEC did not have detailed written policies or operating procedures for establishing initial account passwords or replacement passwords. OCIO officials stated that "When systems administrators (SAs) are notified, through the FEC System Access **(**FSA), that there is a need to establish an account, the SA then establishes an account with a generic password of his or her choosing; this password is not recorded for security reasons. Then either through the new hire orientation program, or through the help desk, the person is instructed to change this password and it must be changed before access to the system is granted."

  The absence of specific FEC policies and operating procedures prevents FEC from setting requirements for this important area, and unnecessarily places this area at risk.

[6] The term used for an account that has privileges that normal accounts do not. In most cases, for the system or network on which it is located, the account could have almost unlimited authority.

[7] These terms are used to describe that part of the administration of password (authentication controls) when a predetermined (or generic) password is provided to a new user during initial login process and when replacement passwords are provided to existing users who are unable to login with an existing password (e.g. password is forgotten).

- **Login Passphrase for Contractors:** An audit report released by the Office of the Inspector General (OIG), *2010 Follow-Up Audit of Privacy and Data Protection, Federal Election Commission, Audit Report Number OIG-10-03*, contained a finding related to access controls. The OIG stated in their audit report,

  > "We were informed by the Information Systems Security Officer that encrypted laptops assigned to contractors use an encryption passphrase assigned by the FEC. …it appears the same passphrase is used for all contractors. The passphrase assigned to contractors is not suitably complex, is relatively intuitive, and could be easily guessed or "hacked" by using basic password detection or "cracking" software. The lack of a unique secret passphrase for each individual increases the risk that the data on that laptop could be accessed by an unauthorized individual."

  We followed up on this issue and confirmed that the problem reported by the auditors in 2010 continued into FY 2013. For example, the same passphrase has been provided to us for use since 2009, and we were not required to change the passphrase. Therefore, we agree with the prior auditors' conclusion that this weakness substantially negates the effectiveness of this control.

  The CISO advised that the OCIO currently has the licenses needed to provide all users with their own unique passphrase, and believes that this item should be closed. However, as noted above, when we initiated the 2013 financial statement audit, we were provided the same login passphrase as we had used since 2009. The system did not require us to change the assigned password. Therefore, we believe that this problem has not yet been corrected.

Recommendations

12. Revise FEC policies and operating procedures to require the minimum best practices controls contained in the Federal Desktop Core Configuration (FDCC) and the United States Government Configuration Baseline (USGCB) for those systems that require user identification and passwords.

13. Undertake a comprehensive review of user accounts that have been granted non-expiring passwords. Require detailed information from account owners on the need for non-expiring accounts, including the development of other alternatives, before reauthorizing the accounts' access. Develop FEC policies and operating procedures to implement this recommendation.

14. Whenever possible, require accounts with non-expiring passwords to be changed at least annually. Establish substantially more robust password requirements for accounts granted non-expiring passwords. Develop FEC policies and operating procedures to implement this recommendation.

15. Immediately terminate those accounts with non-expiring passwords that have not accessed their accounts within the last 12 months. Develop FEC policies and operating procedures to implement this recommendation to include a data retention policy for historical data.

FEC Response Recommendations 12-15

OCIO officials advised that they concur with these recommendations. OCIO officials noted that they will investigate the feasibility, workload and impact of implementing this recommendation.

Auditor Comments

While OCIO officials advised that they concur with the recommendations, they further state that they plan to "investigate the feasibility" of the recommendations. We continue to believe that the recommendations should be fully implemented, and would further strengthen FEC's IT security program.

16. Strengthen controls over the establishment of initial and replacement (default) passwords, to include requiring that random passwords be used, and the default passwords used be changed monthly. Develop FEC policies and operating procedures to implement this recommendation.

FEC Response

OCIO officials advised that they do not believe that the current process presents security risks. The default password is created to aid the Help Desk team in the user orientation process. It is not the case that a user would be able to use the default password to login to a client machine without the aid of the Help Desk.

Auditor Comments

NIST SP 800-118, *Guide to Enterprise Password Management (Draft)*, provides that there are two types of techniques used to attack passwords: guessing and cracking. Guessing involves repeatedly attempting to authenticate using default passwords, dictionary words, and other possible passwords. NIST further provides that "Guessing attacks can be mitigated rather easily by using a combination of two methods. First, ensure that passwords are sufficiently complex so that attackers cannot readily guess them….Organizations should also ensure that other trivial passwords cannot be set, such as the username or person's name, "password," the organization's name, simple keyboard patterns, dates, dictionary words, and names of people and places."

NIST SP 800 notes that "…special case of password guessing is the use of default passwords for password resets, such as when accounts are first created. A password reset is often accomplished by setting a one-time password (OTP), which is a password that is set to expire immediately, and thus can only be used to gain access to a system one time. An example of how OTPs are used is a help desk staff member creating a new account. The help desk member sets an OTP

for an account and provides the OTP to the user. The user may log in with the OTP once, at which point the OTP expires and the user is required to set a new password. Randomly generated or arbitrarily chosen OTPs, not default or patterned passwords, should be used during account creation and password reset processes. This ensures that if the user does not promptly change the assigned password, that the password will not be easily guessable.

