U.S. ELECTION ASSISTANCE COMMISSION
OFFICE OF INSPECTOR GENERAL

FINAL REPORT:

U.S. Election Assistance Commission

Compliance with the Requirements of the Federal Information Security Management Act

Fiscal Year 2014

No. I-PA-EAC-02-14
November 2014

U.S. ELECTION ASSISTANCE COMMISSION
OFFICE OF INSPECTOR GENERAL
1335 East West Highway - Suite 4300
Silver Spring, MD 20910

Memorandum

November 10, 2014

To: Alice Miller
Acting Executive Director

From: Curtis W. Crider
Inspector General

Curtis W. Crider

Subject: Final Report –U.S. Election Assistance Commission's Compliance with the Requirements of the Federal Information Security Management Act Fiscal Year 2014 (Assignment No. I-PA-EAC-02-14)

The Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA), an independent certified public accounting firm, to conduct an audit of the U.S. Election Assistance Commission's (EAC) compliance with the Federal Information Security Management Act and related information security policies, procedures, standards, and guidelines. The audit included assessing the EAC's effort to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the EAC. CLA found that EAC had a properly designed and effective information security program.

The audit was required to be conducted in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. CLA is responsible for the final audit report and the conclusions expressed in the report. The OIG performed the procedures necessary to obtain a reasonable assurance about CLA's independence, objectivity, qualifications, and technical approach.

The legislation creating the Office of Inspector General requires that we report to Congress semiannually on all audit reports issued, actions taken to implement our recommendations, and recommendations that have not been implemented. Therefore, we will include the information in the attached audit report in our next semiannual report to Congress.

If you have any questions regarding this report, please call me at (301) 734-3104.

CliftonLarsonAllen

Audit of the Election Assistance Commission Compliance with the Federal Information Security Management Act of 2002

Fiscal Year 2014

CliftonLarsonAllen

CliftonLarsonAllen LLP
www.claconnect.com

October 31, 2014

Mr. Curtis Crider
Inspector General
U.S. Election Assistance Commission
1335 East West Highway
Suite # 4300
Silver Spring, MD. 20910

Dear Mr. Crider:

CliftonLarsonAllen LLP (CLA) is pleased to submit its report on U.S. Election Assistance Commission's (EAC) compliance with the requirements of the Federal Information Security Management Act (FISMA) for fiscal year 2014.

The objective of this audit was to evaluate the effectiveness of EAC's information security program and practices, compliance with FISMA and related information security policies, procedures, standards, and guidelines. Our evaluation included tests for compliance with controls covered by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. Our audit was performed in accordance with *Government Auditing Standards*, issued by the Comptroller general of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We found that EAC had a properly designed and effective information security program. The audit fieldwork was performed at EAC's headquarters in Silver Spring, MD, from July 28, 2014 to October 2, 2014.

We very much appreciate the opportunity to serve you and will be pleased to discuss any questions you may have.

Very truly yours,

CliftonLarsonAllen LLP

GFF/sgd

TABLE OF CONTENTS

Executive Summary

The Federal Information Security Management Act of 2002 (FISMA) requires the Election Assistance Commission (EAC) to develop, document, and implement an information security program for the EAC network, which is used for email, voice over (Internet Protocol) IP, and access to EAC applications. Additionally, FISMA requires EAC to undergo an annual independent evaluation of its information security program and practices applicable to EAC and an assessment of compliance with the requirements of the Act. EAC has contracted with CliftonLarsonAllen LLP (CLA) to evaluate EAC's information security program and practices as required by FISMA.

The objective of this performance audit was to evaluate the effectiveness of the EAC information security program and practices, including EAC's compliance with FISMA and related information security policies, procedures, standards and guidelines. Our methodology for the FY 2014 FISMA evaluation included testing of EAC's network general support system for compliance with selected controls covered by National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*. Our audit was performed in accordance with *Government Auditing Standards,* issued by the Comptroller General of the United States.

