Independent Evaluation of
U. S. Equal Employment Opportunity Commission
Compliance with Provisions of the
Federal Information Security Management Act of 2002
(OIG Report No. 2014-08-EOIG)

For Fiscal Year 2014

Prepared by:

Brown & Company CPAs, PLLC
Certified Public Accountants and Management Consultants
1101 Mercantile Lane, Suite 122
Largo, Maryland 20774
(240) 770-4903

Date: December 16, 2014

BROWN & COMPANY CPAs, PLLC

CERTIFIED PUBLIC ACCOUNTANTS AND MANAGEMENT CONSULTANTS

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

For Fiscal Year 2014

Inspector General of the
U.S. Equal Employment Opportunity Commission:

Brown & Company CPAs, PLLC (Brown & Company) is pleased to submit this report in support of evaluation services provided pursuant to requirements of the Federal Information Security Management Act of 2002 (FISMA).

Brown & Company conducted an independent evaluation of the U.S. Equal Employment Opportunity Commission's information security program for the fiscal year (FY) ended September 30, 2014. The period covered by this independent evaluation is October 1, 2013 through September 30, 2014. The FISMA evaluation was performed from July 14, 2014 to October 31, 2014.

We conducted the FISMA evaluation in accordance with the *Government Auditing Standards* and Office of Management and Budget's most recent FISMA reporting guidance. These standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on the evaluation objectives.

Brown & Company

Largo, Maryland
December 16, 2014

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

For Fiscal Year 2014

Table of Contents

1. Executive Summary

For Fiscal Year (FY) 2014, the U. S. Equal Employment Opportunity Commission (EEOC), Office of Inspector General (OIG) contracted with Brown & Company CPAs, PLLC (Brown & Company) to conduct an independent valuation 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 the evaluation, Brown & Company concluded that the agency has made positive strides in addressing information security weaknesses, however, the agency still faces challenges to fully implement information security requirements as stipulated in various federal guidelines and mandates. This report contains nineteen (19) FISMA findings with nineteen (19) recommendations concerning issues such as:

1. Development of a risk assessment at the organization and mission-business level to include field offices.
2. Update to system level risk assessment report.
3. Improvement to Bring Your Own Device (BYOD) program.
4. Improvement to privacy notifications on the EEOC official website and alerts when visitor are directed to non-government websites.
5. Improvement to virtual private network configuration settings for password length.
6. Implementation of encryption to protect digital backup media during transport.
7. Update to policies and procedures to include EEOC's response time for security alerts.
8. Update to policies and procedures to include file integrity process for detecting unauthorized changes to software, firmware, and information.
9. Improvement to monitoring laptops issued to employees for disaster recovery and ensuring that patches and updates are installed for operating systems, antivirus software and other security applications.
10. Implementation of background checks for student interns to ensure international visas are current.
11. Improvement to the security awareness training program to ensure all personnel in field offices that use information systems receive annual training.
12. Development of policies and procedures to properly manage physical security access cards.
13. Implementation of full device encryption or container-based encryption for mobile laptops.
14. Development of Continuity of Operations Plan for field offices.
15. Development of a telecommuting policy that meets FISMA requirements.
16. Development of policies and procedures for managing shared group accounts.
17. Improvement to account management procedures that include disabling inactive accounts as required.
18. Improvement to physical access control to the data center and technology storage room.
19. Resolution of high and medium vulnerabilities identified from the internal vulnerability assessment.

2. Background

Federal Information Security Management Act of 2002 (FISMA)

FISMA was enacted into law as Title III of the E-Government Act (E-Gov) of 2002 (Public Law. 107-347, December 17, 2002). The two key requirements of FISMA are:

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. OIGs are to conduct an annual 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 (Cyberscope) an annual report matrix that depicts the effectiveness of the agency's information security program.

The Organization

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 a Headquarters (HQ) in Washington, D.C. The EEOC is composed of five Commissioners and a General Counsel appointed by the U.S. President and confirmed by the U.S. Senate. Commissioners are appointed for five-year staggered terms; the General Counsel's term is for 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 within 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.

3. Objective

The objective of this independent evaluation is to conduct a review of EEOC's information security program and practices. The objective involved reviewing the effectiveness of the agency's oversight of 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 meets the requirements of FISMA. In assessing EEOC's adherence with FISMA, the following areas were reviewed:

- Continuous Monitoring Management
- Identity and Access Management
- Risk Management
- Plan of Action and Milestones
- Telework and Bring Your Own Device
- Contingency Planning
- Security Capital Planning
- Configuration Management
- Incident Response and Reporting
- Security Training
- Remote Access Management
- Background Checks
- Contractor Systems

The period covered by this independent evaluation is October 1, 2013 through September 30, 2014. Work was performed in accordance with generally accepted government auditing standards (GAGAS).

5. Testing Methodology

Brown & Company's testing methodology include interviews with EEOC management and staff; review of legal and regulatory requirements; and review of documentation relating to EEOC's information security program. Brown & Company also contracted with Digital Defense, Inc. (DDI), the premier provider of managed security risk assessment solutions , to conduct an internal vulnerability assessment and penetration testing to determine the exploitability of identified vulnerabilities.

6. Findings and Recommendations

The results of our independent evaluation identified areas in need of improvement to the EEOC information system security program. These nineteen (19) findings and recommendations are discussed below.

Finding 1	**EEOC risk management program was not fully developed to meet an organization-wide risk management program required by FISMA and by the NIST SP 800-37 Rev. 1.**

<u>Condition:</u>

EEOC OIT Risk Assessment Report, dated July 2014, does not address risk-related concerns from an organizational level and a mission-business process level that is required by NIST SP 800-37 Rev.1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. Specifically, EEOC OIT Risk Assessment Report does not address the major element of an organization-wide and mission risk assessment such as vulnerabilities in governance structures (including field offices; mission/business processes; enterprise architecture; information security architecture; facilities, equipment, system development life cycle processes; supply chain activities; and external service providers).