We believe the NIST publication supports that FEC should adopt this recommendation.

17. Establish written procedures and develop a policy for FEC contractor computer orientation that requires contractors to create their own unique login passphrase. Also, ensure that all current contractors have created their own unique login passphrase.

FEC Response

OCIO officials advised that it "disagrees with this finding," and "OCIO assigned a new passphrase to all users."

Auditor Comments

As discussed in this report, when we initiated the FY 2013 audit, our newly assigned laptops were assigned the same passphrase login being used by contractors since 2009. Therefore, management's assertion in their response that all users have been assigned a new passphrase is incorrect. We believe that FEC's control in this area is not operating effectively; OCIO does not have a control in place to determine if all contractors have established a unique passphrase. We continue to believe this recommendation should be implemented.

c. FEC's Vulnerability Scanning Program Needs Significant Strengthening to Further Reduce Risks

FEC's vulnerability scanning program did not meet best practices. We found during our 2013 audit that individual employees' workstations continued to be excluded from the scanning process, a significant omission. Additionally, system vulnerabilities identified from the scanning process were not timely mitigated.

Best practices address vulnerability scanning as one of the recommended security controls and part of the risk assessment process. For example, NIST recommends that organizations: "Analyze findings, and develop risk mitigation techniques to address weaknesses. To ensure that security assessments provide their ultimate value, organizations should conduct root cause analysis upon completion of an assessment to enable the translation of findings into actionable mitigation techniques. These results may indicate that organizations should address not only technical weaknesses, but weaknesses in organizational processes and procedures as well."

Without the scanning of individual workstations included as part of an effective scanning program, FEC cannot detect and correct vulnerabilities and assure that devices have proper security configurations. In addition, the failure to correct known vulnerabilities identified in the scanning process is a significant internal control weakness. These weaknesses and related uncorrected vulnerabilities present opportunities for intrusions into FEC's information and information systems. The lack of an effective agency wide scanning program, (that would include workstations, servers, applications, etc.), in our opinion, contributed to the control issues that allowed recent intrusions into FEC's website.

Recommendations

18. Include all components of the general support system (GSS), including employees' workstations, and other FEC devices and applications into the organization's vulnerability/security scanning process and ensure that they are assessed at least semi-annually.

19. Strengthen controls to ensure that vulnerabilities/weaknesses identified through the vulnerability scanning tests are completed within 60 days of identification, or document an analysis and acceptance of risks for longer term remediation.

FEC Response

OCIO officials agreed with this recommendation. OCIO officials advised that the agency is in the process of purchasing a software security application to ensure FEC assets are patched regularly. Any high vulnerability that cannot be patched in 60 days will be documented, and an acceptance memorandum will be created for CIO/designee signature on longer term remediation.

Auditor Comments

Since OCIO officials agreed to this recommendation, we have no additional comments.

d. Configuration Security Controls and FDCC/USGCB Requirements Need Strengthening

FEC needs to further strengthen its configuration security controls so that significant vulnerabilities do not continue to impact FEC's IT security program. Currently, the integrity of the FEC change management process relies on the manual recording of all system changes in an outside application, there is no tool in place to identify all changes made to the configuration of FEC's system, and there are no logs that collect changes made to the system. Therefore, there is reduced assurance that all changes are processed under the change management framework established, or that changes made outside the framework will be identified. Further, our current and prior audits found that while FEC has issued configuration baseline standards for a number of its systems; these standards have not been fully implemented.

The current FEC baseline configuration standards require that machines' "administrator account" be renamed and that access to administrator authorities be limited to only those users requiring such access. Based on the computer settings we reviewed, users had been given administrator rights allowing them to change local settings, such as disabling the screen saver and the ability to start "services" manually. By disabling the screen saver, users can override the communication control setting in which re-authentication (password) is required after a set period of inactivity. These settings do not adhere to the United States Government Configuration Baseline (USGCB), formerly referred to as the Federal Desktop Core Configuration (FDCC) mandate.

In addition, audits found that FEC had not yet fully implemented security control requirements that OMB established in 1997 as "best practices" security requirements for Windows computers. FEC advised us in past years that it planned to implement FDCC requirements, that the agency agreed to adopt, in a phased approach when new desktop/laptop computers are replaced[8]. While FEC has performed an evaluation of workstations for compliance with USGCB (United States Government Configuration Baseline), an evaluation of Internet Explorer configuration settings was not included in the evaluation. Key security settings are also provided for Internet Explorer in the FDCC/USGCB. Therefore, FEC is still not in full compliance with these OMB requirements, almost ten years after they were first issued.

Recommendations

20. Implement baseline configuration standards for all workstations and require documentation by the CIO to approve and accept the risk of any deviation.

