Independent Evaluation of U. S. Equal Employment Opportunity Commission Compliance with Provisions of the Federal Information Security Management Act of 2002

Fiscal Year 2013

Final Report

December 5, 2013

Prepared by:
Brown & Company CPAs, PLLC
Certified Public Accountants and Management Consultants

1. Executive Summary

For Fiscal Year (FY) 2013, the U. S. Equal Employment Opportunity Commission (EEOC), Office of Inspector General (OIG), contracted with Brown & Company CPAs, PLLC to conduct an Independent Evaluation of EEOC's compliance with the provisions of the Federal Information Security Management Act of 2002 (FISMA). 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.

Based on the results of its evaluation, Brown & Company concluded that the Agency has made positive strides over the last year in addressing information security weaknesses and continues to make progress in becoming fully FISMA compliant. However, the Agency still faces challenges to fully implement information security requirements as stipulated in various federal guidelines and mandates. This report contains twelve (12) FISMA findings with twelve (12) recommendations concerning issues such as:

- Implementation of Continuous Monitoring policy and procedures;
- Improvement to the physical access security controls for Headquarters and the Alternate Telecom Site;
- Improvement to the Configuration Management policies and procedures;
- Implementation of Multifactor Authentication for physical and logical access; and
- Resolving Internal Vulnerability Assessment results.

2. 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 (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; and
2. An annual OIG independent evaluation of the agency's information security programs and practices.

Furthermore, the OIG must submit annually to the Office of Management and Budget (OMB), through the OMB Max Portal an annual OIG report matrix that depicts the effectiveness of the Agency's information security program.

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 53 field offices, and has its headquarters in Washington, D.C. 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 EEOC Office of Information Technology (OIT) is responsible for planning, developing, implementing and maintaining EEOC's Information Technology (IT) program, policies, standards and procedures. OIT promotes the application and use of information technologies and administers policies and procedures in EEOC to ensure compliance with related federal laws and regulations, to include information security. OIT is responsible for designing the enterprise information architecture; determining the requirements of EEOC's information systems, and developing the integrated systems for nationwide use. OIT plans, evaluates, procures and maintains EEOC's voice and data telecommunications systems, and computer hardware and software in order to provide effective working tools to EEOC employees; and OIT provides a variety of computer services to EEOC offices.

3. Objective

The objective of this independent evaluation is to conduct a review the Agency's information security program and practices. The objective involved reviewing the effectiveness of the Agency's oversight with the information security program and evaluation of the following information systems:

1. Data Network System
2. Document Management System (DMS)
3. Financial Cloud Solutions (FCS)
4. Integrated Mission System (IMS)
5. Federal Personnel Payroll System (FPPS)
6. EEO-1 Survey System

4. Purpose and Scope

The purpose of the independent evaluation is to determine if EEOC's information security program met the requirements of FISMA. In assessing EEOC's adherence to FISMA, 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

The period covered by this independent evaluation is October 1, 2012 through September 30, 2013. Work was performed in accordance with generally accepted government auditing standards (GAGAS).

5. Testing Methodology

Brown & Company's testing methodology included: interviews with EEOC management and staff members; review of legal and regulatory requirements; and review of documentation relating to EEOC's information security program[1].

Brown & Company also contracted with Digital Defense, Inc. (DDI)[2] to conduct an internal vulnerability assessment and penetration testing to determine the exploitability of identified vulnerabilities[3].

6. Findings and Recommendations

Given the range of potential security threats, EEOC is focusing their information security activity on the most cost-effective and efficient controls relevant for their organizations and related mission needs. EEOC is developing strategies, in conjunction with Department of Homeland Security (DHS), to improve the Agency's information security posture.

During our review we identified areas of improvement to the EEOC information system security program. These twelve (12) findings and recommendations are discussed below.

[1] These documents included, but were not limited to, EEOC's 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 system controls.

[2] Digital Defense, Inc. is the premier provider of managed security risk assessment solutions protecting billions in assets for small businesses to Fortune companies in over 65 countries.

[3] The vulnerability assessment is an automated assessment of Internet or intranet connected assets, including firewalls, routers, web and mail servers and other hosts residing within the provided IP address range. Penetration testing involves launching non-destructive, real-world attacks that will identify methods to circumvent security controls.

Finding 1	**EEOC physical access controls are not effective for limiting access to EEOC controlled areas.**

Condition:

During our review of physical access controls at the EEOC Headquarters, Washington, D.C., we observed EEOC personnel entering and exiting EEOC controlled areas without being required to scan their EEOC provided employee identification badges at security entry points. Specifically, on multiple occasions we observed EEOC security doors on the fourth and fifth floor propped open, allowing an individual access to EEOC controlled areas without proper security system authorization using an EEOC provided credential. For example, during the week of July 25, 2013, we observed five individuals exiting the fifth floor elevator and walking through the open security doors without scanning their badge.