Our audit covered the following control areas and security functions:

- Network and application servers and firewalls;
- Databases;
- Communication equipment (routers and switches);
- Physical and logical security controls;
- Security administration procedures and practices for assessing risk, providing training, granting personnel access, and maintaining and monitoring security controls;
- Shared security administration controls and procedures between the Commission and the General Services Administration; and
- Contractor that maintains the EAC website

These objectives included evaluating and reporting on whether a) security programs, plans, policies, and procedures in place were in compliance with applicable federal laws and regulations, b) controls provide reasonable assurance to adequately safeguard and protect EAC sensitive data and ensure that financial data are reliable and complete and provided timely, and c) controls were adequate to prevent or detect unauthorized activities, including external intrusion, theft, or misuse of EAC data, and destruction of EAC hardware, software and data.

We found that EAC generally had sound controls for its information security program.

Background

Federal Information Security Management Act

The Federal Information Security Management Act of 2002 (FISMA) was enacted into law as Title III of the E-Government Act of 2002, Public Law No. 107-347. Key requirements of FISMA include:

- The establishment of an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source;
- An annual independent evaluation of the agency's information security programs and practices; and
- An assessment of compliance with the requirements of the Act.

In addition, FISMA requires Federal agencies to implement the following:

- Periodic risk assessments;
- Information security policies, procedures, standards, and guidelines;
- Delegation of authority to the Chief Information Officer to ensure compliance with policy;
- Security awareness training programs;
- Periodic (annual and more frequent) testing and evaluation of the effectiveness of security policies, procedures, and practices;
- Processes to manage remedial actions for addressing deficiencies;
- Procedures for detecting, reporting, and responding to security incidents;
- Plans to ensure continuity of operations; and
- Annual reporting on the adequacy and effectiveness of the information security program.

The Office of Management and Budget (OMB) has issued executive branch policy for implementing FISMA: Circular No. A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources* (OMB Circular A-130, Appendix III), dated November 28, 2000. This circular establishes a minimum set of controls to be included in Federal agency automated information security programs. In particular Appendix III of OMB Circular A-130 defines adequate security as security commensurate with the risk and magnitude of the harm resulting from loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls.

Additionally, OMB has issued guidance related to information security with regard to plans of action and milestones (POA&Ms) for addressing findings from security control assessments, security impact analyses, and continuous monitoring activities. Per OMB Memoranda M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, POA&Ms provide a roadmap for continuous agency security improvement and assisting agency officials with prioritizing corrective action and resource allocation.

Further, OMB is responsible for reporting to Congress a summary of the results of Federal agencies' compliance with FISMA requirements.

NIST Security Standards and Guidelines

FISMA requires the National Institute of Standards and Technology (NIST) to provide standards and guidelines pertaining to federal information systems. Standards prescribed are to include information security standards that provide minimum information security requirements and are otherwise necessary to improve the security of federal information and information systems. FISMA also requires that federal agencies comply with Federal Information Processing Standards (FIPS) issued by NIST. In addition, NIST develops and issues Special Publications (SPs) as recommendations and guidance documents.

FIPS Publication (PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems* (FIPS PUB 200), mandates the use of NIST Special Publication (SP) 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations* (NIST SP 800-53). The purpose of NIST SP 800-53 is to provide guidelines for selecting and specifying security controls for information systems supporting an agency to meet the requirements of FIPS PUB 200. The security controls described in NIST SP 800-53 are organized into 18 families. Each security control family includes security controls associated with the security functionality of the family. In addition, there are three general classes of security controls: management, operational, and technical.

The NIST SP 800-53 security control families are as follows:

Table 1: Security Control Families

Control Class	Security Control Family
Management Controls	Risk Assessment
	Planning
	System and Services Acquisition
	Security Assessment and Authorization
Operational Controls	Personnel Security
	Physical and Environmental Protection
	Contingency Planning
	Configuration Management
	Maintenance
	System and Information Integrity
	Media Protection
	Incident Response
	Awareness and Training
Technical Controls	Identification and Authentication
	Access Control
	Audit and Accountability
	System and Communications Protection

CLA determined whether EAC complied with the following key standards and guidelines:

- FIPS Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST Special Publication (SP) 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*
- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*
- NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*
- NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*
- NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*
- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*
- NIST SP 800-60 Vol. 1 Rev.1, Volume 1: *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-92, *Guide to Computer Security Log Management*
- OMB, Circular No. A-130, *Management of Federal Information Resources*, Appendix III, Security of Federal Automated Information Resources

SCOPE AND METHODOLOGY

Scope

We conducted this audit in accordance with Government Auditing Standards, issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. The audit was designed to determine whether EAC implemented selected minimum security controls for selected information systems to reduce the risk of data tampering, unauthorized access to and disclosure of sensitive information, and disruptions to EAC's operations.

The audit included the testing of selected management, technical, and operational controls outlined in National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4.* We assessed EAC's performance and compliance with FISMA in the following areas:

- Access Controls
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Personnel Security
- Program Management
- Risk Assessment
- Security Assessment and Authorization
- System and Information Integrity
- System and Services Acquisition

For this audit, we reviewed the EAC network general support system. See Appendix V for a listing of selected controls. In addition, the audit included a follow up on prior year audit recommendations[1] to determine if EAC had made progress in implementing any recommended improvements.

Methodology

To determine if EAC's information security program met FISMA requirements, we conducted interviews with EAC officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. We also reviewed documents supporting the information security program. These documents included, but were not limited to, EAC's (1) information security policies and procedures; (2) incident response policies and procedures; (3) access control procedures; (4) identification and authentication policies and procedures; and (5) change control documentation. Where appropriate, we compared documents, such as the IT policies and procedures, to requirements stipulated in NIST special publications. In addition, we performed tests of system

[1] *Audit of the Election Assistance Commission's Fiscal Year 2013 Compliance with the Federal Information Security Management Act of 2002* (Audit Report No. A-OPC-13-006-P), September 26, 2013.

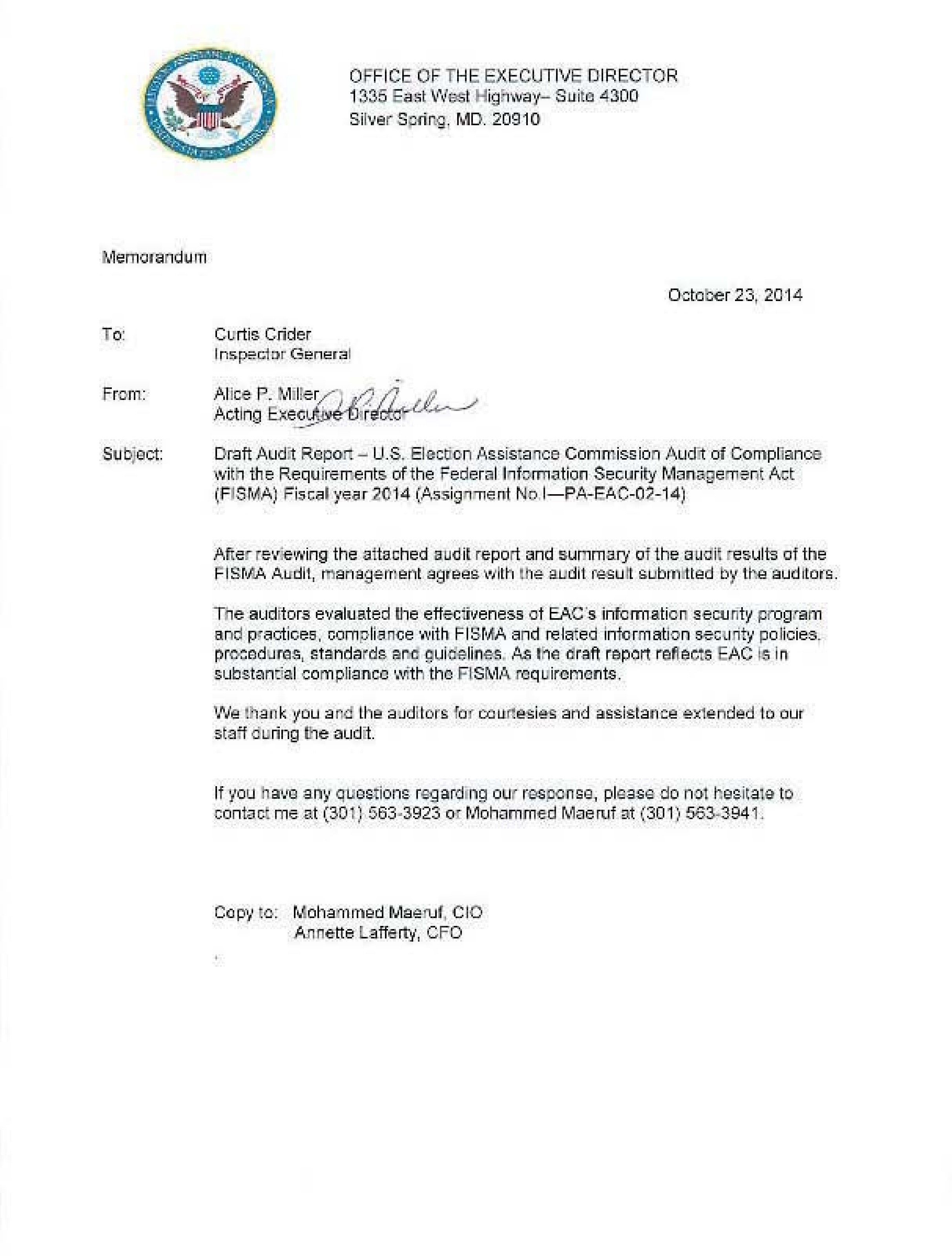
processes to determine the adequacy and effectiveness of those controls. We also reviewed the status of the audit recommendations in the fiscal year 2013 FISMA audit report.[2]