    FEC Response
    OCIO officials advised that the FEC is currently working to implement USGCB standards. OCIO officials noted that the agency has purchased a software security application to monitor configuration changes in users' workstations. Any deviation will be documented and approved by CIO or his designated official.

    Auditor Comments
    Since OCIO officials have agreed to implement this recommendation, we have no additional comments.

21. Implement automated logging of all configuration changes and review logs regularly to ensure that all system changes, including changes to workstations, are processed through the change management framework.

[8] FEC has replaced its laptops, and the standards have still not been fully implemented.

FEC Response

OCIO officials advised that the agency has purchased a software security application, which provides OCIO the capability to automate logging of all configuration changes and review of logs. The full implementation of this application is estimated to be completed by the end of December 2013.

Auditor Comments

Since OCIO officials have agreed to implement this recommendation, we have no additional comments.

22. Fully implement USGCB/FDCC standards and perform scanning of Internet Explorer configuration settings.

FEC Response

OCIO officials advised that the agency plans to begin USGCB implementation agency-wide the second quarter of calendar year 2014. OCIO officials noted that the project completion date is dependent upon the successful implementation of the various phases of the project. A project plan is being developed, and the plan will include evaluating Internet Explorer settings.

Auditor Comments

Since OCIO officials have agreed to implement this recommendation, we have no additional comments.

e. Assessment and Accreditation of the FEC's General Support System Still Not Completed

FEC needs to perform an assessment of its general support system to identify vulnerabilities that could allow further network intrusions and data breaches. In addition, FEC has not followed FEC policy 58-2.4, Certification and Accreditation Policy, which establishes controls over the process of obtaining independent assurance that FEC major applications and general support system (GSS) are capable of enforcing the security policies that govern their operations. FEC 58-2.4 states that "This policy is designed to help increase FEC managers', users', and external consumers' confidence and trust that information technology systems will behave in a reliable, predictable manner, and with security controls commensurate with information sensitivity and risk levels. This policy is enabled by independent certifications carried out at regular intervals, and by management's deliberate acceptance of residual risk (accreditation)."

In our prior audit, we reported that FEC had not performed an assessment of its key medium risk GSS since December 2008; needed to strengthen FEC policy 58-2.4 to provide additional guidance on what decision points determine when a new accreditation is required, and provide more specific documentation requirements so the agency could track changes made in the GSS. These changes would enable

FEC officials to make informed decisions on whether security controls and operations need to be assessed and the system's accreditation to be updated.

During our 2013 audit, we followed up to determine whether the FEC had taken actions to assess and accredit its GSS. Similar to information we obtained during our 2012 audit, FEC officials advised that the agency is planning to perform a new assessment of the GSS, and subsequently accredit that the FEC has sufficient controls for the information and data in the GSS. We were advised that the review will be implemented in November 2013.

Recommendations

23. Perform within this fiscal year a new assessment and accreditation of the GSS using NIST SP 800-53 as the review criteria.

    FEC Response
    OCIO officials advised that they concur with this recommendation. OCIO officials noted that the agency will have a Risk Vulnerability Assessment performed by the Department of Homeland Security (DHS) in November 2013. In addition, OCIO officials stated that the agency has signed a Memorandum of Agreement with DHS to obtain the necessary hardware and software to implement continuous monitoring for the FEC's LAN.

    Auditor Comments
    Since OCIO officials have agreed to implement this recommendation, we have no additional comments.

24. Strengthen FEC Policy 58-2.4 so that it provides additional guidance on what decision points determine when a new assessment and accreditation is required; and the specific documentation requirements that need to be maintained in order for the agency to track changes so it can make informed decisions on when major changes drive the need for a new assessment and/or updated accreditation.

    FEC Response
    OCIO officials advised that the agency will look at this policy and update it as necessary, and that the agency will implement continuous monitoring in FY 2014.

    Auditor Comments
    OCIO officials stated that they will review the cited policy and update as necessary. We believe that the cited FEC policy is outdated and needs to be revised to address the problem areas noted in this document.

f. Testing and Exercise FEC's COOP - Key Documentation Not Available

FEC still has not yet fully and effectively tested and exercised the Continuity of Operations Plan (COOP) – a critical element in development of a comprehensive

and effective plan. As discussed in Federal Continuity Directive (FCD) No. 1, until the COOP plan is tested and exercised, any deficiencies in the plan cannot be determined, and the agency remains at risk of not being able to carry out the mission of the agency in the event of a disruption to normal business operations.

During fiscal years 2011 through 2013, we reviewed documents provided by FEC officials, and determined that FEC did not meet either its own testing requirements or the federal requirements that are applicable to the agency. In fiscal year 2013, we requested documentation from FEC officials that would enable us to follow-up on findings and recommendations in our prior audit report. We reviewed documents provided by FEC officials, and found that the documents were the same as we had reviewed in 2012. The table below lists key federal requirements, and whether the test documentation provided was in substantial compliance with these requirements.

