CliftonLarsonAllen LLP
www.cliftonlarsonallen.com

Evaluation of Equal Employment Opportunity Commission's (EEOC) Compliance with Provisions of the Federal Information Security Management Act of 2002

Fiscal Year 2012

Final Report

TABLE OF CONTENTS

Executive Summary

The EEOC Office of Inspector General (OIG) contracted with CliftonLarsonAllen LLP (CLA) to conduct an audit of EEOC' compliance with the provisions of the Federal Information Security Management Act of 2002 for Fiscal Year (FY) 2012. The Federal Information Security Management Act of 2002 (FISMA) requires agencies to develop, document, and implement 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.

The audit meets the FISMA requirement for an annual evaluation of EEOC' information security program. The overall objective of this audit was to determine if EEOC' information security program met the requirements of the Federal Information Security Management Act of 2002. Specifically, we performed audit work associated with the FISMA Office of Management and Budget (OMB) annual reporting requirements for OIGs and completed a review of six EEOC information systems: The EEOC Network, EEO-1 Survey System, Document Management System (DMS), Integrated Mission System (IMS), Financial Cloud Solutions (FCS), and Federal Personnel and Payroll System (FPPS). In addition, four Notice of Finding and Recommendations (NFRs) were submitted to EEOC management to include findings from both the system reviews and component level review.

The audit concluded that EEOC met most, but not all, of the key requirements of FISMA. The Agency has made positive strides over the last year in addressing information security weaknesses and continues to make progress in becoming fully compliant with FISMA. However, EEOC still faces challenges to refine its information security program. These challenges involve:

- Maintaining documentation for network access requests/approvals. (See page 6)
- Implementing multi-factor authentication. (See page 7)
- Maintaining documentation of acceptance and understanding of information security responsibilities. (See page 8)
- Revising the incident response policy to reflect all US-CERT categorization types (See page 9)

Consequently, EEOC' operations and assets may be at risk of misuse and disruption. The report contains four recommendations to help EEOC improve its information security program and practices.

This report is intended solely for the information and use of the management of EEOC and OIG and is not intended to be and should not be used by anyone other than these specified parties.

Background

Organization

The U.S. Equal Employment Opportunity Commission (EEOC) is responsible for enforcing federal laws that make it illegal to discriminate against a job applicant or an employee because of the person's race, color, religion, sex (including pregnancy), national origin, age (40 or older), disability or genetic information. It is also illegal to discriminate against a person because the person complained about discrimination, filed a charge of discrimination, or participated in an

employment discrimination investigation or lawsuit. The EEOC has the authority to investigate charges of discrimination against employers who are covered by the law.

The EEOC is composed of five Commissioners and a General Counsel appointed by the President and confirmed by the Senate. Commissioners are appointed for five-year staggered terms; the General Counsel's term is four years. The President designates a Chair and a Vice Chair. The Chair is the Chief Executive Officer of the EEOC.

The EEOC has 53 field offices, and has its headquarters in Washington, D.C. Additional information about EEOC may be found at http://www.eeoc.gov.

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 (E-Gov) of 2002 (P.L. 107-347, December 17, 2002). Key requirements of FISMA include:

1. 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.
2. An annual independent evaluation of the agency's information security programs and practices; and
3. An assessment of compliance with the requirements of the Act.

FISMA requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management is integrated with the agency strategic and operation planning processes. All agencies must also report annually to the Office of Management and Budget (OMB) and Congressional committees on the effectiveness of their information security program. In addition, FISMA has established that the standards and guidelines issued by the National Institute of Standards and Technology (NIST) are mandatory for Federal agencies.

Audit Objective

A key requirement of the Federal Information Security Management Act of 2002 is an annual independent evaluation of the Agency's information security program. As a result, CLA was contracted by EEOC OIG to review the Agency's information security program and practices as set forth by the Federal Information Security Management Act of 2002 for FY 2012. The work performed under this engagement involved a review of the effectiveness of the Agency's Office of Information Technology (OIT) oversight of the Agency's information security program and evaluation of six EEOC information systems: The EEOC Network, EEO-1 Survey System, Document Management System, Integrated Mission System, Financial Cloud Solutions, and Federal Personnel and Payroll System.

In addition, we were required to complete the FY 2012 OMB FISMA Reporting Template included as an annual reporting requirement for OIGs.