<u>Criteria:</u>

NIST SP 800-53, Rev. 4*, Security and Privacy Controls for Federal Information Systems and Organizations*, RA-1 “Risk Assessment” section states:

The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Documents risk assessment results in security plan; risk assessment report; organization-defined document;
c. Reviews risk assessment results frequently; and
d. Updates the risk assessment frequently or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

NIST SP 800-37 Rev.1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* states:

> Tier 1 addresses risk from an organizational perspective with the development of a comprehensive governance structure and organization-wide risk management strategy.
>
> Tier 2 addresses risk from a *mission* and *business process* perspective closely associated with enterprise architecture and core missions and business processes for the organization.
>
> Tier 3 addresses risk from an information system perspective and is guided by the risk decisions at Tiers 1 and 2.

Cause:

The NIST SP 800-37 requires risk assessments to be performed on three levels: organizational, mission/business and information system level. EEOC has made an effort by preparing an organization-wide risk assessment program to comply with the newly released NIST SP 800-37. EEOC's approach to meet the standard was to compile their system level risk assessments into a single report. Compiling the system level assessment reports only meets the Tier 3 requirement. In addition, the assessment lacked organizational risk governance structure that covers field offices.

Effect:

The lack of an organization-wide risk assessment program leaves the organization with the inability to identify, measure, and prioritize risk in order to take appropriate action to minimize losses.

EEOC cannot address risk from an organizational perspective without the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1.

Recommendation 1:

We recommend EEOC develop, document, and implement organizational level and mission-business process level risk assessment strategies that include a clear expression of the risk tolerance for the organization, including field offices; acceptable risk assessment methodologies; risk mitigation strategies; the organization's defined metrics for acceptable risk tolerance; and approaches for monitoring risk.

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

"OIT Response: Management concurs with the recommendation and will update policy to better document and implement risk assessment strategies, as outlined."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation will resolve the reported condition.

Finding 2 EEOC system level risk assessment reports were not updated therefore reports do not reflect the current status of the systems.

Condition:

In FY14, EEOC combined all system level risk assessments into one single report. However, the EEOC OIT Risk Assessment Report was not first updated, and therefore contains outdated information. For example, the EEOC HQ network configuration diagram (dated February 2, 2008) in the OIT Risk Assessment Report does not reflect the current infrastructure. In addition, the EEOC network configuration diagrams for field offices were not included in the report at all.

Criteria:

NIST SP 800-37 Rev.1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, states:

> Updates to the risk assessment reports help to ensure that the information system owners, common control providers, and authorizing officials maintain the appropriate awareness with regard to security control effectiveness. The overall effectiveness of security controls directly affects the ultimate security state of the information system and decisions regarding explicit acceptance of risk.

Cause:

EEOC has not updated its information security system level risk assessment reports. Therefore the reports do not reflect the near real-time risk conditions of its information systems.

Effect:

Without an updated system level risk assessment reports the organization loses the ability to manage and take appropriate action to minimize losses. For example, a loss of reputation and public image could increase legal liability and add additional cost for unforeseen circumstances.

Recommendation 2:

We recommend that EEOC OIT update its system level management report to ensure that risk for these systems are adequately assessed, evaluated, mitigated, accepted, and monitored. Knowing the real-time risk of these systems will help to reduce uncertainties, which in turn would improve the rate of success for carrying out the business mission of the organization.

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

"OIT Response: Management concurs that the system level risk assessment report, which was updated in FY 2014, contained some outdated diagrams and did not include network configuration diagrams for EEOC field offices. EEOC will ensure that all diagrams are updated during our FY 2015 update and review cycle."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation will resolve the reported condition.

Finding 3 EEOC has not thoroughly developed a Bring Your Own Device (BYOD) program that addresses OIT responsibility for operation, maintenance, and disposal of mobile devices.

Condition:

EEOC does not have a BYOD policy that addresses telework and remote access requirements defined in NIST SP 800-124 Rev. 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*. EEOC has a "Bring Your Own Device (BYOD) Policy and Rules for Behavior" for operating and carrying a mobile device containing EEOC data; however, the policy does not address the major elements of a BYOD program such as:

- Restrictions on Mobile Devices and Access Levels;
- Additional User Requirements;
- Development;
- Implementation;
- Operations and Maintenance; and
- Disposal.

Criteria:

NIST SP 800-124 Rev. 1, ***Guidelines for Managing the Security of Mobile Devices in the Enterprise*** states:

> A mobile device security policy should define which types of the organization's resources may be accessed via mobile devices, which types of mobile devices are permitted to access the organization's resources, the degree of access that various classes of mobile devices may have—for example, organization-issued devices versus personally-owned (bring your own device) devices—and how provisioning should be handled. It should also cover how the organization's centralized mobile device management servers are administered, how policies in those servers are updated, and all other requirements for mobile device management technologies. The mobile device security policy should be documented in the

system security plan. To the extent feasible and appropriate, the mobile device security policy should be consistent with and complement security policy for non-mobile systems.

Cause:

The "Bring Your Own Device (BYOD) Policy and Rules for Behavior" is not a comprehensive BYOD policy that addresses security for mobile devices as defined in NIST SP 800-124 Rev.1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise.*

Effect:

The lack of comprehensive mobile device security policy and procedures increases the risk of an unauthorized remote access to EEOC information and information systems. Mobile devices are at a higher risk of threat than other client devices. They are more likely to be lost or stolen, increasing the risk of data being compromised.

Recommendation 3:

We recommend that EEOC develop, document and implement a BYOD policy that addresses security for mobile devices as defined in NIST SP 800-124 Rev.1*, Guidelines for Managing the Security of Mobile Devices in the Enterprise,* to include:

- Restrictions on Mobile Devices and Access Levels;
- Additional User Requirements;
- Development;
- Implementation;
- Operations and Maintenance; and
- Disposal.

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

"OIT Response: Management concurs with the recommendation and will update BYOD policy to better document operation, maintenance, and disposal of mobile devices, as outlined."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation will resolve the reported condition, and address OIT responsibility for operation, maintenance, and disposal of mobile devices.

Finding 4 Visitors to the EEOC official website are not informed of the demarcation of privacy between EEOC and third-party websites. In addition, social media websites published by the agency lead visitors to other non-governmental websites without alerting. In addition, some EEOC social media websites are not branded.