Federal Continuity Directive No. 1, Appendix K	**Auditor Comments**
Annual testing of alert, notification, and activation procedures for continuity personnel and quarterly testing of such procedures for continuity personnel at agency headquarters.	This requirement was not met.
Annual testing of plans for recovering vital records (both classified and unclassified), critical information systems, services, and data.	Documentation was provided to show that critical information systems were tested.
Annual testing of primary and backup infrastructure systems and services (e.g., power, water, fuel) at alternate facilities.	This requirement was not met.
Annual testing and exercising of required physical security capabilities at alternate facilities.	This requirement was not met.
Testing and validating equipment to ensure the internal and external interoperability and viability of communications systems, through monthly testing of the continuity communications capabilities outlined in Annex H (e.g., secure and non-secure voice and data communications).	This requirement was not met.
An annual opportunity for continuity personnel to demonstrate their familiarity with continuity plans and procedures and to demonstrate the agency's capability to continue its essential functions.	This requirement was not met.
An annual exercise that incorporates the deliberate and preplanned movement of continuity personnel to an alternate facility or location.	This requirement was not met.
An opportunity to demonstrate that backup data and records required supporting essential functions at alternate facilities or locations are sufficient, complete, and current.	Some documents were provided that showed some portions of this requirement were tested.

The OIG issued an Inspection Report, *Inspection of the Federal Election Commission's Disaster Recovery Plan and Continuity of Operations Plans*, dated

January 2013, which addressed FEC's COOP, and noted problems similar to what we reported in our 2012 audit report. The inspection report stated:

> "…the FEC Continuity of Operations Plans (COOP) for Information Technology Division (ITD) does not include a COOP exercise schedule or plan. In addition, FEC's exercise plan should be in compliance with federal government requirements such as FCD 1, rather than FEC's internal policies that are not fully aligned with federal government standards. FEC has not developed an exercise plan that is a simulation of an emergency designed to validate the viability of one or more aspects of the COOPs… In addition, FEC has not developed and maintained a viable contingency planning program for their information systems to include exercising the plan. FEC will not be able to identify planning gaps that may only be discovered during an exercise. Key personnel have not validated their operational readiness for emergencies by performing their duties in a simulated operational environment…."

FDC No.1, Appendix K, Test, Training and Exercise, require that COOP documents must be validated through tests, training, and exercises (TT&E), and that all agencies must plan, conduct, and document periodic TT&Es to prepare for all-hazards, continuity emergencies and disasters, identify deficiencies, and demonstrate the viability of their continuity plans and programs. Deficiencies, actions to correct them, and a timeline for remedy must be documented in an organization's CAP (corrective action plan). FEC Policy No. 58.2.9, *Continuity of Operations and Disaster Recovery Policy*, provides that plans should not be considered valid until tested for practicality, executability, errors and/or omissions. The initial validation test should consist of a simulation or tactical test. Once validated, plans should be tested annually, or when substantive changes occur to the system, to the system environment, or to the plan itself. Test results should be maintained in a journal format and retained for analysis. Validated change recommendations resulting from testing activities should be incorporated into plans immediately.

Recommendations

25. Ensure that sufficient resources are assigned to the task of testing the COOP, a critical IT control process, in order to reduce risk to the FEC, and complete all required tests in a timely manner. Ensure that appropriate documentation is retained as required by FCD No. 1 to support that FEC has met all applicable federal TT&E requirements.

FEC Response

OCIO officials advised that they agree with this recommendation, and will assign staff to ensure the COOP is tested in a timely manner.

Auditor Comments

Since OCIO officials have agreed to implement this recommendation, we have no additional comments.

26. Develop a detailed POA&M to ensure that required COOP testing and exercises are completed as soon as possible.

    FEC Response
    OCIO advised that they agree with this recommendation, and that a plan of action and milestone document will be developed to ensure COOP testing and exercises are completed as soon as possible.

    Auditor Comments
    Since OCIO officials have agreed to implement this recommendation, we have no additional comments.

We noted another control issue that did not rise to the level of a reportable condition in a separate letter dated December 12, 2013 for management's consideration.

A summary of the status of prior year recommendations is included as Attachment 1.

REPORT ON COMPLIANCE

As part of obtaining reasonable assurance about whether the agency's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, and significant provisions of contracts, noncompliance with which could have a direct and material effect on the determination of financial statement amounts, and certain other laws and regulations. We limited our tests of compliance to these provisions and we did not test compliance with all laws and regulations applicable to the FEC. Providing an opinion on compliance with certain provisions of laws, regulations, and significant contract provisions was not an objective of our audit and, accordingly, we do not express such an opinion.

In connection with our audit, we noted one instance described below of noncompliance that is required to be reported according to *Government Auditing Standards* and the OMB audit bulletin guidelines. No other matters came to our attention that caused us to believe that FEC failed to comply with applicable laws, regulations, or significant provisions of laws, regulations, and contracts that have a material effect on the financial statements insofar as they relate to accounting matters. Our audit was not directed primarily toward obtaining knowledge of such noncompliance. Accordingly, had we performed additional procedures, other matters may have come to our attention regarding the FEC's noncompliance with applicable laws, regulations, or significant provisions of laws, regulations, and contracts insofar as they relate to accounting matters.