Criteria:

NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations

In accordance with NIST SP 800-53, rev 3, the agency is required to have effective physical access controls over controlled areas. A control area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.

PE-3 Physical Access Control

Control: The organization:

- Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);
- Verifies individual access authorizations before granting access to the facility;
- Controls entry to the facility containing the information system using physical access devices and/or guards; and
- Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk.

Cause:

EEOC has implemented a practice (for the convenience of its employees) of propping open the security doors that lead to EEOC office suites with a rubber door stop during business hours.

Effect:

The effects of open security doors are: lack of enforcement of the Agency's physical access controls which includes identification of personnel accessing control areas; lack of control over unauthorized individuals physically accessing EEOC space, and possibly obtaining unauthorized access to EEOC information and information systems; and lack of monitoring controls which includes recording badge identifications that are used to access EEOC controlled areas.

Recommendation 1:

We recommend that EEOC Office of the Chief Financial Officer, Central Services Division require all security doors to be closed at all times and require EEOC employees to use their EEOC provided employee identification badges (proximity/HSPD-12) to gain entrance to EEOC controlled spaces.

Management Response:

Management agrees with the finding and recommendation. The recommendation has been implemented to close security doors on the fourth and fifth floor and require EEOC employees to use their EEOC provided employee identification to gain entrance to EEOC controlled spaces.

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation.

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

Finding 2	**EEOC Configuration Management Plans do not define hardware and software which compromises the various Information Systems.**

Condition:

During our review of the configuration management plans, the hardware/software inventory has not been identified and incorporated into the baseline Configuration Management Plans. The hardware/software inventory is listed for each system in various schedules maintained by the Agency, but it is not included as part of the Configuration Management Plans.

Criteria:

NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations

In accordance with NIST SP 800-53, rev 3, CM-9, the agency is required to define the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management.

CM-9 Configuration Management Plan

Control: The organization develops, documents, and implements a configuration management plan for the information system that:

- Addresses roles, responsibilities, and configuration management processes and procedures;
- Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management;
- Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.

Cause:

EEOC OIT has documented the hardware/software inventory in separate documents other than the Configuration Management Plan in order to update the list as needed, without revising the Configuration Management Plan.

Effect:

As a result of hardware/software listing included within separate documentation other than the Configuration Management Plan, incorrect hardware, software and incorrect versions of that respective hardware and software can be installed within the various information systems.

Recommendation 2:

We recommend that EEOC OIT define the configuration items (hardware/software inventory) for the information system within the Configuration Management Plan. We recommend that OIT document the hardware/software inventory in the Configuration Management Plan or provide a direct reference to where the current hardware/ software inventory lists are located.

Management Response:

Management agrees with the audit finding and recommendations. The following comment was provided: "OIT will create an appendix to the Configuration Management Plan which provides the DMS links to the various system HW/SW inventories."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendations.

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

Finding 3	**EEOC Security Plan, which covers physical security controls, is not updated to include consideration of federal authorities' current guidelines.**

Condition:

The EEOC security management program has been developed, documented, and implemented in its System Security Plans and EEOC Directives.

As stated in EEOC Order 240-005 *Information Security Program chg,* the Order "provides policies, standards, procedures and methods related to EEOC's Information Security Program, as required by the Federal Information Security Management Act of 2002 (FISMA) and Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*. It explains in greater detail EEOC's Information Security Program, which is described in general terms in Appendix C of EEOC Order 370.002, *EEOC Security Plan*. This Order also serves as a handbook for the implementation of EEOC's Information Security Program and policy."

The EEOC Order 370.002, *Security Plan* consists of four policy statements that focus on Physical Security, Workplace Violence, Automated Information Security, and Personnel Suitability and Investigations. The EEOC Security Plan outlines policies and procedures that serve to sustain a safe and secure workplace.

During our research, we noted that the following authorities sited by EEOC Order 370-002, *Security Plan* have issued new directives and guidelines since June 2000:

- "Title 18, United States Code (18 USC); Occupational Safety and Health Act (OSHA) of 1970 (P.L. 91-596); Public Law 91-596 84 STAT. 1590 91st Congress, S.2193 December 29, 1970" – has been amended through January 1, 2004.

In addition, OSHA announces changes to recordkeeping rule for federal agencies to improve tracking of federal workplace injuries, illnesses effective August 2013.

- "Federal Property Management Regulations, 41 CFR 101-20" – has been update through "SOURCE: 67 FR 76883, Dec. 13, 2002".

During our review, we noted that the EEOC Order 370-002, *Security Plan* dated June 28, 2000 has not been updated to include federal authority updates since 2000.