Condition:

Visitors to the EEOC official website are not informed of the demarcation of privacy policies between the agency and third-party websites. EEOC has placed external links to third-party websites that do not display "popup" alert warnings that they are leaving EEOC's official website and stating that the agency's privacy policies are not inherited. In addition, social media websites published by the agency lead visitors to other non-governmental websites without alerting the visitor. The EEOC Privacy Policy posted on its official website does not include a complete list of social media websites published by the agency. One of the social media websites published by the agency does not include an official agency branding. Another social media website published by the agency allows external visitors to post content with links that lead to their social media page, thereby giving the impression of endorsement from the EEOC. On September 23, 2014, two law firms shared a "like posting" that automatically posted their company's links onto the EEOC's Official social media website.

Criteria:

OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications* states:

> If an agency posts a link that leads to a third-party website or any other location that is not part of an official government domain, the agency should provide an alert to the visitor, such as a statement adjacent to the link or a "pop-up," explaining that visitors are being directed to a non-government website that can have different privacy policies from those of the agency's official website." In addition, the guideline states that "the agency should apply appropriate branding to distinguish the agency's activities from those of non-government actors" by applying a seal or emblem to its profile page.

Cause:

EEOC has embedded pop-up alerts for links on its website to warn visitors that they are leaving EEOC's official website, and the privacy policies from EEOC's Official website will not be inherited. There was a technical coding error on the homepage of the EEOC official website that prevented the pop-up alert from appearing for social media links. The agency branded all social media websites except one.

Effect:

Improperly designed websites that do not protect visitors' privacy could unknowingly provide personal privacy information to third parties.

Recommendation 4:

We recommend that EEOC develop, document and implement procedures for reviewing and monitoring websites published by the agency to ensure compliancy with OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications* requirements. At the same time, EEOC should comply with the requirements in this Memorandum to ensure that privacy is fully protected.

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

"OCLA Response: The areas identified in the report concerning the pop up warnings, privacy policy and official agency branding issues have been resolved. The one area remaining is the action item section referencing the EEOC linking to third-party websites such as Twitter and Facebook. The EEOC has the proper notifications in place on our website. However, we are not aware of any way to comply in the case of links posted on our social media accounts. Third-party social media platforms don't give users the ability to provide pop-up notifications, and limits on the size of postings often makes adding a statement adjacent to the link impractical. This restriction also applies to the Twitter feed posted to the front of eeoc.gov. Additionally, it is not possible to prevent users from posting links to third-party sites on our social media accounts. We do however address the issue of posting of inappropriate links and endorsements in the comments policy statement. Finally, we have reached out through the Federal Web Content Manager's Forum to learn of best practices in this area and will continue to do so to determine an adequate solution."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation for providing an alert to the visitor, such as a statement adjacent to the link or a "pop-up," explaining that visitors are being directed to a non-government website that can have different privacy policies from those of the agency's official website.

Management's response to seek best practices to reduce the security risk associated with visitor's links posted on EEOC's social media accounts is appropriate. We recommend management monitors the posting of links to the EEOC social media accounts to ensure the links do not violate agency's security policies and procedures.

Finding 5 Weak virtual private network (VPN) configuration settings

Condition:

The VPN password configurations do not meet the EEOC's strong password policy (eight characters, one upper and lower case character). In addition, VPN configuration contains default settings that are not recommended by the vendor. For example, the VPN 3000 Concentrator Series Manger's configuration general parameters for minimum password length are set to five characters, and there is a default setting for alphabet only passwords to be used, which is not recommended by the vendor.

Criteria:

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, "IA-5 Authenticator Management" section states:

> The organization manages information system authenticators for users and devices by:
>
> a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
> b. Establishing initial authenticator content for authenticators defined by the organization;
> c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
> d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
> e. Changing default content of authenticators upon information system installation;
> f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
> g. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type];
> h. Protecting authenticator content from unauthorized disclosure and modification; and
> i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

EEOC *Office of Technology Password Policy* minimum password requirements:

- Password length is eight characters
- One uppercase character
- One lowercase character
- One numeric character

Cause:

EEOC does not have effective policies and procedures to ensure VPN configurations meet the agency's policy requirements and NIST authenticator management controls.

Effect:

Attackers attempt to determine weak passwords and to recover passwords using two types of techniques: guessing and cracking. Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, and easily discoverable. Therefore, they present a significant security risk and should be changed upon installation.

Recommendation 5:

We recommend that EEOC develop, document, and implement policies and procedures to ensure VPN configurations meet the agency's policy requirements and NIST authenticator management controls.

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

"OIT Response: Management concurs with the audit finding; however, EEOC's current VPN architecture does not technically allow automatic enforcement of password requirements at this level. OIT has identified a VPN management solution which is expected to overcome these limitations, at an expected cost of about $36,000. The limiting factor is lack of funds to acquire this VPN solution, or to substantially upgrade our enterprise authentication architecture (such as implementation of two-factor authentication). Depending on the amount of our final FY 2015 budget allocation (post Continuing Resolution), OIT will allocate FY2015 funds toward the VPN management upgrade, or will request the funding during mid-term and/or end-of-year budget calls.

As an interim compensation pending funding, OIT has promulgated a Strong Password Policy, and in particular has stressed that to VPN participants, who must individually apply for the VPN facility. In response to this finding, OIT will redouble its efforts to notify VPN users of the password requirements through specific modules of its annual Security Awareness Training, targeted security tips, and VPN application and operation instructions. EEOC accepts these policy and training actions as compensating controls."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation will help to ensure VPN configurations meet the agency's policy requirements and NIST authenticator management controls.

Finding 6 EEOC is not using encryption to protect digital backup media during transport or while it is waiting to be transported outside of controlled areas.

Condition:

Protection of digital backup media during transport or while waiting to be transported outside of controlled areas of the agency was not clearly defined. EEOC System Backup Procedure states that digital backup media is performed by writing the data to a removable drive and then sending the removable drive offsite to a third party vendor storage area without encryptions.

Criteria:

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, MP-5 "Media Transport" section states:

> The organization:
>
> a. Protects and controls information system media during transport outside of controlled areas using security safeguards;
> b. Maintains accountability for information system media during transport outside of controlled areas;
> c. Documents activities associated with the transport of information system media; and
> d. Restricts the activities associated with the transport of information system media to authorized personnel.

Section 4, "Media Transport / Cryptographic Protection," states:

> The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Cause:

EEOC catalogs backup media when it leaves the agency and is sent offsite to a third-party vendor's storage area. EEOC backup and offsite storage policy and procedures do not address how digital data is protected and controlled when it is transported or waiting to be transported to a third-party's secured area. In addition, the agency has not chosen cryptographic mechanisms to protect the confidentiality and integrity of digital backup data stored offsite.