Noncompliance with Comprehensive National Cyber Security Initiative

We determined that the FEC is noncompliant with The Homeland Security Presidential Directive 23, and National Security Presidential Directive 54, *Cyber Security and Monitoring*. These establish the Comprehensive National Cyber Security Initiative, and

relate to Initiative No. 1, *Manage the Federal Enterprise Network as a Single Enterprise with a Trusted Internet Connection (TIC).*

TIC was introduced in OMB Memorandum M-08-05, *Implementation of Trusted Internet Connections*, dated November 20, 2007. The initiative was described in the memorandum as an effort to develop "a common [network] solution for the federal government" that would reduce the number of external Internet connections for the entire government to 50. The memorandum stated that "each agency will be required to develop a comprehensive POA&M (Plan of Action and Milestones)" to implement TIC, but it neither defined "agency" nor referred to any legal authority supporting the initiative. FEC's Office of General Counsel (OGC) analyzed this document and determined that since the FEC is exempt from the Federal Information Security Management Act (FISMA), and its predecessor statute, the Government Information Security Reform Act, and because the TIC requirement to implement POA&Ms appeared to be an expansion of a FISMA related information security requirement, FEC was exempt from implementing TIC.

In a June 2009 memorandum to the Staff Director, OGC provided that on January 8, 2008, former President Bush signed HSPD-23 which authorizes the Department of Homeland Security (DHS) to deploy Einstein 2, an automated intrusion detection system (IDS), across federal networks. Einstein 2 would allow the DHS National Cyber Security Division of the U.S. Computer Emergency Readiness Team (US-CERT) to consolidate Federal system intrusion detection, incident analysis and cyber response capabilities. The directive also provided that logon banners be set in place for both internal and external access to Federal Government information systems. HSPD-23 is classified; therefore the specific authorizing statute for the directive and the extent of its application to the Federal Election Commission is unknown. The OGC stated that "We confirmed with DHS on November 12, 2008 that in DHS's view the Commission is within the scope of the presidential directive. However, unclassified legal briefing materials provided by the Department of Justice indicate that at least part of the directive may be authorized by FISMA, from which the FEC is exempt. Thus, there is a possibility that HSPD-23 is only partially applicable to the FEC, or is not applicable at all to the FEC. Since the directive itself is classified, and limited unclassified information has been released, we do not have sufficient information at this time to confirm HSPD-23's applicability to the FEC."

In FY 2012, we provided additional documentation to FEC's OGC that indicated that TIC was applicable to FEC, and we requested that OGC reassess its determination on this matter. In an August 2012 memorandum to the Staff Director, the OGC stated that "…we conclude that FEC must comply with all requirements of…TIC." Based upon this OGC opinion, FEC officials agreed, in their response to our 2012 financial statement audit report, to implement TIC. However, our 2013 audit tests found that no actions have been taken by FEC to implement this Presidential Directive over five years after the directive mandated this security requirement. Had FEC performed necessary due diligence on this control as far back as 2007, it would have improved IT security controls that may have prevented or alerted responsible officials of a network intrusion.

Recommendation

27. Develop a time-phased corrective action plan to address the prompt implementation of the TIC by FEC.

FEC Response

OCIO officials advised the agency will continue to work with a TIC provider to create a solution for TIC implementation. The OCIO will create a plan to implement TIC as soon as they are able to find a cost effective solution.

Auditor Comments

We continue to believe that the FEC should implement this long-standing presidential and DHS directive.

Restricted Use Relating to Reports on Internal Control and Compliance

The purpose of the communication included in the sections identified as "Report on Internal Control" and "Report on Compliance" is solely to describe the scope of our testing of internal control over financial reporting and compliance, and to describe any material weaknesses, significant deficiencies, or instances of noncompliance we noted as a result of that testing. Our objective was not to provide an opinion on the design or effectiveness of the FEC's internal control over financial reporting or its compliance with laws, regulations, or provisions of contracts. The two sections of the report referred to above are integral parts of an audit performed in accordance with *Government Auditing Standards* in considering the FEC's internal control over financial reporting and compliance. Accordingly, those sections of the report are not suitable for any other purpose.

AGENCY COMMENTS

The Acting Chief Financial Officer (ACFO) responded to the draft report in a memorandum dated December 10, 2013, which indicated that the agency responses to each recommendation had been previously provided. We have included a synopsis of FEC's response, and our comments after each recommendation. The ACFO also noted in the memorandum that the agency has taken significant steps during FY 2013 to develop and implement a plan to improve the agency's IT security posture. Specifically, the CIO has signed a Memorandum of Agreement (MOA) with DHS to perform a comprehensive Risk Vulnerability Assessment, and another MOA to participate in DHS's Continuous Diagnostics and Mitigation (CDM) program beginning in January 2014. The ACFO believes "The new service will allow the agency to better identify and defend against cyber threats."