Criteria:

NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations

PE-1 Physical and Environmental Protection Policy and Procedures

Control: The organization develops, disseminates, and reviews/updates:

- A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

Cause:

EEOC has not completed the process of updating security management program documents. EEOC has stated in the Security Awareness Training that the EEOC Security Plan (Order 370.002) is under revision.

Effect:

The effect of not updating EEOC Order 370-002, *Security Plan* is that the Agency risks not producing the procedures that are required for the effective implementation of selected security controls and control enhancements in the physical and environmental protection family. The policy and procedures may not be consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Recommendation 3:

We recommend that EEOC Office of the Chief Financial Officer, Central Services Division update EEOC Order 370-002, *Security Plan* to reflect consideration of updated authorities.

Management Response:

Management agrees to update the Security Plan.

Auditor's Evaluation of Management's Response:

Management should ensure updates to the Security Plan include the procedures that are required for the effective implementation of security controls and are consistent with current applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

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

Finding 4	**EEOC did not fully implement multifactor authentication to allow remote access to EEOC systems.**

Condition:

EEOC has not implemented multifactor authentication where one of the factors is provided by a device separate from the computer gaining remote access.

EEOC requires only a user ID and password to access EEOC information system and does not require the use of an authentication device such as a token or HSPD-12 PIV card for remote computer or network authentication.

Criteria:

NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations

IA-2 Identification and Authentication (Organizational Users)

Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

NIST SP 800-53, 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."

OMB M-06-16, *Protection of Sensitive Agency Information*, dated June 23, 2006, states the following regarding two-factor authentication: "The National Institute of Standards and Technology (NIST) provided a checklist for protection of remote information…recommending all departments and agencies take the following actions:

1. Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing;
2. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;

3. Use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity; and
4. Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required."

Cause:

EEOC's implementation of a multifactor authentication process to access systems remotely requires coordinating and funding the engineering, design, procurement, deployment and support of the Common Identification Standard for Federal Employees and Contractors (HSPD-12 PIV card) within EEOC. Currently, due to lack of funding and other Agency priorities, EEOC is not able to implement the standards for multifactor authentication by a device separate from the computer gaining access.

Effect:

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

Recommendation 4:

We recommend EEOC Office of Information Technology implement multifactor authentication for remote access. We recommend EECO uses multifactor authentication where one of the factors is provided by a device separate from the computer gaining access.

Management Response:

Management agrees with the audit findings and recommendations. The following comment was made:

"OIT concurs with the need to implement two-factor authentication for remote access. We are continuing to look at alternatives, as solutions continue to improve and evolve. EEOC's priority for FY 2014 is migration to Windows 7 from Windows XP. Pilot implementation for remote two-factor authentication during 2014 is pending funding and staff resource availability."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation.

Full implementation of two-factor authentication will resolve the finding.

Finding 5	Configuration change requests did not have approval signatures by Change Configuration Board (CCB).

Condition:

During our review of OIT Configuration Control Change Request (CCCR) form, certain changes did not have approval signatures by Configuration Control Board (CCB) team. The change request form has section for appropriate personnel to approve changes, but the field was blank. For example, the CCB sign off was missing for:

- CCCR #: 0012, System: Windows XP Workstation Configuration Update, Configuration Item: Update JAVA client to JAVA 6 Update 35, Proposed By/Date: 10/31/12, Proposed Implementation Date: 10/31/12.

Criteria:

NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations

In accordance with NIST SP 800-53, rev 3, the agency is required to determine the types of changes to the information system that are configuration controlled. Configuration change control for the information system involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications.

CM-3 Configuration Change Control

Control: The organization:

- Determines the types of changes to the information system that are configuration controlled;
- Approves configuration-controlled changes to the system with explicit consideration for security impact analyses;
- Documents approved configuration-controlled changes to the system;
- Retains and reviews records of configuration-controlled changes to the system;
- Audits activities associated with configuration-controlled changes to the system; and
- Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board)] that convenes [Selection: (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].

Cause:

EEOC does not ensure that all configuration changes are signed by CCB. Change request approvals are not documented.

Effect:

The effects of unapproved change request are baseline configuration compromised, security considerations not considered and unauthorized configuration changes occurring.

Recommendation 5:

We recommend OIT ensure all configuration change request forms are signed to document review and approval.

Management Response:

Management agrees with the audit findings and recommendations. The following comment was made:

"OIT will incorporate an electronic approval process into the new automated Configuration Change request process that will be developed in Service Now during FY 2014. In the interim, OIT will maintain the current manual process of emailing the Change Request to the applicable parties for review/comment/concurrence, with ISOs noting the final overall concurrence in the change request log."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation.

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

Finding 6	**EEOC internal vulnerability assessment identified risk vulnerabilities that should be analyzed and resolved.**

Condition:

An Internal Vulnerability Assessment was performed on EEOC's internal computer networks from August 26, 2013 to August 29, 2013 by DDI on behalf of Brown & Company CPAs, PLLC. The Vulnerability Assessment is an automated assessment of Internet or intranet connected assets, including firewalls, routers, web and mail servers and other hosts residing within the provided IP address range.