Scope

CLA performed the audit in support of the EEOC OIG's FISMA reporting requirements. The period covered by this audit ended September 30, 2012. We conducted the audit in accordance with generally accepted government auditing standards. 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

The purpose of the audit was to determine if EEOC' information security program met the requirements of FISMA. In assessing, EEOC' adherence to FISMA, we conducted component level and system level testing to support FISMA compliance. In conducting our review of the Agency's Office of the CIO's oversight over EEOC' information security program and practices, the following areas were reviewed:

- Organizational responsibilities and authority
- Information security policies and procedures
- System security plans
- Risk Assessments
- Continuity of operations plan
- Security incident reporting
- Security Awareness, Training, and Education
- Certification and accreditation process
- Remedial action process (plan of action and milestones)
- System Configuration Management
- Annual information security program reporting

In regards to the system level testing, CLA in conjunction with the EEOC OIG selected the EEOC Network, EEO-1 Survey System, Document Management System, Integrated Mission System, Financial Cloud Solutions, and Federal Personnel and Payroll System to evaluate as part of the scope of work. The audit included the testing of selected management, technical, and operational controls of the information systems outlined in National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 3 *Recommended Security Controls for Federal Information Systems*. The following NIST Special Publication 800-53 Controls were reviewed for the EEOC Network, EEO-1 Survey System, Document Management System, Integrated Mission System, Financial Cloud Solutions, and Federal Personnel and Payroll System.

- Access Controls
- Audit and Accountability
- Certification, Accreditation and Security Assessments
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Maintenance
- Security Planning
- Risk Assessment
- System and Service Acquisition
- System and Communications Protection
- System and Information Integrity

In addition, we completed a follow-up review of prior year FISMA findings and recommendations to determine if EEOC had made progress on implementing the recommended improvements in its information security program.

Four NFRs were submitted to EEOC management to include findings from both the system reviews and component level review.

At the time of the audit, EEOC operated the following information systems:

EEOC Network (General Support System)

Major Applications

1. EEO-1 Survey System
2. Document Management System (DMS)
3. Integrated Mission System (IMS)
4. Financial Cloud Solutions (*owned by another Federal Agency*)

This report is intended solely for the information and use of the management of EEOC and the EEOC OIG and is not intended to be and should not be used by anyone other than these specified parties.

Testing Methodology

To determine if EEOC' information security program met the requirements of FISMA, we conducted interviews with EEOC staff members and reviewed legal and regulatory requirements stipulated by FISMA. We also reviewed documentation related to EEOC' information security program. These documents included, but were not limited to, EEOC' security policies and procedures, plan of action and milestones, system security plans, risk assessments, certification and accreditation documentation, contingency plans, and incident reporting procedures. In addition, we performed tests of system processes to determine the adequacy and effectiveness of those controls.

We also evaluated available data supporting EEOC annual FISMA report to OMB on its information system security program.

Findings and Recommendations

EEOC has achieved progress towards FISMA compliance over the last year. Specifically, EEOC has implemented the following FISMA requirements:

- The Agency has strengthened its vulnerability scanning and patch remediation program and procedures.
- Updated their business impact analysis (BIA) so it accurately maps to disaster recover testing results.
- Implemented a revalidation and review process to remove and disable unneeded virtual private network accounts.

Although, EEOC has made improvements in its information security program, the agency still faces challenges to refine its information security program. These challenges involve:

- Maintaining documentation for network access requests/approvals. (See page 6)
- Implementing multi-factor authentication (See page 7)

- Maintaining documentation of acceptance and understanding of information security responsibilities (See page 8)
- Maintaining the incident response policy to reflect all US-CERT categorization types (See page 9)

These findings are further discussed below.

Access Control/Identification and Authentication

1. Network access request forms were not adequately maintained. (NFR Reference # 2012 – 1)

Access request forms which document request and approval for network access were not provided for two out of twenty-five individuals sampled.

In addition, Integrated Mission System (IMS) access request forms were not provided for six of ten individuals sampled.

Without an appropriate access request form, excessive access to agency information may be provided and sensitive information could be compromised.

National Institute of Standards and Technology Special Publication (NIST SP) 800-53 Revision 3, Recommended Security Controls for Federal Information Systems control *AC-2, states the following regarding account management*, "The organization manages information system accounts, including: Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); Establishing conditions for group membership; Identifying authorized users of the information system and specifying access privileges; Requiring appropriate approvals for requests to establish accounts; Establishing, activating, modifying, disabling, and removing accounts; Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to know/ need-to-share changes; Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users; Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and Reviewing accounts.

Recommendation:
Recommendation No.1: We recommend that EEOC implement a centralized repository to maintain control of access request forms.

Management Response:
Management indicated concurrence with this finding.