AUDITOR EVALUATION

We continue to believe that the FEC's information and information systems are at high risk because of the decision made by FEC officials not to adopt all applicable minimum IT security requirements that the Federal government has established. In addition, FEC

has not timely implemented actions necessary to remediate identified weaknesses in IT controls, some of which we first reported in FY 2009.

The FEC's December 10, 2013, written response to the audit is included in its entirety as Attachment 2. The FEC's written response was not subjected to the auditing procedures applied in the audit of the financial statements and accordingly, we express no opinion on it.

Leon Snead & Company, P.C.
Rockville, Maryland
December 12, 2013

Status of Prior Year Recommendations

Rec. No.	Audit Recommendations	Status as of September 30, 2013
1.	Formally adopt as a model for FEC, the NIST IT security controls established in FIPS 200 and SP 800-53, as the Government Accountability Office has done.	Recommendation open.
2.	Revise FEC policies to require that FEC contractors adhere to the FAR FISMA related requirements, and mandate that FEC contractors follow FISMA IT controls when providing services to the federal government. Use NIST SP 800-53 as guidance for establishing IT controls that contractors must follow.	Recommendation open.
3.	Develop a time-phased corrective action plan to address the prompt implementation of the TIC by FEC. Ensure that TIC is implemented as soon as possible, but no later than June 2013.	Recommendation open.
4.	Revise FEC policies and procedures to require a documented, fact-based risk assessment prior to deciding not to adopt a government-wide IT security best practice, or IT security requirement contained in the Federal Acquisition Regulations. Require the CIO to approve and accept the risk of any deviation from government-wide IT security best practices (i.e. NIST, FAR IT controls) that are applicable to the FEC business operations. Retain documentation of these decisions.	Recommendation open.
5.	Immediately implement government-wide requirements relating to strengthened password controls. Revise FEC policies and operating procedures to require the minimum best practices controls contained in FDCC and USGCB.	Recommendation open.
6.	Undertake a comprehensive review of user accounts that have been granted non-expiring passwords. Require certification from account owners detailing the need for non-expiring accounts, including the development of other alternatives, before reauthorizing the accounts' access. Develop FEC policies and operating procedures to implement this recommendation.	Recommendation open.
7.	Whenever possible, require accounts with non-expiring passwords to be changed at least annually. Establish substantially more robust password requirements for accounts granted non-expiring passwords. Develop FEC policies and operating procedures to implement this recommendation.	Recommendation open.
8.	Immediately terminate those accounts with non-expiring passwords that have not accessed their accounts within the last 12 months. Develop FEC policies and operating procedures to implement this recommendation.	Recommendation open.
9.	Remove the 400 disabled accounts noted during this audit by the end of the calendar year, and on a semi-annual basis conduct a review of the active directory to remove disabled accounts. Revise FEC policies and operating procedures to implement this recommendation.	Closed.
10.	Strengthen controls over the establishment of initial and replacement (default) passwords, to include requiring that random passwords be used, and the default passwords used be changed monthly. Develop FEC policies and operating procedures to implement this recommendation.	Recommendation open.
11.	Research and fix the problem that enables use of a default password to access other contractor email accounts.	Closed.

12.	Establish procedures that require contractors to create their own unique login passphrase.	Recommendation open.
13.	Require all employees and contractors with remote access to FEC's networks to comply with the dual-factor authentication requirement for their FEC laptop, as federal and FEC policies mandate.	Closed.
14.	Establish an FEC policy that requires annual recertification of users' access authorities.	Recommendation open.
15.	Review FEC current system capabilities in implementing recertification of user access authorities. Develop and document a detailed project plan based on management's review, and assign sufficient resources to this project so that it can be completed on or prior to June 2013.	Recommendation open.
16.	Revise FEC policies to: require a certification of its systems at least once every three years.	Closed.[9]
17.	Perform a re-certification of the GSS using NIST SP 800-53 as review criteria within this calendar year.	Recommendation open.
18.	Strengthen FEC Policy 58.2.8 so that it provides additional guidance on what decision points drive when a new C&A is required; and specific documentation requirements that need to be maintained in order for the agency to track changes so it can make informed decisions on when major changes drive the need for a re-certification.	Closed.[10]
19.	Include all components of the general support system, including workstations, into the organization's vulnerability/security scanning process and ensure that the general support system in its entirety is assessed at least annually.	Recommendation open.
20.	Implement procedures to ensure that scan results are subject to a "root cause" analysis to ensure that remediation actions address technical as well as organizational processes and procedures.	Recommendation open.
21.	Strengthen controls to ensure that vulnerabilities identified through the vulnerability scanning tests are remediated within 30 days, or document acceptance of these risks.	Recommendation open.
22.	Implement baseline configuration standards for all workstations.	Recommendation open.
23.	Fully implement USGCB/FDCC standards and perform scanning of Internet Explorer configuration settings.	Recommendation open.
24.	Implement logging of all configuration changes and review logs regularly to ensure that all system changes, including changes to workstations, are processed through the change management framework.	Recommendation open.
25.	Review the conditions that caused the employee to retain network access beyond the FEC's standard, and strengthen controls as appropriate.	Closed.
26.	Review the FSA database and remove those personnel shown as current employees or contractors who have departed the agency.	Closed.
27.	Review all outstanding audit recommendations contained in the agency's financial statement audit reports, and develop a current, detailed, time-phased corrective action plan (CAP) for each audit finding and recommendation.	Recommendation open.
28.	Modify key officials' annual performance plan[11] and rating elements to include, as a critical element, the timely completion of corrective action plans.	Recommendation open.