The Internal Vulnerability Assessment executive summary report and detail report were presented to EEOC Office of Information Technology for review and analysis. The assessment discovered 2,616 hosts. The hosts have 1,075 occurrences of 31 high-risk vulnerabilities, 607 occurrences of 20 medium-risk vulnerabilities, and 5,156 occurrences of 83 low-risk vulnerabilities.

Criteria:

NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations

RA-5 Vulnerability Scanning

Control: The organization:

- Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported;
- Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
  -Enumerating platforms, software flaws, and improper configurations;
  -Formatting and making transparent, checklists and test procedures; and
  -Measuring vulnerability impact;
- Analyzes vulnerability scan reports and results from security control assessments;
- Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and
- Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Cause:

EEOC OIT has not scanned all devices connected to EEOC systems in order to identify and/or resolve the risk vulnerabilities.

As stated in the EEOC *OIT Implementation for Credential-Based Vulnerability Scanning*, "PC-based workstations have not heretofore been scanned due to:(1) limitation of resources (especially as to scanning tool in prior use), (2) expectation that risk has been low because all such target systems have been created in cloned image with administrative rights restricted from users, and (3) firewall blocks substantially reducing utility of attempts at agentless scanning. Also "the second target group consists of devices which will not be scanned during FY2012, for which the Agency accepts risk. These will include network-enabled printers and printer-based multifunctional devices, because scanning techniques available to EEOC do not support effective scans of such devices, and certain 'service network' non-data devices, such as alarm systems, because OIT does not maintain these systems."

Effect:

The effects of high-risk and moderate-risk vulnerabilities if exploited are (1) an intruder could gain user or administrative access to the EEOC host and have the ability to run commands,

access or delete files, and launch attacks against other EEOC hosts; and/or (2) an intruder would gain valuable information about the EEOC host which could aid in gaining access.

The effect of low-risk vulnerabilities if exploited is an intruder could gain information about the EEOC system, but it would not necessarily lead to access.

Recommendation 6:

We recommend the EEOC OIT review and analyze high-risk and moderate-risk vulnerability. These vulnerabilities should be resolved to avoid compromise to the EEOC's system; or the Agency should document acceptance of the risk or reclassification of the risk.

Management Response:

Management agrees with the audit finding and recommendation.

Auditor's Evaluation of Management's Response:

Effective implementation of the recommendation should resolve the reported condition and recommendation.

Finding 7	**Emergency change requests are not identified within configuration change request.**

Condition:

EEOC could not document whether emergency changes were performed during the fiscal year, since the same configuration change request form is use for all types of occurrences.

Criteria:

NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations

In accordance with NIST SP 800-53, rev 3, configuration change control includes changes to components of the information system, changes to the configuration settings for information technology products (e.g., operating systems, applications, firewalls, and routers), emergency changes, and changes to remediate flaws.

CM-3 Configuration Change Control

The organization:

- Determines the types of changes to the information system that are configuration controlled;

- Approves configuration-controlled changes to the system with explicit consideration for Security impact analyses;
- Documents approved configuration-controlled changes to the system;
- Retains and reviews records of configuration-controlled changes to the system;
- Audits activities associated with configuration-controlled changes to the system; and
- Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, Board)] that convenes [Selection: (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].

Cause:

EEOC configuration change request document does not define what type of change is occurring.

Effect:

Configuration Control Board (CCB) is not able to determine if changes are for normal configuration changes or emergency changes.

Recommendation 7:

We recommend EEOC Office of Information Technology include an option box or a check box on the Change Request forms for emergency changes to ensure CCB approvers have enough information pertaining to the type of change request.

Management Response:

Management agrees with the audit finding and recommendation.

Auditor's Evaluation of Management's Response:

Effective implementation of the recommendation should resolve the reported condition and recommendation.

Finding 8	**EEOC has not consistently documented the exit clearance process for separated/terminated personnel.**

Condition:

EEOC Headquarters' Administrative Offices /District Directors and/or their designees have the responsibility to ensure that each exiting employee is properly cleared prior to separating from the EEOC. The EEOC exit clearance process requires the exiting employee to return, and surrender to the responsible EEOC officials, all Government property and all other official documents and materials. To ensure the exit clearance process is complete, the EEOC requires

the exiting employee to receive and complete an Exit Questionnaire provided by the Office of Human Resources and/or Servicing Personnel Office; and an EEOC Form 470, Employee Clearance Record provided by the Administrative Official.