Effect:

Transporting digital data that is not encrypted reduces the agency's ability to ensure only authorized individuals are able to access the media. In addition, the ability to track and/or obtain explicit records of transport activities as the media moves through the transportation system can be lost. The effects of not implementing cryptographic mechanism on digital backup media will compromise the confidentiality, integrity, and availability of agency data.

Recommendation 6:

We recommend that EEOC encrypt digital media during transport or while it is waiting to be transported according to NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organization,* MP-5 Media Transport requirement. Incorporate encryption mechanisms into the agency backup media system to provide confidentiality and integrity protections for media while in transit and storage.

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

"OIT Response: Management does not concur with the recommendation; but has implemented compensating controls. EEOC currently has a contract with Iron Mountain for the secure transportation and storage of backup media tapes offsite at Iron Mountain facilities. While the backup media awaits pickup, it is secured in controlled server room, accessible only by authorized personnel. It is then hand-transferred by EEOC staff to official Iron Mountain staff, not third-party delivery personnel, using sealed, steel, locked boxes. Validation codes are entered into Iron Mountain security devices by both the EEOC employee and the Iron Mountain employee for identity verification. Individual media are bar-coded and logged, and the bar-code is scanned by the Iron Mountain staff during both acceptance and return. The media is additionally validated against the media cycling schedule for returned media. The media that is transported via this method is limited to HQ Network server backups, so no sensitive PII is included on the data backups.

EEOC has accepted the risk of the method, which has been developed as a compensating control due to the unreliability of restoring from encrypted media using OIT devices, especially when attempting to restore on different equipment; minor bit errors, otherwise easily corrected or of minor impact, tend to make the entire encrypted backup unusable. An unusable backup in a disaster recovery situation, due to de-encryption issues, is an unacceptable risk."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. We recommend that management document the acceptance of this risk, and reassess the risk at least annually.

Finding 7 EEOC response time for security alert reviews is not clearly defined.

Condition:

EEOC does not define response time for security alert reviews within EEOC *Incident Response Plan* (IRP), dated December 2013. Instead, the IRP includes such statements as "if it is determined that a security breach occurred, it should be reported to the Information Security Officer in a timely fashion." Without a defined response time, the agency cannot determine if the response to and resolution of an incident was conducted in a timely manner in an effort to minimize further damage.

Criteria:

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, IR-6 "Incident Reporting" section states:

> The organization:
>
> a. Requires personnel to report suspected security incidents to the organizational incident response capability within defined time period; and
> b. Reports security incident information to authorities.

Cause:

There is no defined response time in place regarding intra-organization review of security alerts. Each alert generated by a security device should be reviewed within a defined amount of time and a determination made as to whether the security alert needs further investigation or should be escalated as a security event.

Effect:

The effect of not implementing a timely review of security alerts may allow threats to escalate and result in loss of or compromised of data. Without a defined and documented response time, alerts may be generated in real time, but sit in a queue for extended durations before being reviewed.

Recommendation 7:

We recommend that EEOC update its policies and procedures to define the response time to review security alerts; implement the capability and staffing to meet the response time; and generate associated metrics for review and approval by management.

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

"OIT Response: Management concurs with the recommendation and will update our Incident Response Plan to better document incident response requirements related to security alerts."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation will define response time for security alert reviews.

Finding 8	EEOC has not implemented a process for file integrity monitoring to detect unauthorized changes to software, firmware, and information systems and resources.

Condition:

EEOC has not implemented a process for file integrity monitoring to detect unauthorized changes to software, firmware, and information systems and resources.

Criteria:

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, SI-7 "Software, Firmware and Information Integrity" section states:

The organization:

a. Employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information.

Section-1, "Software, Firmware, and Information Integrity Checks," states:

a. The information system performs an integrity check of software, firmware, and information at startup; at transitional states or security-relevant events; frequently.
b. Supplemental Guidance: Security-relevant events include, for example, the identification of a new threat to which organizational information systems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include, for example, system startup, restart, shutdown, and abort.

Section – 7, "Software, Firmware, and Information Integrity / Integration of Detection and Response," states:

a. The organization incorporates the detection of unauthorized security-relevant changes to the information system level system into the organizational incident response capability.

Cause:

EEOC has implemented monitoring tools to detect malware and other threats; however, the process for file integrity monitoring has not been implemented.

Effect:

The effects of not implementing a process for file integrity monitoring can result in information systems and resources being compromised and the loss of confidentiality and integrity. Without a process for file integrity monitoring, the agency lacks documented steps in which to detect, track, monitor or correct unauthorized changes to configuration setting or unauthorized elevated access to information systems and information. In addition, the agency runs the risk of losing historical records to identify and discern adverse actions over an extended period of time and for possible legal action.

Recommendation 8:

We recommend that EEOC implement a file integrity monitoring process that identifies and detects unauthorized changes to software, firmware, and information to protect information systems and information against errors and malicious activity. The implementation should meet the NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, section SI-7 "Software, Firmware and Information Integrity requirements."

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

"OIT Response: Management concurs with the recommendation. With the deployment of Windows 7, EEOC will be implementing Novell Dynamic Local User (DLU) policies which administratively restrict grants of rights needed to change workstation configurations or install/remove software. EEOC will also use central software deployment tools to deploy software being issued to more than 25 individuals, to ensure consistent configuration and versioning. Beyond deployment, EEOC inventories workstations on an automated, scheduled basis and now has the ability to report on the workstation operating systems, software, and firmware."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation will resolve the condition and provide for file integrity monitoring to detect unauthorized changes to software, firmware, and information systems and resources.

Finding 9 Laptop computers issued to employees for Disaster Recovery (DR) are not checked to ensure that patches and updates are installed for operating system, antivirus software and other security applications.

Condition:

The agency has issued laptop computers to employees to use as alternate devices during and after a disaster. These laptops are not periodically checked, monitored and maintained to ensure that the latest patches and software updates have been applied. Agency policy does not require individuals to log into the network to update their DR computers. In addition, the monitoring and patching tool report showed that 32 laptops had not been scanned nor patched within the last 12 months.