[9] NIST requirements have been modified in this area, and a continuous monitoring requirement has replaced the three year recertification requirement.
[10] See note 9.
[11] Recommendation modified to address OMB Circular A-50 language.

29.	Develop a tracking process that would include monthly reports to the CIO, highlight key tasks that may or have miss(ed) target dates, and assign one key OCIO official as responsible for monitoring OCIO corrective action plans.	Recommendation open.
30.	Ensure that sufficient resources are assigned to timely complete the testing of FEC's COOP in order to reduce risk to the FEC.	Recommendation open.
31.	Ensure that appropriate documentation is retained as required by FCD No. 1 to support that FEC has met all applicable federal testing requirements.	Recommendation open.
32.	Develop a detailed POA&M to ensure that required COOP testing and exercises are completed as soon as possible.	Recommendation open.
33.	Establish controls that would automatically suspend an individual's network access if security awareness training is not completed within required timeframes.	Recommendation open.

THE FEDERAL ELECTION COMMISSION
Washington, DC 20463

December 10, 2013

MEMORANDUM

TO: Leon Snead & Company, P.C.

FROM: Judy Berning
Acting Chief Financial Officer

SUBJECT: **Management Response to Audit Findings**

Please find attached the management response to the audit findings as provided in the draft document sent by the Office of Inspector General on December 4, 2013.

Please contact me at extension 1217 should there be additional questions.

cc: Lynne McFarland, Inspector General
Alec Palmer, Staff Director
Gregory Baker, Deputy General Counsel - Administration
Lisa Stevenson, Deputy General Counsel - Law

Attachment 2

Federal Election Commission

Fiscal Year 2013 Financial Statement Audit

Management Responses to Audit Findings

The Federal Election Commission (FEC) has made significant strides in addressing findings and recommendations that arise through the annual financial statement audit. In FY 2012, the FEC fully resolved the significant deficiency related to internal controls over financial reporting and did not have any material weaknesses or significant deficiencies in FY 2013 over financial reporting. The FEC continues to address Information Technology (IT) security control needs identified that relate to Information Technology policies, practices and procedures. The Federal Election Commission's responses to the FY 2013 audit findings were provided in the draft document sent by the Office of the Inspector General on December 4, 2013.

The agency maintains the highest level of commitment to its information technology security and systems. The FEC recognizes that it is important to have a controls framework that protects entity data and minimize security threats. The agency continues to evaluate ways to improve the FEC's controls framework to mitigate risk and improve overall operational effectiveness. The FEC has in place directives and a corrective action plan that is reviewed twice a year to mitigate potential risk factors. The agency's financial management systems are provided by the National Finance Center (NFC) and General Services Administration (GSA) under shared service agreements. The FEC receives and relies upon SSAE 16 audit reports to obtain assurance over financial applications provided by GSA and NFC.

The Office of the Chief Information Officer (OCIO) understands the agency's complex IT security needs and has taken significant steps during FY 2013 to develop and implement a plan to improve the agency's IT security posture. For example, the FEC recently acquired a security tool that will allow the agency's IT staff to continuously monitor client machines, such as laptops, for configuration changes and viruses that could negatively impact the FEC's system security. This tool will allow the FEC to address several of the audit's recommendations concerning workstation security scans and configuration security controls. Another tool acquired this year will allow the agency to ensure that FEC assets are regularly patched and that vulnerabilities that cannot be patched are documented.

