Clifton Gunderson LLP
Certified Public Accountants & Consultants

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

Fiscal Year 2011

Final Report

11710 Beltsville Drive, Suite 300
Calverton, MD 20705-3106
tel: 301-931-2050
fax: 301-931-1710

www.cliftoncpa.com

Member of
HLB International

EEOC/Office of Inspector General
Assessment of EEOC's Compliance with Provisions of the Federal Information Security Management Act
Fiscal Year 2011

TABLE OF CONTENTS

EEOC/Office of Inspector General
Assessment of EEOC's Compliance with Provisions of the Federal Information Security Management Act
Fiscal Year 2011

Executive Summary

The EEOC Office of Inspector General (OIG) contracted with Clifton Gunderson LLP (CG) to conduct an audit of EEOC' compliance with the provisions of the Federal Information Security Management Act of 2002 for Fiscal Year (FY) 2011. (See page 3) 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. (See page 3)

The audit meets the FISMA requirement for an annual evaluation of EEOC' information security program. (See page 4) 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. (See page 4) 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, Integrated Mission System, Integrated Financial Management System, and Federal Personnel and Payroll System. In addition, five 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. (See page 6) These challenges involve:

- Maintaining documentation for network access requests/approvals. (See page 6)
- Implementing multi-factor authentication (See page 7)
- Updating the agency-wide Business Impact Analysis (BIA) (See page 8)
- Implementing controls over the agency's vulnerability assessment process (see page 9).
- Removing Virtual Private Network (VPN) access for separated employees timely. (See page 10)

Consequently, EEOC' operations and assets may be at risk of misuse and disruption. The report contains five 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, Clifton Gunderson (CG) was contracted by EEOC Office of Inspector General (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 2011. 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, Integrated Financial Management System, and Federal Personnel and Payroll System.

In addition, we were required to complete the FY 2011 OMB FISMA Reporting Template included as an annual reporting requirement for OIGs.

Scope

CG performed the audit in support of the EEOC OIG's FISMA reporting requirements. The period covered by this audit ended September 30, 2011. 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, CG in conjunction with the EEOC OIG selected the EEOC Network, EEO-1 Survey System, Document Management System, Integrated Mission System, Integrated Financial Management System, 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, Integrated Financial Management System, 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.

Five 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) (*owned by another Federal Agency*)
4. Integrated Financial Management System Federal Personnel and Payroll System (*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 established and is maintaining a certification and accreditation program including sufficiently detailed documented procedures.

- Developed policies which define auditable events and log retention requirements as part of EEOC's continuous monitoring program.

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 and approvals
- Implementing multi-factor authentication
- Updating the agency-wide Business Impact Analysis (BIA)
- Implementing controls over the agency's vulnerability assessment process
- Removing Virtual Private Network (VPN) access for separated employees timely.

These findings are further discussed below.

Access Control/Identification and Authentication

1. **Network access request forms were not adequately maintained. (NFR Reference # 2011 – 5)**

   Access request forms which document request and approval for network access could not be provided for seven out of thirty employees 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:
   EEOC concurs and will create a centralized repository to maintain control of access request forms.

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

2. EEOC did not fully implement multi-factor authentication (NFR Reference # 2011 - 1)

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. Additionally, through inquiry with management, we were informed that full implementation of multi-factor authentication has been delayed due to budget constraints.

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:
EEOC concurs that multi-factor authentication has not been fully implemented due to budget constraints. The EEOC Chief Information Officer has reviewed the in-place compensating controls and accepted the risk of delayed implementation of multi-factor authentication, pending full distribution (80%) of HSPD-12 PIV2 Federal ID cards to agency staff. This acceptance of risk applies to access via both the new laptops as well as the older "COOP" laptops.

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

Contingency Planning

3. A Agency-wide Business Impact Analysis (BIA) had not been updated since 2002. (NFR Reference # 2011 - 2)

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.

The lack of an up-to-date Business Impact Analysis creates a deficiency in the contingency planning process. A deficiency in this process means that key impacts or threats could be overlooked leading to the ineffective or delayed recovery of agency systems.

National Institute of Standards and Technology (NIST) Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* states: “The BIA is a key step in implementing the CP controls in NIST SP 800-53 and in the contingency planning process overall. The BIA enables the ISCP Coordinator to characterize the system components, supported mission/business processes, and interdependencies. The BIA purpose is to correlate the system with the critical mission/business processes and services provided, and based on that information, characterize the consequences of a disruption. The ISCP Coordinator can use the BIA results to determine contingency planning requirements and priorities. Results from the BIA should be appropriately incorporated into the analysis and strategy development efforts for the organization’s COOP, BCPs, and DRP.”