During our review of the EEOC's personnel termination policies and procedures, we sampled 18 of 125 separated personnel for the period October 1, 2012 through June 30, 2013. For the samples selected, we requested and examined EEOC Exit Questionnaires and EEOC Form 470, Contractor and Employee Clearance Record forms to determine whether EEOC:

- Conducts exit interviews;
- Retrieves all security-related organizational information system-related property; and
- Retains access to organizational information and information systems formerly controlled by terminated individual.

EEOC did not have Exit Questionnaires for 15 of the 18 samples selected. EEOC did not have Form 470 forms for 8 of the 18 samples selected. We conclude that EEOC exit clearance process is not effective.

Criteria:

EEOC Order 501.006 CLEARANCE PROCEDURES POLICY.

It is EEOC policy that upon termination of employment, EEOC employees must turn in all Government personal property and other "official" items they are responsible for, such as their Government charge card, office keys, and outstanding debts owed to the Federal Government. It is also EEOC policy to "clear" employees prior to their separation or termination date. Therefore, EEOC Form 470, Employee Clearance Record, must be initiated immediately upon the employee's intent to separate from EEOC.

The EEOC Form 470 requires the following EMPLOYEE'S STATEMENT - *I am returning, and have surrendered to the responsible EEOC officials, all Government property, and all other official documents and materials with which I was charged, for which I was accountable, or which I had in my POSSESSION.*

NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations

PS-4 Personnel Termination

Control: The organization, upon termination of individual employment:

- Terminates information system access;
- Conducts exit interviews;
- Retrieves all security-related organizational information system-related property; and
- Retains access to organizational information and information systems formerly controlled by terminated individual.

Cause:

EEOC Headquarters' Administrative Offices and District Directors do not have effective procedures to ensure exiting employee complete the clearance process including completing the Exit Questionnaire and EEOC Form 470 Clearance Record.

Effect:

Lack of completing the exit clearance process increases the risk that information system-related property including authentication devices, system administration technical manuals, keys, identification cards, and building passes are not returned to the EEOC.

EEOC does not have effective exit interviews procedures to ensure that individuals understand any security constraints imposed by being former employees and that proper accountability is achieved for all information system related property.

Recommendation 8:

We recommend that the EEOC Office of Chief Human Capital Officer work with EEOC Headquarters' Administrative Offices and District Directors regarding:

1 - Implementing procedures and to ensure compliance with EEOC Order 501.006 Clearance Procedures; and

2 - Implementing procedures to ensure that all separated/terminated EEOC employees complete the EEOC Exit Questionnaire and EEOC Form 470, Contractor and Employee Clearance Record.

Management Response:

Management agrees with the audit findings and recommendations.

Auditor's Evaluation of Management's Response:

Effective implementation of the recommendations should resolve the reported condition and recommendation.

Finding 9	**EEOC Alternate Telecom Site does not use Radio Frequency Identification (RFID) card reader system to monitor and document access to the server room.**

Condition:

EEOC currently has two systems in place for data recovery: the first is the Alternate Telecom Site at the Baltimore Field Office for Internet access, GroupWise, DNS, VPN, and BlackBerry,

and the second is the SunGard Recovery site located in Philadelphia for IMS and DMS. Both sites are used to support EEOC Contingency Plan and Continuity of Operations, and must be secured and monitored at all times.

During our visit to the Alternate Telecom Site, we noted that the data server rooms were secured with lock and key but did not use a RFID card reader system which establishes a log of individuals accessing the control areas. Without a RFID card reader system, EEOC OIT is not able to monitor and accurately document access to the Alternate Telecom Site.

Criteria:

NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations

PE-6 Monitoring Physical Access

Control: The organization:

- Monitors physical access to the information system to detect and respond to physical security incidents;
- Reviews physical access logs [*Assignment: organization-defined frequency*]; and
- Coordinates results of reviews and investigations with the organization's incident response capability.

Cause:

The OIT issued policies and procedures requiring proximity cards and reader for monitoring access to EEOC Headquarter data center, but did not issue similar requirements for the Alternate Telecom Site.

Effect:

Without implementing the use of a RFID card reader system to access the Alternate Telecom Site the Agency is unable to monitor and document access to sensitive systems and control areas. The lack of monitoring secured areas increases the risk of unauthorized access to sensitive information and information systems required to support EEOC operations.

Recommendation 9:

We recommend EEOC OIT develop and implement procedures that require the use of RFID card reader system to access the EEOC Alternate Telecom Site and monitor access on a regular basis.

Management Response:

Management does not agree with recommendations and provided the following response:

"In response to this finding, EEOC looked into alternatives to provide card reader access to better secure the Alternate Telecom Site located at our Baltimore Field Office. One option considered was to implement a card system that would interface with the security system at EEOC Headquarters (HQ), to allow OCFO staff to provide the system administration and oversight for Baltimore through our pre-existing system. This option was not possible as our HQ Security network is not connected to the EEOC wide-area network. It is an isolated network within Headquarters, purposely segregated from the primary network for security reasons. The second option considered was a stand-alone local system located within the Baltimore office space. This solution was determined to be impractical, as the Baltimore Office does not have an IT Specialist onsite, nor the resources to provide system administration, card management, and security oversight.