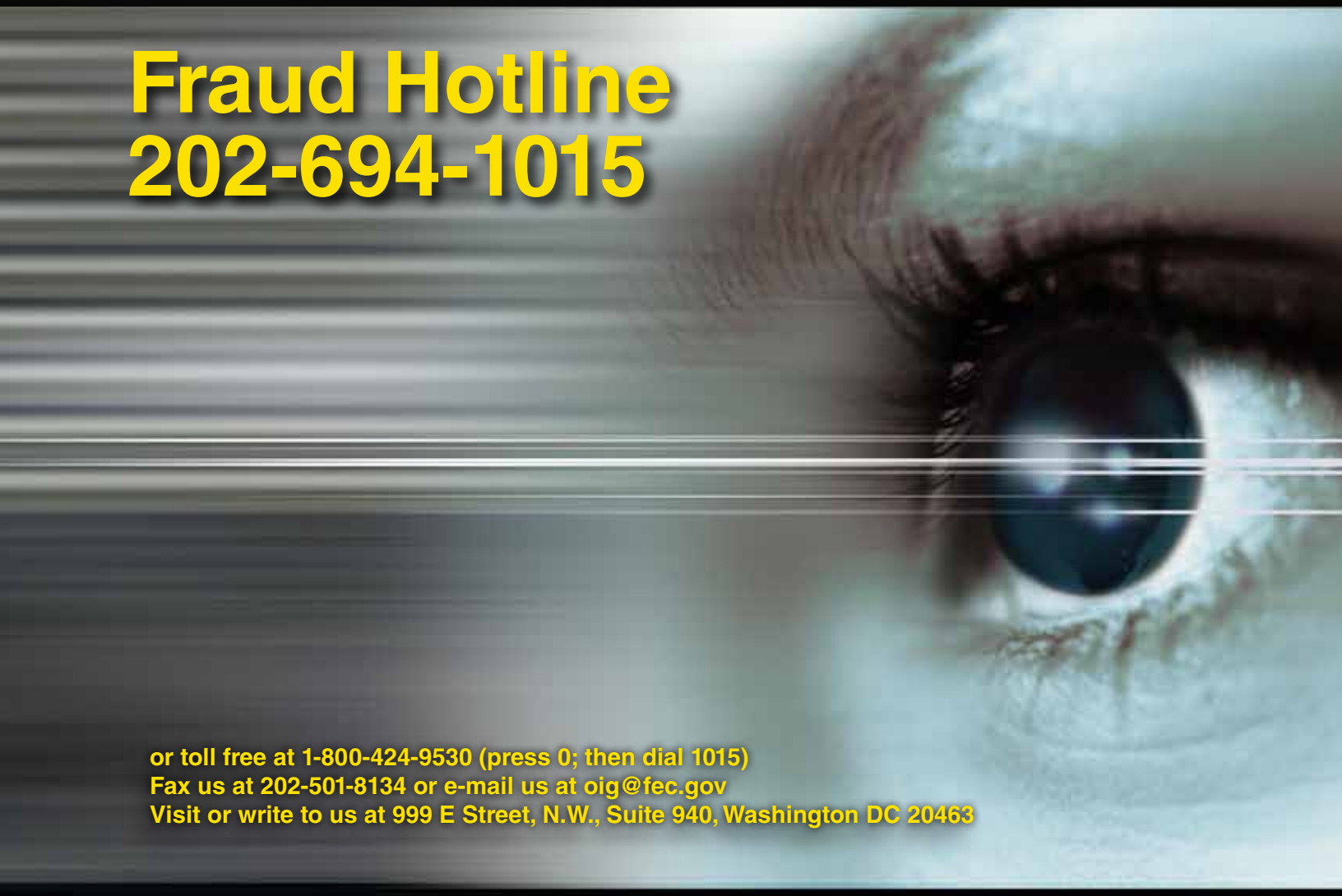
In addition, we are in collaboration with the Department of Homeland Security (DHS) to acquire new services that are now becoming available to the FEC. The new service will allow the agency to better identify and defend against cyber threats. The audit recommends that the FEC perform an assessment and accreditation of its major applications and general support systems (GSS) within this calendar year. In July of this year, the CIO signed a Memorandum of Agreement (MOA) with DHS to perform a comprehensive Risk Vulnerability Assessment, which is actively

going on. This assessment, which is being conducted at no cost to the FEC, will be completed in December 2013. As part of this assessment, DHS mapped the network to track data flow through the environment and scanned the FEC's database, operating system, network and wireless security. A web application scan was conducted to identify any undetected malware in system applications. DHS staff undertook penetration testing to see whether and how the agency's systems could be breached.

In July 2013, the CIO also signed an MOA with DHS to participate in DHS's Continuous Diagnostics and Mitigation (CDM) program, which provides capabilities and tools that enable network administrators to know the state of their networks at any given time, understand the relative risks and threats and help system personnel identify and mitigate flaws at near-network speed. The FEC will become eligible for participation in January 2014. This service will also be made available at no cost to the agency. Both of these programs will allow the FEC to improve cyber security and respond to the audit recommendations within the budget and staffing limitations of the agency.

Although the FEC is exempt from Federal Information Security Management Act (FISMA) compliance, the agency continues to adopt FISMA requirements for the FEC's IT security program where those requirements are feasible and appropriate for the agency. The FEC has already established numerous policies and procedures to govern and define the agency's IT security program, following the guidance published by the National Institute of Standards and Technology (NIST). The FEC has concurred with a number of the recommendations provided by the audit, and will continue to implement those recommendations where economically and technically feasible and where such actions fit within the management framework of the agency. While the FEC requests budget funds to comply with applicable IT control standards, the FEC will need Commission approval to adopt a requirement from which Congress has made the agency exempt. The OCIO has incorporated many industry "best practices" in establishing the FEC's IT security and monitoring program. Management's responses to each individual IT finding are contained within this report, with an explanation as to why the FEC may not agree with the finding.

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.