Recommendation:

Recommendation No. 3: We recommend that EEOC management reevaluate and update the agency Business Impact Analysis to ensure it accurately represents the current EEOC environment and addresses the deficiencies noted in the disaster recovery tests.

Management Response:

EEOC concurs that the BIA is out-of-date and had prior plans to update this document during the first quarter of 2012. EEOC notes, however, that primary information in the BIA has been maintained and updated in the EEOC IT Contingency Plan.

Auditor’s Evaluation of Management’s Response:

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

Configuration Management

4. Network vulnerability assessment control weaknesses. (NFR Reference # 2011 - 3)

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.

Not updating servers promptly could expose EEOC to known security vulnerabilities that expose the systems to potential unauthorized access, data loss, data manipulation, and system unavailability.

EEOC Office of Information Technology *Patch Management and System Maintenance Procedures, Version 1.3, dated June 2, 2009*, states: "Standard patching for Windows and Novell servers will be performed during regular monthly maintenance weekends (as required). Standard patching for the Oracle and Unix environments will occur quarterly, during the scheduled maintenance weekend. Patching/upgrade of the desktop environment will also occur quarterly (Feb, May, Aug, Nov), through network distribution. Patching of routers and switches will be conducted on an "as necessary" basis, with the timing dependant on the criticality of the patch."

National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations* states "SI-2 - The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation.

<u>Recommendation:</u>

Recommendation No. 4: We recommend that EEOC management:

1. Apply software security patch releases on a timely basis to protect against known vulnerabilities.
2. Follow Federal guidance in applying Critical Patch Updates on the required timelines to ensure the systems are not left susceptible to known vulnerabilities.
3. Perform credential scans.

<u>Management Response:</u>

For recommendation items 1&2, EEOC concurs that security patch releases and critical patch updates should be implemented in a timely fashion. EEOC notes, however, that this finding is based on scan results for Apache software, which although was not at the most current version, was up-to-date with all patches (as demonstrated in screen shots and provided to the auditor). EEOC will upgrade to the recommended version by the end of October.

For recommendation item #3, EEOC will assess credential-based agent-less scans (via Nessus) against agent-based scans (via Zenworks 11), as the agent-based alternative appears to have additional benefits, such as elimination of the need by system administrators to maintain credentials on the scanning tools. EEOC will select the preferred approach and identify configuration requirements in 1Q 2012. Credentialed scans or agent-based equivalents will be initiated during 2Q 2012.

Auditor's Evaluation of Management's Response:

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

Account and Identity Management

5. Excessive Virtual Private Network (VPN) Accounts (NFR Reference # 2011 - 4)

Through testing of active VPN accounts, we found 1 separated contractor and 8 separated employees on the list of active VPN accounts.

By having enabled VPN accounts accessible to separated users, EEOC faces increased exposure to the risk of unauthorized access attempts.

EEOC OIT Account Management Procedure (version 2.0) Dated 07/11/2011 states: "Appendix D – Separation Activities Schedule and POCs: It is the responsibility of the VPN admin under the offices of OIT and TND, for both headquarters and field offices, that they

1. Disable and delete account as of COB date of separation or upon receipt of notification e-mail (if notice is post-separation).
2. Send confirmation e-mail to DSSD telework administrator.
3. Update list of VPN users on S:\CLEARANCE

National Institute of Standards and Technology, Special Publication 800-53 Revision 3, Access Control, AC-2 "Account Management" states: "The organization manages information system accounts, including: Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users.

Recommendation:

Recommendation No. 5: We recommend that EEOC management remove VPN accounts of separated employees/contractors and adhering to agency policy. A recertification of accounts should be performed to ensure only active employees have active accounts.

Management Response:

EEOC concurs and will institute quality assurance measures to ensure that current policy for timely removal of VPN accounts and annual recertification are being followed.

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 (FY2010) Findings

Item #	Finding	Description	Control Family	Current Year Status	Comments
1	Certification and accreditation procedures are not fully developed or consistently implemented.	During interviews it was determined that NIST 800 series documents are followed as guidance for C&A but there is no detailed documentation of EEOC procedures for completing a C&A. SSPs reviewed do not show identification of common controls or usage of common controls within the organization. SSP reviews show that "organization defined" portions of NIST controls are not documented.	Certification and accreditation	Closed	Certification and accreditation policy and procedures were established.
2	Information systems are not properly categorized (FIPS 199/SP 800-60).	We did not find any approval signatures on the FIPS categorization document as required by the CIO/CSO;	Certification and accreditation	Closed	CIO/CSO reviewed and signed categorization documents for each system.
3	Minimum baseline security controls are not adequately applied to information systems (FIPS 200/SP 800-53).	FISMA/NIST requires implementation of the NIST 800-53 Rev 3 controls within one year of the release of the document. EEOC systems are not currently using the Rev3 controls and do not have a documented plan to transition to NIST 800-Rev 3. Revision 3 was released August 2009.	Certification and accreditation	Closed	Security Plans are in compliance with NIST 800-53, Revision 3.
4	Other –	The Data Net SSP references the Momentum and IFMS as two separate major applications. It was clarified during interviews that the name refers to the same system. Data Net as a GSS on which multiple information systems reside does not delineate the common controls it provides	Certification and accreditation	Closed.	References were fixed and common controls and minor systems are now listed.