Additionally stating "Network access forms – EEOC would like to note that we do have a centralized repository for maintaining network user access forms. We concur with the 92% compliance finding for retrieval of network access forms in FY 2012 and are encouraged that this area shows progress over the 77% compliance rate finding in FY 2011. OIT expects that this rate will remain at the >90% level until we can move away from manual processes and implement more automated on-boarding/account creation practices. In the interim, EEOC accepts the >90% rate as an acceptable level of compliance risk.

IMS – OIT will conduct a recertification of all IMS users in the first quarter of FY 2013 and will review and update policies related to preservation of account authorization forms. Remediation dates will be determined and included in the system POA&M."

Auditor's Evaluation of Management's Response:
Management agrees with the condition of the missing access request forms. CLA's recommendation on a centralized repository was based upon management's need to obtain and request access request forms for several individuals from various field offices since not available at headquarters. We agree that a more automated on-boarding/account creation practices would assist in mitigating the risk of lost forms under current manual processes.

Effective implementation of actions noted in management's response for IMS users should resolve the reported condition and recommendation.

2. EEOC did not fully implement multi-factor authentication (NFR Reference # 2012 - 3)

Through inquiry with management and review of the Data Net System Security Plan, EEOC has not fully implemented multi-factor authentication for remote access through Virtual Private Network (VPN), as well as for network and local accounts. Although an Acceptance of Risk was provided for new imaged laptops, legacy laptops use a common password as part of their two-factor authentication.

Without a fully implemented multi-factor authentication process, this increases the risk of unauthorized access attempts.

National Institute of Standards and Technology Special Publication (NIST SP) 800-53 Revision 3, Recommended Security Controls for Federal Information Systems control *IA-2, states the following regarding identification and authentication*, "The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). And applicable control enhancements: "(1) The information system uses multifactor authentication for network access to privileged accounts. (2) The information system uses multifactor authentication for network access to non-privileged accounts. (3) The information system uses multifactor authentication for local access to privileged accounts. (8) The information system uses [Assignment: organization-defined replay-resistant authentication mechanisms] for network access to privileged accounts."

Recommendation:
Recommendation No.2: We recommend that EEOC implement multifactor authentication for network access to non-privileged and privileged accounts.

Management Response:
Management indicated concurrence with this finding.

Additionally stating "EEOC continues to acknowledge that we have not implemented multifactor authentication for network access. This project is dependent on full (>80%) implementation of HSPD-12 PIV cards to all EEOC users as well as funding to deploy the logical access requirements. EEOC has a risk acceptance on file, signed by the CIO, for this vulnerability."

Auditor's Evaluation of Management's Response:
EEOC agrees that they have not implemented multifactor authentication for network access. Although the compensating controls described within the risk waiver rely upon data encryption and utilities to detect and mitigate malicious activity, versus an additional strengthening of existing user authentication controls to mitigate for the lack of multifactor authentication.

Effective implementation of actions noted in management's response should resolve the reported condition and recommendation.

Planning

3. Documented acceptance and understanding of information security responsibilities were not adequately maintained (NFR Reference # 2012- 2)

Documented acceptance and understanding of information security responsibilities were not available for 12 (48%) out of 25 individuals hired during FY 2012.

If acknowledgment of security responsibilities is not documented, users may be unaware of potential risks and their responsibilities in the use of EEOC information systems.

EEOC Order 240.005 states the following, "The Chief Human Capital officer is responsible for: Assuring that all new employees, as part of their orientation package, receive and sign an acknowledgment of receipt of "Information Security Responsibilities of EEOC System Users" (Appendix A)."

National Institute of Standards and Technology Special Publication (NIST SP) 800-53 Revision 3, Recommended Security Controls for Federal Information Systems control *PL-4, states the following regarding rules of behavior*, "The organization establishes and makes readily available to all information system users, a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information."

Recommendation:
Recommendation No.3: We recommend that EEOC management ensure that all network users have read and signed acknowledgment of receipt of Information Security Responsibilities of EEOC System Users and that forms are managed in a centralized location.

Management Response:
Management indicated concurrence with this finding.

Additionally stating "OIT would like to clarify that this finding specifically relates to interns/volunteers, not "New Hires" which implies a newly hired employee. EEOC "new hires" go through a formal on-boarding process in both Headquarters and the Field which includes the review and signature of the Information Security Responsibilities document (which is then stored with their personnel file). All 12 individuals who were identified as not

having evidence of acknowledgement were interns, volunteers, or temps – some of which may not go through the formal new-hire process.