Therefore, EEOC will accept the risk related to key-based access, with the implementation of additional compensating controls to reduce overall risk. Access to the Baltimore building is restricted to key card access after hours, and guard identification card review during office hours. Within the building, access to the EEOC office space is controlled by a combination cipher lock. The Server Room within this space is kept locked, with four keys that are issued to the Office Director, the Resource Management Director, the OIT Data Center Manager, and a single spare which is locked in a key box. To provide additional compensating controls to lessen the overall risk, OIT and OCFO will work with Baltimore staff to document and implement new procedures to enforce a strict physical key control system and manual written access log process."

Auditor's Evaluation of Management's Response:

The Alternate Telecom Site located in the Baltimore Field Office is the second most important EEOC maintained data site. The site maintains sensitive and important EEOC information and information system connectivity. The site provides the means for the Agency to continue its most critical work even if the primary site is rendered inoperable. Due to the importance of this site, ensuring that strong physical security controls are in place and consistent with EEOC Headquarters' Computer Room Access Policy, which requires card reader access, should be high priority for the Agency.

Management's implementation of additional compensating controls will not provide a level of security commensurate to the level of importance of the site or the Agency's policy for computer room access. The implementation of strict physical key control system and manual written access log process will not provide monitoring of the physical access to the information system to detect and or allow for a timely respond to physical security incidents. The use of an RFID system using Homeland Security Presidential Directive (HSPD) – 12 Personal Identity Verification (PIV) Cards provides for better security, accountability and audit log management than a key control system and manual written access log process.

Furthermore, concerning the resources necessary to establish and maintain a RFID system there are a number of systems on the market that that are not resource intensive or require a specialized information technology/security skill set to properly manage.

We continue to recommend EEOC OIT develop and implement procedures that require the use of RFID card reader system to access the EEOC Alternate Telecom Site and monitor access on a regular basis.

Finding 10	**EEOC card access control system reports a significant number of false alarms for "Door Held Open" and "Door Force Open," and adversely affects the Agency's ability to identify physical security incidences and monitor physical access.**

Condition:

During our review of physical security access controls at the EEOC Headquarters, Washington DC, we examined card access control system logs for the period June 1, 2013 thru September 15, 2013 covering the EEOC's primary entrances (main conference room, fourth floor, fifth floor, and sixth floor). Our analysis of the card access control system logs data reported 22,740 "Door Held Open" recordings and 4,106 "Door Forced Open" recording for all entrances reviewed. The following is a summary of recordings by EEOC entrances:

EEOC Entrances	Door Held Opened	Door Forced Opened
1ST FL MAIN CONF CENTER	1,617	1,338
4TH FL E-LBY	7,361	40
4TH FL NW. STAIRWELL-1	9	762
5TH FL E-LBY	4,555	435
6TH FL E-LBY	9,023	456
6TH FL Z12A DOOR	175	1,075
Totals	22,740	4,106

EEOC Office of the Chief Financial Officer (OCFO), Central Services Division (CSD) management explained that the "Door Held Open" recording is typically associated with the security door being opened using the Americans with Disabilities Act (ADA) exit button; or propped open; or someone physically holding it open while exiting for a specified period of time for alarm, which the system records as "Door Held Open." Also, it was explained that when a person is exiting a managed and secured EEOC space and approaches a secured door, the sensor is triggered and disengages the lock, the person pushes the door open - the C*CURE system records that as "Door Forced Open."

In most cases, these "Door Held Open" and "Door Forced Open" alarms are false alarms and occurred when access card holders used the access controlled door in normal manner, yet the card access control system triggered an alarm. Consequently, the card access control system reports a significant number of false alarms for "Door Held Open" and "Door Force Open," and adversely affects the Agency's ability to identify physical security incidences and monitor physical access.

Criteria:

NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations

In accordance with NIST SP 800-53, rev 3, the agency is required to have effective physical access controls over controlled areas. A control area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.

PE-6 Monitoring Physical Access

Control: The organization:

- Monitors physical access to the information system to detect and respond to physical security incidents;
- Reviews physical access logs [*Assignment: organization-defined frequency*]; and
- Coordinates results of reviews and investigations with the organization's incident response capability.

  Supplemental Guidance: Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities are part of the organization's incident response capability.