Criteria:

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, MA-2 Controlled Maintenance section states:

> The organization:
>
> a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
> b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
> c. Requires personnel or roles explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
> d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
> e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
> f. Includes maintenance-related information in organizational maintenance records.

Cause:

EEOC utilizes a monitoring tool to patch, monitor and report on the software security conditions, such as operating security patches and application updates, for laptops issued by the agency to be used during and after a disaster. Once laptops are connected to the network, the devices are scanned and updated via the tool. Laptops that have missed scheduled reviews or have not received the latest application updates are not checked for potential security weaknesses.

Effect:

Laptop security specifications are in constant state of change due to new security patches and ongoing application updates for correcting software flaws, addressing security threats and improving functionality. If the agency does not review the status of ongoing maintenance of laptops, they cannot ensure that security controls that were put in place are still functioning properly.

Recommendation 9:

We recommend that EEOC check all laptops for unapplied patches and software updates, and enforces policies and procedures that support NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, section MA-2, "Controlled Maintenance" that require laptops to be checked frequently to ensure that security controls that were put in place are still functioning properly.

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

"OIT Response: Management concurs with the recommendation. With the deployment of Windows 7, EEOC will be de-provisioning the current Dell D620 "COOP" laptops (recovering the laptops from users for disk wipe and GSA excessing). Dell E6500 laptops are automatically updated when they connect to the EEOC network, and new ZENworks monitoring tools will allow EEOC to validate that patches are completed against the E6500 devices. EEOC will implement policies to require that workstations that do now show on the reports as being updated are brought into the office for connection to the network and update, as required."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation will resolve the condition and help ensure that patches and updates are installed on employee laptops for operating system, antivirus software and other security applications.

Finding 10	**Student interns were hired in 2014 without complete background checks being performed. One of the overseas students worked at the agency on an expired visa.**

Condition:

EEOC conducted a student intern program in FY14 that lasted less than 180 days. Background checks were not performed on these individuals, based on the agency's policy that requires background checks for individuals occupying the building after 180 days. It was later discovered that one of the individuals in the program was volunteering/working on an expired visa. The individual was expelled from the program and immediately escorted out of the building.

Criteria:

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, PS-3 "Personnel Screening" section states:

The organization:

a. Screens individuals prior to authorizing access to the information system; and
b. Rescreens individuals according to organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening.

Cause:

EEOC does not require background screenings on individuals volunteering/working at the agency for less than 180 days. EEOC relied on third parties to ensure that all individuals in the program had valid visas. However the agency did not validate the status of the visas with the outside third-party agency.

Effect:

If EEOC does not validate an individual's trustworthiness and gives them access to information systems and information, the agency is at risk for unforeseen threats, such as the individuals obtaining unauthorized access to agency information systems and information.

Recommendation 10:

We recommend that EEOC update its personnel policy and procedures requiring screening and background checks for all individuals having access to information systems and information, as defined by NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, PS-3 Personnel Screening. The agency should ensure all individuals are processed through the E-Verify program, and no exception exists for those who have previously been verified by a third-party.

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

"OCHCO Response: Management concurs with the recommendation and will develop, document, and implement a policy, as referenced in the findings based upon guidance in accordance with OPM regulatory guidelines:

a. *Executive Order (EO) 10450, Security Requirements for Government Employment, and related Office of Personnel Management (OPM) regulations, Title 5 Code of Federal Regulations (CFR) Part 731, provide that all Federal appointments are subject to investigation. The lowest level of investigation used in the Equal Employment Opportunity Commission (EEOC) is the National Agency Check with Written Inquiries (NACI), which includes a check of Federal Bureau of Investigation (FBI) fingerprint files, with written inquiries to former employers and supervisors, references, and schools attended by the person under investigation. OPM exempts certain positions, provided agencies conduct such checks they determine appropriate to ensure employment and retention is consistent with suitability/fitness requirements for federal employment.*
b. *According to 5 CFR 731.104, OPM does not require a background investigation for certain positions. However, federal agencies "must conduct such checks as it deems appropriate to ensure the suitability of the person." The checks required need not rise to the level required for an investigation of a covered position under 5 CFR 731. EEOC will administer such checks as appropriate to ensure that the employment or retention of such individuals in these positions is consistent with the efficiency and integrity of the agency. Included in the exempt category are student volunteers, interns, and affiliates (under the exempt category) who work for 6 months (180 days consecutive) or less, or who work for 180 days aggregate for a calendar year, or who work in either*

a single continuous appointment or series of appointments that do not exceed an aggregate of 180 days per calendar year.

c. *The Security Agreement Check (SAC) known as a fingerprint check will be required prior to entry on duty for all new personnel in the exempt category."*

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation will resolve the condition and require background screenings on all individuals volunteering/working at the agency for less than 180 days.

Finding 11 EEOC did not conduct security awareness training for at least 95% of all individuals that use information systems within the organization.

Condition:

EEOC did not conduct at least 95% Security Awareness Training for all information system users in the agency in FY14. Thirty-one EEOC offices did not conduct security awareness training for at least 95% of their information system users.

Security Awareness Training Summary - EEOC Field Offices
32.5% - Field Offices - Less than 95% of users received training

67.5% - Field Offices - 95% of users or more received training

Security Awareness Training - Summary EEOC HQ Offices
4.2 % -HQ Office - Less than 95% of users received training

95.8% - HQ Office - 95% of user or more received training

Criteria:

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, AT-2 "Security Awareness Training" section states:

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

a. As part of initial training for new users;
b. When required by information system changes; and
c. Frequently thereafter.

Cause:

OIT is not effectively coordinating with field offices to ensure full compliance to security awareness training; therefore, individuals are operating systems without initial/ongoing security awareness training.

Effect:

If individuals do not receive security awareness training, they may not be aware of information security risks associated with their activities, and their responsibilities in complying with agency policies and procedures designed to reduce these risks. Without proper training, personnel could make costly errors. For example, an individual could click on a phishing email that contains a malicious virus that could spread throughout the EEOC network.

Recommendation 11

We recommend that EEOC enforce its policies and procedures to ensure that all individuals receive security awareness training as defined by NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, section AT-2 Security Awareness. In addition, we recommend that the agency perform frequent reviews of its security awareness program to ensure that every individual has taken the required security awareness training. If any deficiencies are noticed, a communication notice should be sent immediately to the individual's direct report or sponsor.