In testing for the adequacy and effectiveness of the security controls, we exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered relative risk, and the significance or criticality of the specific items in achieving the related control objectives. In addition, we considered the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review. In some cases, this resulted in selecting the entire population. However, in cases that we did not select the entire audit population, the results cannot be projected and if projected may be misleading.

[2] *Evaluation of the U.S. Election Assistance Commission's Fiscal Year 2013 Compliance with the Requirements of the Federal Information Security Management Act* (Audit Report No. I-PA-EAC-02-13), September 19, 2013.

Appendix II

MANAGEMENT COMMENTS



OFFICE OF THE EXECUTIVE DIRECTOR
1335 East West Highway– Suite 4300
Silver Spring, MD. 20910

Memorandum

October 23, 2014

To: Curtis Crider
Inspector General

From: Alice P. Miller
Acting Executive Director

Subject: Draft Audit Report – U.S. Election Assistance Commission Audit of Compliance with the Requirements of the Federal Information Security Management Act (FISMA) Fiscal year 2014 (Assignment No.I—PA-EAC-02-14)

After reviewing the attached audit report and summary of the audit results of the FISMA Audit, management agrees with the audit result submitted by the auditors.

The auditors evaluated the effectiveness of EAC's information security program and practices, compliance with FISMA and related information security policies, procedures, standards and guidelines. As the draft report reflects EAC is in substantial compliance with the FISMA requirements.

We thank you and the auditors for courtesies and assistance extended to our staff during the audit.

If you have any questions regarding our response, please do not hesitate to contact me at (301) 563-3923 or Mohammed Maeruf at (301) 563-3941.

Copy to: Mohammed Maeruf, CIO
Annette Lafferty, CFO

EVALUATION OF MANAGEMENT COMMENTS

EAC management indicated concurrence with the FISMA report.

STATUS OF PRIOR YEAR FINDINGS

The following table provides the status of the FY 2013 FISMA audit recommendations.[3]

No.	FY 2013 Audit Recommendation	EAC Status	Auditor's Position on Status
1	None	N/A	N/A

[3] *Audit of the Election Assistance Commission's Fiscal Year 2013 Compliance with the Federal Information Security Management Act of 2002* (Audit Report No. A-OPC-13-006-P), September 26, 2013.