Cause:

The EEOC access controlled doors have the following devices: card reader on outside (non-secured) side of door, request-to-exit (REX) device (sensor) on inside (secured) side of door, electric lock hardware, and door position switch. All of the devices at the door are connected to the access control system. A false alarm will occur as a result of any of the following:

- Miscoding the " Door Held Open" criteria for an alarm, such as using the ADA devices to exit
- Miscoding the "Door Forced Open" criteria for an alarm, such as triggering the sensor when exiting
- Improper request-to-exit (REX) device (sensor) motion detector coverage
- Improper REX/sensor motion detector settings
- Improper lock hardware function

Effect:

The EEOC access control system is not effective in reporting physical security incidents so that the EEOC security monitoring center is notified whenever a valid "Door Held Open" or "Door Forced Open" condition occurs, allowing an appropriate security response to be made.

The possible miscoding of alarm criteria and improper device setting cause hundreds of false alarms per day; and eventually, monitoring staff may become complacent about "Door Held Open" or "Door Forced Open" alarms, or choose to ignore them completely.

The effects of not monitoring physical access are: lack of enforcement of the Agency's physical access controls which includes identification of personnel accessing control areas; lack of control over unauthorized individuals physically accessing EEOC space, and possibly obtaining unauthorized access to EEOC information and information system; and lack of monitoring controls which includes recording badge identifications that are used to access EEOC controlled areas.

Recommendation 10:

While false alarms can never be entirely eliminated, they can be significantly reduced through effective system design.

We recommend that EEOC, Office of the Chief Financial Officer, Central Services Division:

1. Develop and implement door monitoring procedures to improve security and provides assurance that all doors are being used as intended.
2. Examine the cause of "Door Held Open" and "Door Force Open" alarms and implement corrective action to significantly dues the number for false alarms.
3. Recode the security monitoring system to identify physical security incidents that warrants an investigation or response; specifically define criteria for "Door Held Open" and "Door Force Open"
4. Develop access control reports that uniquely identify security violation and suspicious physical access activities.

Management Response:

Management disagrees with the findings and recommendations and provided the following response: "The terminology, or language, used within the C*CURE system for door monitoring of "Held Open" and "Force Open" are not false alarms. EEOC Security Specialists will inquire with the software provider if the capability exists with the end user to change such language within the operating system."

Auditor's Evaluation of Management's Response:

Management's response does not address the Agency's ability to correctly identify physical security incidences, monitor physical access, and respond in an appropriate manner using the card access control system logs. As explained by the Supervisory Security Specialist, "when a person is exiting EEOC space and approaches a secured door, the sensor is triggered and disengages the lock, the person pushes the door open - the C*CURE system records that as "Force Open." In this situation, when a "Force Open" is recorded but does not meet the criteria of a valid alarm, it is considered a "false alarm." The change in terminology to identify physical

security violations, if implemented effectively, should properly report alarms that put the Agency at risk and requires the security personnel to investigate.

Until card access control system terminology is changed or the system's software/hardware is adjusted to reduced or resolved "Door Held Open" and "Door Force Open" alarms, we continue to recommend that management:

1. Develop and implement door monitoring procedures to improve security and provides assurance that all doors are being used as intended.
2. Examine the cause of "Door Held Open" and "Door Force Open" alarms and implement corrective action to significantly reduce the number for false alarms.
3. Recode the security monitoring system to identify physical security incidents that warrant an investigation or response; specifically define criteria for "Door Held Open" and "Door Force Open."

Finding 11 EEOC physical access controls are not adequate for monitoring the cleaning crew's access to EEOC's controlled areas.

Condition:

The Office of the Chief Financial Officer (OCFO), Central Services Division (CSD) Security Team issued DATAWATCH proximity cards for the EEOC janitorial contractor and cleaning crew members. The CSD Security Specialist maintains a Key Control Log listing each cleaning crew's name and badge number. The CSD Security Specialist holds the badges and issues the cleaning crew members their respective/assigned access badge upon reporting to work.

During our review of the EEOC Headquarters' physical security access logs and records, we noticed that thirteen of the cleaning crew's proximity cards are recorded in the Card security profile under the same name and numbered 1 thru 13. Lack of recording the name of the badge holders is not adequate record keeping and reduces the effectiveness of monitoring physical access.

Criteria:

NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations

In accordance with NIST SP 800-53, rev 3, the agency is required to have effective physical access controls over controlled areas. A control area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.

PE-3 Physical Access Control

Control: The organization:

- Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);
- Verifies individual access authorizations before granting access to the facility;
- Controls entry to the facility containing the information system using physical access devices and/or guards; and
- Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk.

Cause:

Due to the turnover of cleaning crew personnel, EEOC has implemented a practice of recording the crew member badges under one name.

Effect:

The effects of not properly recording the cleaning crew member name in the security log are: lack of enforcement of the Agency's physical access controls which includes identification of personnel accessing control areas; lack of control over unauthorized individuals physically accessing EEOC space, and possibly obtaining unauthorized access to EEOC information and information system; and lack of monitoring controls which includes recording badge identifications that are used to access EEOC controlled areas.