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

"OIT Response: While EEOC achieved an overall compliance rate of 95% for Security Awareness Training (SAT), management concurs that 32% of field offices and 4% of Headquarters' offices did not achieve 95% compliance. EEOC will update policy and implement procedures to better enforce SAT compliance and communicate deficiencies to management, as required."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation will resolve the condition and help enforce the requirement that all individuals receive security awareness training.

Finding 12 EEOC does not have policies and procedures to properly manage HQ physical security access cards.

Condition:

EEOC has distributed physical security access cards (DATA Watch and SigNet) to offices within the EEOC HQ to manage and control. On February 1, 2013 the agency reported 81 DATA watch cards and 85 SigNet cards lost or stolen. The agency has disabled the cards since the report, but has not enforced the agency's policies and procedures to properly manage and account for the EEOC physical security access cards. Specifically, the agency does not maintain a current log for all physical access cards.

Criteria:

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, PE-1 Physical and Environmental Protection Policy and Procedures states:

> The organization develops, disseminates, and reviews/updates:
>
> a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
> b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

Cause:

EEOC issued data access cards to offices within the agency for limited use by new hires, employees needing access to certain controlled areas and visitors. However, logs were not maintained by the individual offices to account for distribution of the access cards.

Effect:

The lack of policies and procedures increase the risk of the agency losing accountability and control of physical access cards, and thereby allowing unauthorized individuals to gain access to controlled areas, such as executive offices.

Recommendation 12:

We recommend that EEOC develop, document, and implement policies and procedures for managing access cards that give individuals access to work areas within the agency. The policies and procedures should be in accordance with NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, PE-1 Physical and Environmental Protection Policy and Procedures.

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

"OCFO Response: EEOC concurs with the recommendation. Current draft plans include a 100% inventory in January 2015 of all DataWatch and SigNet (proximity) cards within the HQ Offices. Policy and procedures are being developed to return centralized control of these entry access cards to the EEOC HQ Security Specialists and Support Specialists, to include a complete numbered inventory log."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation will resolve the condition and help manage access cards that give individuals access to work areas within the agency.

Finding 13 EEOC does not employ full-device encryption or container encryption to protect the confidentiality and integrity of information on Agency laptops.

Condition:

EEOC does not employ full-device encryption or container encryption to protect the confidentiality and integrity of information on Agency laptop computers. EEOC's laptops are configured with folder level encryption to protect sensitive data. However, folder level encryption does not meet the NIST requirement for providing full-device encryption or container-based encryption for mobile devices.

Criteria:

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, AC-19 Access Control for Mobile Devices section states:

> The organization:
>
> a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
> b. Authorizes the connection of mobile devices to organizational information systems.
>
> **Section-5, "Access Control for Mobile Devices | Full Device / Container-based encryption," states:**
>
> > The organization employs full-device encryption; container encryption to protect the confidentiality and integrity of information on mobile devices.

NIST SP 800-53, Rev. 4, also defines a mobile device as a computing device that can be easily carried by a single individual, operable without physical connective and containing its own power source.

Cause:

EEOC has implemented folder level encryption for laptops that are removed from the agency's premises. This method of encryption meets the requirement for laptops that do not leave the agency's premises; however, it does not meet the encryption standards for mobile devices for use outside of EEOC offices.

Effect:

The main threat to mobile devices is the increased risk of unauthorized access to information if a device is lost or stolen. Folder level encryption is transparent, meaning that anyone with access to the file system can view the names and possibly other metadata for the encrypted files and folders, including files and folders within encrypted folders, if they are not protected through operating system (OS) access control features. For a computer that is not booted, all the information encrypted by full-device encryption is protected with pre-boot authentication.

Recommendation 13:

We recommend that full-device encryption be implemented for laptop computers that are removed from the agency's premises to avoid unauthorized access to information on a lost or stolen device and to meet the requirements defined by NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, section AC-19 "Access Control for Mobile Devices."

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

"*OIT Response: Management concurs with the recommendation as a best practice, but due to hardware limitations, will implement it in a two-step process. EEOC divides its local workstations into two partitions: a C:\ partition containing the operating system and applications, and a D:\ partition containing user files. Under Windows XP, now being superseded, EEOC uses Microsoft's Encrypted File System (EFS) to encrypt locally stored data within D:\MyFiles. Under Windows 7, EEOC will transition to Novell ZENworks Full Disk Encryption (container level encryption) for the entirety of the D:\ partition. All user preferences, temporary files, and data files not stored on the network will be stored on the D:\ partition. When EEOC workstations are replaced (FY 2016, pending availability of funds), encryption use will be expanded to include the operating system and application files as recommended by the findings.*"

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation will resolve the condition and help reduce the risk of unauthorized access to information on a lost or stolen device.

Finding 14 EEOC has not developed COOP Implementation Plans for its respective field offices.

Condition:

The EEOC has developed COOP Implementation Plans for its HQ office and Baltimore field office. In FY14, the agency stated a new initiative to develop COOP Implementation Plans for field offices. Initial drafts were prepared for 3 of its 53 field offices: St. Louis District Office, Miami District Office and Tampa Field Office. However the agency has not developed COOP Implementation Plans for all of its field offices.

Criteria:

EEOC Order 180.003, *Contingency of Operations*, Section 8 "Procedures," states:

> Headquarters Directors will develop an Office COOP Implementation Plan for their respective offices, including the policies and procedures which support the overall implementation of this Order. The Office COOP Implementation Plan will, at a minimum, identify all personnel and technical resources, systems and applications which are necessary to continue essential supporting tasks in a short term or sustained continuity of operations event. This includes developing and documenting manual systems that might be required to support mission essential functions MEFs while automated systems are being restored.

Cause:

EEOC COOP Implementation Plan focused mainly on providing system support for the HQ and Baltimore field office, without developing, documenting, and implementing COOP Implementation Plans for field offices.

Effect:

Without an agency-wide COOP Plan, EEOC cannot ensure that field offices are able to perform mission essential function across a wide range of potential emergencies including natural, man-made and technological disasters.

Recommendation 14:

We recommend that EEOC expand its existing COOP Implementation Plan to include field offices to meet the requirements of *EEOC Order 180.003, Contingency of Operations*, Section 8 Procedures, to include processes such as reviewing field plans annually and including field offices in annual contingency exercises.