SUMMARY OF RESULTS OF EACH CONTROL REVIEWED

Control	Control Name	Is Control Effective
EAC Network		
AC-1	Access Control Policy & Procedures	Effective
AC-2	Account Management	Effective
AC-3	Access Enforcement	Effective
AC-5	Separation of Duties	Effective
AC-6	Least Privilege	Effective
AC-11	Session Lock	Effective
AC-17	Remote Access	Effective
AC-19	Access Control for Mobile Devices	Effective
AT-1	Security Awareness & Training Policy and Procedures	Effective
AT-2	Security Awareness	Effective
AT-3	Security Training	Effective
AT-4	Security Training Records	Effective
AU-6	Audit Review, Analysis, and Reporting	Effective
CA-1	Security Assessment and Authorization Policy & Procedures	Effective
CA-2	Security Assessments	Effective
CA-3	Information System Connections	Effective
CA-5	Plan of Action and Milestones	Effective
CA-6	Security Authorization	Effective
CA-7	Continuous Monitoring	Effective
CM-1	Configuration Management Policy and Procedures	Effective
CM-2	Baseline Configuration	Effective
CM-3	Configuration Change Control	Effective
CM-6	Configuration Settings	Effective
CM-7	Least Functionality	Effective
CM-8	Information System Component Inventory	Effective
CP-1	Contingency Planning Policy & Procedures	Effective
CP-2	Contingency Plan	Effective
CP-4	Contingency Plan Testing and Exercises	Effective
CP-6	Alternate Storage Sites	Effective
CP-7	Alternate Processing Sites	Effective
CP-9	Information System Backup	Effective
CP-10	Information System Recovery & Reconstitution	Effective
IA-1	Identification and Authentication Policy and Procedures	Effective
IA-2	Identification and Authentication (Organizational Users)	Effective
IA-3	Device Identification and Authentication	Effective
IA-4	Identifier Management	Effective
IA-5	Authenticator Management	Effective
IR-1	Incident Response Policy and Procedures	Effective
IR-4	Incident Handling	Effective
IR-5	Incident Monitoring	Effective
IR-6	Incident Reporting	Effective
IR-8	Incident Response Plan	Effective
PS-6	Access Agreements	Effective

Control	Control Name	Is Control Effective
RA-1	Risk Assessment Policy and Procedures	Effective
RA-2	Security Categorization	Effective
RA-3	Risk Assessment	Effective
SA-1	System and Services Acquisition Policy and Procedures	Effective
SA-5	Information System Documentation	Effective
SA-9	External Information Systems	Effective
SC-7	Boundary Protection	Effective
SC-8	Transmission Integrity	Effective
SI-2	Flaw Remediation	Effective
PL-4	Rules of Behavior	Effective
PM-1	Information Security Program Plan	Effective
PM-3	Information Security Resources	Effective
PM-4	Plan of Action and Milestones Process	Effective
PM-5	Information System Inventory	Effective
PM-6	Information Security Measures of Performance	Effective
PM-9	Risk Management Strategy	Effective
PM-10	Security Authorization Process	Effective

OIG's Mission

Help to ensure efficient, effective, and transparent EAC operations and programs

Obtaining Copies of OIG Reports

Copies of OIG reports are available on the OIG website, www.eac.gov/inspector_general/

Copies of OIG reports can be requested by e-mail: (eacoig@eac.gov).

Mail orders should be sent to:
U.S. Election Assistance Commission
Office of Inspector General
1335 East West Highway - Suite 4300
Silver Spring, MD 20910

To order by phone: Voice: (301) 734-3104
Fax: (301) 734-3115

To Report Fraud, Waste and Abuse Involving the U.S. Election Assistance Commission or Help America Vote Act Funds

By Mail: U.S. Election Assistance Commission
Office of Inspector General
1335 East West Highway - Suite 4300
Silver Spring, MD 20910

E-mail: eacoig@eac.gov

OIG Hotline: 866-552-0004 (toll free)

On-Line Complaint Form: www.eac.gov/inspector_general/

FAX: (301)-734-3115