To mitigate risk of users not remembering or not previously acknowledging the Security Responsibilities document, in July 2012, EEOC conducted an on-line review and acceptance of the "EEOC Network/Desktop Rules of Behavior" and the "Information Security Responsibilities of EEOC System Users" for all system users - with the user's acknowledgement stored in a centralized location. Therefore, all system users on-board during this timeframe acknowledged their responsibilities. In addition, in August 2012, we conducted the annual Security Awareness Training which is mandatory for all system users.

OIT acknowledges that these annual certification measures may miss some of the interns, volunteers, and temporary staff that are only on-board for a few weeks or months. Therefore, we will develop plans and procedures to better ensure that the Rules are acknowledged within a specified period of time of network account creation. Timelines related to this remediation will be documented in the system POA&M. "

Auditor's Evaluation of Management's Response:
Effective implementation of actions noted in management's response (last paragraph) should resolve the reported condition and recommendation.

Incident Response

4. The Incident Response Policy is incomplete. (NFR Reference # 2012 - 4)

EEOC's incident response policy (V1.4) only reflects 4 of 6 current incident categorization types, prescribed by the United States Computer Emergency Response Team (US-CERT).

Without the inclusion of all 6 severity ratings, EEOC increases the risk of not notifying proper officials about the incident in a timely manner so that action can be taken to avoid and minimize the compromised information system and data.

NIST SP800-61, Rev. 2 ***Incident Response to Computer Security Events*** **Section 2.3.1 "Policy Elements"** states:

Policy governing incident response is highly individualized to the organization. However, most policies include the same key elements:

- Statement of management commitment
- Purpose and objectives of the policy
- Scope of the policy (to whom and what it applies and under what circumstances)
- Definition of computer security incidents and related terms
- Organizational structure and definition of roles, responsibilities, and levels of authority; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, the requirements for reporting certain types of incidents, the requirements and guidelines for external communications and information sharing (e.g., what can be shared with whom, when, and over what channels), and the handoff and escalation points in the incident management process
- Prioritization or severity ratings of incidents

- Performance measures (as discussed in Section 3.4.2)
- Reporting and contact forms.

Recommendation:
Recommendation No. 4: We recommend that EEOC management revise the agency's policy to correctly reflect the entire severity rating list published by US-CERT.
Management Response:
Management indicated concurrence with this finding.

Additionally stating "OIT had purposefully documented four categories in our Incident Response Policy, as Category 6 is not applicable to reporting and Category 5 was incorporated into our Category 3. However, we have updated the policy and related log sheets to reflect the full six categories, based on the auditor's recommendation. These updated documents were provided to the auditor on 10/19/12."

Auditor's Evaluation of Management's Response:
Effective implementation of actions noted in management's response should resolve the reported condition and recommendation.

Appendix A: Status of Prior Year (FY2011) Findings

Item #	Finding	Description	Control Family	Current Year Status	Comments
1	EEOC has not fully implemented multifactor authentication for remote access.	Through inquiry with management and review of the Data Net System Security Plan, EEOC has not fully implemented multi-factor authentication for remote access through Virtual Private Network (VPN), as well as for network and local accounts. Although an Acceptance of Risk was provided for new imaged laptops, legacy laptops use a common password as part of their twofactor authentication.	Access Control	Open	Multifactor authentication for remote access is still not fully implemented. **NFR # 2012 – 03**
2	The agency-wide Business Impact Analysis (BIA) has not been updated.	Through inquiry with the EEOC Chief Security Officer, the EEOC agency-wide Business Impact Analysis (BIA) has not been updated since 2002 to reflect the current system environment and to address the weaknesses identified during subsequent disaster recovery tests.	Contingency Planning	Closed	The Business Impact Analysis (BIA) was updated.
3	Vulnerability scanning conrol weaknesses were identified.	Through inquiry with management and performance of an external network vulnerability assessment, we noted the following control weaknesses: 1. EEOC Management did not apply version releases promptly (1 critical and 5 high vulnerabilities were found) to critical network devices. 2. Credentialed network vulnerability scanning is not being performed.	Configuration Management	Closed	Version releases were applied promptly and credentialed network vulnerability scanning has occurred.

Item #	Finding	Description	Control Family	Current Year Status	Comments
4	Excessive Virtual Private network (VPN) accounts were discovered.	Through testing of active VPN accounts, CLA discovered 1 employee as separated but still remained on the enabled VPN list.	Account and Identity Management	Closed.	Through FY2012 testing of active VPN accounts, there were no active separated individuals.
5	Access request forms could not be provided for all employees sampled.	Access request forms which document request and approval for network access could not be provided for seven out of thirty employees sampled.	Identity and Access Management	Open	Access request forms which document request and approval for network access were not provided for two out of twenty-five individuals sampled. **(See NFR # 2012 – 01)**