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

"OCFO Response: EEOC accepts the recommendation. The EEOC Field Office COOP Plan Development Initiative began on July 3, 2014. A standardized blank COOP template was provided to each Field Office and their initial draft was due to EEOC HQ Security Specialists by November 14, 2014. The EEOC Security Specialists have been collaborating with each of their respective Field Office COOP Coordinators. To date all Field Offices have submitted their initial Field Office COOP Plans for technical review. Two (2) Field Offices, Nashville and Newark, are 100% complete. The remaining Field Offices are on track for completion by May 2015. Hard copies of the draft Field Office COOP Plans are available from the EEOC HQ Security Specialist team members."

Auditor’s Evaluation of Management’s Response:

Management’s response is appropriate to address the finding and recommendation. Effective implementation of the recommendation will require field offices to meet the requirements of *EEOC Order 180.003, Contingency of Operations*, Section 8 Procedures.

Finding 15 EEOC has not thoroughly developed a telecommuting policy that meets FISMA requirements.

Condition:

EEOC does not have a telecommuting policy that addresses telework and remote access requirements as defined in NIST SP 800-46 Rev. 1*, Guide to Enterprise Telework and Remote Access Security*. EEOC has an Employee/Supervisor Telework Agreement that address the employee’s responsibility for operating telework computers, but does not have a telework policy that addresses the major elements of an enterprise-wide telework and remote program such as:

- Permitted Forms of Remote Access
- Restrictions on Telework Client Devices and Remote Access Levels;
- Additional User Requirements;
- Development;
- Implementation;
- Operations and Maintenance; and
- Disposal.

Criteria:

NIST SP 800-46 Rev. 1, *Guide to Enterprise Telework and Remote Access Security,* Section 5. “Summary of Key Recommendations” section states:

> A telework security policy should define which forms of remote access the organization permits, which types of telework devices are permitted to use each form of remote access, the type of access each type of teleworker is granted, and how user account provisioning should be handled. It should also cover how the organization's remote access servers are administered and how policies in those servers are updated. The telework security policy should be documented in the system security plan.

Cause:

EEOC is applying the Employee/Supervisor Telework Agreement for operation, maintenance and disposal of government-issued computers used for telework. However, the Employee/Supervisor Telework Agreement is not a comprehensive telecommuting policy that addresses telework and remote access requirements defined in NIST SP 800-46 Rev. *1, Guide to Enterprise Telework and Remote Access Security*.

Effect:

The lack of comprehensive telecommuting of policies and procedures increase the risk of unauthorized remote access to EEOC information and information systems.

Recommendation 15:

We recommend that EEOC develop, document, and implement a comprehensive telecommuting policy that addresses telework and remote access requirements defined in NIST SP 800-46 Rev. 1, *Guide to Enterprise Telework and Remote Access Security* to include:

- Permitted Forms of Remote Access;
- Restrictions on Telework Client Devices and Remote Access Levels;
- Additional User Requirements;
- Development;
- Implementation
- Operations and Maintenance; and
- Disposal.

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

"OIT & OCHCO Response: Management concurs with the recommendation and will develop, document, and implement Telework Security Policy, as referenced in the finding."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation will resolve the condition and address telework and remote access requirements defined in NIST SP 800-46 Rev. 1, *Guide to Enterprise Telework and Remote Access Security.*

Finding 16 EEOC does not have policies and procedures for managing shared group accounts.

Condition:

EEOC has approved the use of shared group accounts for system administrators to install approved software and provide level-1 support. The use of the shared group account has expanded to include the following groups: HQ IT Specialist, Branch Manager, Field Office IT Specialist, Administrators. The agency does not have policies and procedures for managing the shared group account.

Criteria:

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, AC-2 "Account Management" section states:

The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions *information system account types*;
b. Assigns account managers for information system accounts;
c. Establishes conditions for group and role membership;
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals *personnel or roles* for requests to create information system accounts;
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with *procedures or conditions*;
g. Monitors the use of information system accounts;
h. Notifies account managers:
   1. When accounts are no longer required;
   2. When users are terminated or transferred; and
   3. When individual information system usage or need-to-know changes;
i. Authorizes access to the information system based on:
   1. A valid access authorization;
   2. Intended system usage; and
   3. Other attributes as required by the organization or associated missions/business functions;
j. Reviews accounts for compliance with account management requirements *frequently*; and
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Cause:

EEOC has accepted the risk of issuing shared group accounts to allow system administrators to install approved applications, administer local user accounts, and install printers and other peripheral devices. However, the agency has not developed policies and procedures to control the use of shared group accounts for information systems, to include controls such as establishing conditions for the group membership and defining a period when passwords expire. In addition, processes are not defined for creating, enabling, modifying, disabling and removing shared group accounts.

Effect:

If EEOC has not developed policies and procedures to manage shared group accounts, the agency's risk increases that allow unauthorized users will gain access to controlled information systems.

Recommendation 16:

We recommend that EEOC develop, document and implement policies and procedures that address the control of shared group accounts according to NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, section AC-2 Account Management.

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

"OIT Response: Management concurs with the audit findings. With the deployment of Windows 7, EEOC will be using Novell Dynamic Local User (DLU) policies to control the issuance of persistent local admin rights to IT support staff (over specific domains) and to individuals (for specific computers). That is, administrative privileges will be confined to specific offices or districts, will be assigned to a named individual, and will enforce password control. Admin rights granted outside the EEOC's control process will be automatically revoked.

An authorization form has been created for individual right grants which facilitates the annual audit of local admin rights. A comparable authorization form will be created for system administrators covering the information systems for which they have admin rights, to be approved by system owners. The ServiceNow management system will track these requests and from time to time (and as requested) will report on them.

In these ways, the use of the installer account will be drastically minimized, and retained primarily for selected HelpDesk staff to address devices which will not boot at all. EEOC will be implementing recurring 90 day password changes for these workstation level admin accounts (e.g., "installer" account). New passwords will be circulated on a need-to-know basis to IT support staff."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation will address the control of shared group accounts.

Finding 17 EEOC needs to improve account management procedures that include disabling inactive accounts as required.

Condition:

EEOC Account Management policy requires accounts that are inactive for 30 days to be are disabled. There were 35 active accounts in a general support system (email system) that users had not logged into 30 days or more. In addition, a system administrator in the one of the field offices created three accounts in a general support system with passwords expiration dates exceeding the 90-day account policy requirement. These accounts were created on September 10, 2014 with password expiration dates set for July 1, 2015.