Recommendation 11:

1. We recommend the Office of the Chief Financial Officer (OCFO), Central Services Division (CSD) require all cleaning crew member names to be recorded in the physical security reporting system.

2. We recommend the Office of the Chief Financial Officer (OCFO), Central Services Division (CSD) ensure each member of the cleaning crew receives and uses the access card that is properly assigned to the person.

Management Response:

Management does not agree with the findings and recommendations, and provide the following comment: "The Office of the Chief Financial Officer (OCFO), Central Services Division (CSD) Security Specialists issued entry access control cards to Crystal Reddick, Senior Building Manager, Jones, Lang LaSalle (JLL) for the janitorial cleaning crew contracted through Total Quality. Ms. Reddick and her staff maintain a Key Control Log, which was provided to the audit team, and have assigned each cleaning crew member, by name, with a specific entry access control card. It is JLL's key control policy that these entry access control cards remain on the

premises and are issued to the cleaning crew members as they report to work and are subsequently returned. Entry access control logs can be effectively reviewed and audited against the issued card numbers and the JLL Key Control Log."

Auditor's Evaluation of Management's Response:

Management's response to allow the building manager to have unlimited access to the crew member's access cards is not consistent with the Agency's physical security access control policies and procedures for issuing access cards to individuals, who are responsible for the badges. As stated in EEOC Security Plan, it is the responsibility of the EEOC Security Official/Security Representative to monitor the identification badge program including badge issuances, log maintenance, and notifying appropriate staff and guards of any lost or stolen badges. This responsibility cannot be designated to another organization, especially a private organization that is not required to adhere to physical security requirements of FISMA.

Management's response that "entry access control logs can be effectively reviewed and audited against the issued card numbers and the JLL Key Control Log" does not ensure that the access card is given to the correct individual. Also the lack of recording the crew member's name in the Agency system does not identify the individual on the entry access control logs for proper monitoring of physical access to EEOC offices.

We continue to recommend that management require all cleaning crew member names to be recorded in the physical security reporting system and ensure each member of the cleaning crew receives and uses the access card that is properly assigned to the person.

Finding 12	**EEOC's Continuous Monitoring Policy and Procedures are not fully developed and implemented**

Condition:

EEOC Continuous Monitoring policy and procedures have not been fully developed and implemented in accordance with NIST guidelines. EEOC Information Security Continuous Monitoring (ISCM) Plan adopted in 2011 is outdated and is presently being redrafted as the Agency develops a comprehensive continuous monitoring process, as described in NIST SP 800–137, which consists of:

1. Define continuous monitoring strategy
2. Establish continuous monitoring program
   a) Determine metrics
   b) Determine monitoring frequencies
   c) Develop ISCM architecture
3. Implement the monitoring program
4. Analyze security-related information (data) and report findings
5. Respond with mitigation actions OR reject/avoid, transfer, or accept risk
6. Review and update monitoring strategy and program

The draft EEOC ISCM policies and procedures were put on hold, since EEOC was selected as a pilot ('Early Engagement') participant in the new Department of Homeland Security (DHS) Continuous Diagnostics and Mitigations (CDM) program, which provides grants in technology (hardware, software, services), ISCM management and reporting, and training. Also, revision to procedures was needed since there was a substantial difference between EEOC ISCM planning per the NIST-centric ISCM Working Group and the ISCM plans announced by DHS.

Criteria:

NIST Special Publication 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations states:

- Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations selected guidelines are listed below:

CA-7 Continuous Monitoring

Control: The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:

- A configuration management process for the information system and its constituent components;
- A determination of the security impact of changes to the information system and environment of operation;
- Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and
- Reporting the security state of the information system to appropriate organizational officials [*Assignment: organization-defined frequency*]

Cause:

The Agency's ISCM effort and development of policies and procedures have been largely limited by lack of funds. Also, OIT's limited resources were used to support time-sensitive projects such as the Financial Management, HSPD-12 deployment, and Quick Time HR tracking.

Since OIT chose to pursue ISCM implementation through DHS CDM, the Agency needs to update its ISCM policies and procedures.

Effect:

As a result of Continuous Monitoring policy and procedures not being established and incomplete implementation of the DHS CDM pilot program, there is inherent risk for information systems and corresponding system owners not having the appropriate guidance for monitoring the Agency's information and information systems.

Recommendation 12:

1. We recommend EEOC Office of Information Technology continue to develop and implement its continuous monitoring policy and procedures in accordance with NIST guideline to ensure that all security controls (including those controls designated by DHS) are monitored on an ongoing basis.

2. We recommend EEOC continued work under DHS CDM pilot program to support Agency's implementation of Continuous Monitoring.

Management Response

Management agrees with the audit findings and recommendations.

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the findings and recommendations.

Effective implementation of the recommendations should resolve the reported condition and recommendations.