Item #	Finding	Description	Control Family	Current Year Status	Comments
		to the multiple major and minor systems that reside on it. Additionally, the GSS SSP does not list the minor systems that are used by the agency or those that depend on the GSS.			
5	Software scanning capabilities are not fully implemented (NIST 800-53: RA-5, SI-2).	Although software scanning is taking place, currently the scanning capability is limited - scan reports were extremely hard to decipher; authenticated scans are not being conducted; complete vulnerability scans of all devices on the network are not conducted, only representative samples are scanned. Based on review of policy and interviews it was not clear how often scans are conducted. The responses varied between 1 – 6 scans conducted within a year.	Configuration Management	Open	Credentialed scans are still not being performed. Some version upgrade issues were noted. **NFR # 2011 – 03**
6	Remote access procedures are not fully developed or consistently implemented.	Remote access (CISCO configuration screen capture provided) password is not required to be sufficiently complex: password length of 5 characters is permitted and "only character" password is acceptable. The lack of password complexity and length is against best practices, NIST guidance and EEOC policy and procedures.	Remote Access Management	Closed	Password length was revised from 5 characters to a 8 character minimum.
7	Multi-factor authentication is not properly deployed (NIST 800-46, Section 2.2, Section 3.3).	Multi-factor authentication is planned and currently not in place. EEOC has not yet implemented two-factor authentication for remote VPN access to the network because it is waiting to implement the Homeland	Remote Access Management	Open	Multi-factor authentication was not fully implemented. **(See NFR # 2011 – 01)**

Item #	Finding	Description	Control Family	Current Year Status	Comments
		Security Presidential Directive (HSPD) – 12 compliant smart card badge system. This issue has been on the EEOC POA&M for multiple years.			
8	Account management procedures are not fully developed or consistently implemented.	Although account management procedures exist they are not consistently implemented. See g below. 8g identifies the accounts reviewed. We believe that the finding applies to both Cyberscope categories	Account and identity management	Open	Some sampled access request forms were not provided. **(See NFR # 2011 – 05)**
9	Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2).	Several UIDs on the list of enabled VPN accounts corresponded to users who had been separated from the organization for several months. The HP UNIX server reviewed with the UNIX system administrator showed the "hptech" account was not being used but was enabled with admin privileges. Additionally the list of active users on the UNIX server did not match the list of IMS users with elevated privileges provided.	Account and identity management	Open	VPN Access for some sampled separated employees were not disabled. **(See NFR # 2011 – 04)**
10	Agency does not use multi-factor authentication where required (NIST 800-53, IA-2).	Multi-factor authentication is planned and currently not in place.	Account and identity management	Open	Multi-factor authentication was not fully implemented. **(See NFR # 2011 – 01)**
11	Agency does not use dual accounts for administrators (NIST 800-53, AC-5, AC-6).	Per interview with the Windows server system administrator, it was determined that dual accounts for Windows administrators are not used.	Account and identity management	Closed	It was determined that shared accounts were not used in an active directory environment,

Item #	Finding	Description	Control Family	Current Year Status	Comments
					thus the arrangement of shared accounts is accepted.
12	Other –	Microsoft server administrators share admin accounts.	Account and identity management	Closed	It was determined that shared accounts were not used in an active directory environment, thus the arrangement of shared accounts is accepted.
13	Continuous monitoring policy is not fully developed.	A Continuous Monitoring program is currently under development. Policies are missing, including those defining auditable events and log retention requirements.	Continuous Monitoring	Closed	Audit policies were established.
14	Continuous monitoring procedures are not fully developed or consistently implemented.	A Continuous Monitoring program is currently under development. The agency does not define procedures for logging events, reviewing logs and log management.	Continuous Monitoring	Closed	EEOC has defined procedures in policies and security plans.
15	Strategy or plan has not been fully developed for entity-wide continuous monitoring (NIST 800-37).	A Continuous Monitoring program is currently under development	Continuous Monitoring	Closed	EEOC has established a Continuous Monitoring Policy as well as Audit Policies.