Criteria:

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, AC-2 Account Management, Account Management | Disable Inactive Accounts section states:

The organization:

a. The information system automatically disables inactive accounts after a defined time period.

EEOC Account Management Procedures states:

- Inactive accounts, that have not logged in within 30 days are disabled.
- Ensure that upon a user's separation, system access is removed and system accounts are disabled and deleted timely.
- Ensure continuous, periodic review and monitoring of user access listings to identify inactive user accounts and formalize the authority of OIT to disable and delete network and e-mail accounts remotely when appropriate under these guidelines.

Cause:

The general support systems are not configured to disallow administrators to overrides policies.

Effect:

If EEOC does not implement a process to disable expired accounts in general support systems, they increase the risk of individuals gaining unauthorized access to information systems and information. Passwords that are given extensive expiration dates that exceed 90 days provide individuals malicious intent with more time to break the password.

Recommendation 17:

We recommend that controls are implemented into general support systems to avoid overriding policies for account management required by NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, AC-2 Account Management.

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

"OIT Response: Management concurs with recommendation and will update EEOC's Account Management Policy to enforce the use of Service Now for off-boarding users (both scheduled off-boarding and emergency terminations). As users are off-boarded via Service Now, tickets are automatically created and assigned to system administrators for disabling/deleting the various related accounts. Task completion is automatically tracked, with non-compliance with service level agreements reported daily to supervisors.

In addition, the EEOC currently monitors all user and production accounts, and reports on and automatically disables network accounts inactive for more than 30 days. These are then deleted as the reason for inactivity indicates. The exception to this rule is that certain few utility logins provided with servers or necessary for their configuration and maintenance are used only on a ninety-day maintenance cycle or less often, but are required for normal operation of the systems. These are tightly controlled and monitored."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation will resolve the condition and improve account management policies and procedures.

Finding 18 EEOC needs to control physical access to controlled and sensitive areas

Condition:

Access was given to the data center and technology storage room to an individual who was not part of the OIT group and did not have a business-need to enter these areas based on the individual's job responsibilities. EEOC policy states that all guests should be escorted into the LAN/DataCenter by an authorized proximity card holder who has been approved by the Chief Information Officer.

Criteria:

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, PE-3 "Physical Access Control" section states:

The organization:

a. Enforces physical access authorizations at entry/exit points to the facility where the information system resides by;
   1. Verifying individual access authorizations before granting access to the facility; and
   2. Controlling ingress/egress to the facility physical access control systems/devices; guards;

b. Maintains physical access audit logs for entry/exit points;
c. Provides security safeguards to control access to areas within the facility officially designated as publicly accessible;
d. Escorts visitors and monitors visitor activity circumstances requiring visitor escorts and monitoring;
e. Secures keys, combinations, and other physical access devices;
f. Inventories physical access devices every frequently; and
g. Changes combinations and keys frequently and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Cause:

Individuals other than approved OIT staff have access to sensitive OIT controlled areas (e.g. LAN/Data Center) room and OIT storage closets.

Effect:

If OIT does not have control over physical access to information systems, the systems are vulnerable to unauthorized individuals and the information vulnerable to being stolen, destroyed or compromised.

Recommendation 18:

We recommend that EEOC enforce its policies and procedures for access to controlled areas as defined NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, section PE-3 Physical Access Control**.** In addition, we recommend that the agency vet the business need or need-to-know for all individuals with access to controlled areas.

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

"OIT & OCFO Response: Management concurs with the recommendation and will review access procedures and authorizations and will better enforce existing policy."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation will permit greater control over physical access to information systems.

Finding 19 EEOC's 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 September 22, 2014 to September 23, 2014 by Digital Defense Inc. on Brown & Company's behalf. 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 testing results were presented to the OIT for review and analysis. The overall assessment of the network security posture of the systems identified was Fair (within a range of Critical, Poor, Fair, Satisfactory, Good, and Excellent). The assessment found occurrences of high, medium and low risk vulnerabilities. EEOC should analyze and resolve the high and medium risk vulnerabilities as a priority.

Criteria:

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, RA-5 Vulnerability Scanning section states:

The organization:

a. Scans for vulnerabilities in the information system and hosted applications frequently and/or randomly in accordance with procedures and when new vulnerabilities potentially affecting the system/applications are identified and reported;
b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures; and
    3. Measuring vulnerability impact;
c. Analyzes vulnerability scan reports and results from security control assessments;
d. Remediates legitimate vulnerabilities response times in accordance with an organizational assessment of risk; and
e. Shares information obtained from the vulnerability scanning process and security control assessments with personnel or roles to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Cause:

The results of the high vulnerabilities were the result of; (1) legacy information systems (i.e. Apache, SSL) that have are still in production and are end-of-life; (2) the use of default passwords; (3) easily guessable credentials; (4) bypassing authentications; (5) vendor software vulnerabilities; and (6) Vx remote debugging agent accessibility.

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 (2) an intruder would gain valuable information about the EEOC host which could aid in gaining access.
The effect of low-risk vulnerabilities, if maliciously exploited, is that an intruder could obtain information about an EEOC computer system that could aid them in compromising the system.

Recommendation 19:

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

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

"OIT Response: Management concurs with the audit findings. OIT has divided scans into two teams, one within the normal production groups using ZENworks, Trend Micro, and other network monitoring tools, and one team within the ISO group, using Nessus and other network monitoring tools. These will be supplemented through Task Order 2 of the CDM initiative of FNR.DHS, in which program this agency fully participates. The two scanning teams will meet regularly to exchange findings and best practices.

To ensure that findings of the scans are actually addressed promptly, notices of all scan results will be directed monthly to a specific division director for assignment and tracking of remediation through the Service Now tracking system. In addition, notices of critical vulnerabilities will be similarly directed on a weekly schedule. EEOC has also implemented an automated mechanism (in Nessus) through which administrators assigned to remediation are able to request and justify risk acceptance. These requests will be reviewed at least monthly.

OIT will also implement a 'dashboard' whereby agency management and DHS/OPM are directly able to view the risk status of the agency in real time."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation will reduce the vulnerability risks to EEOC's systems.