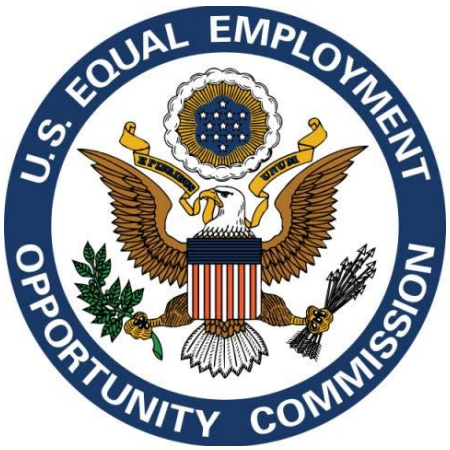
Independent Evaluation of the U.S. Equal Employment Opportunity Commission's Compliance with Provisions of the Federal Information Security Modernization Act of 2014 (FISMA)



For Fiscal Year 2016
Report Number 2016-08-EOIG

Prepared by:

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

Date: January 4, 2017

Proprietary and Confidential

BROWN & COMPANY

CERTIFIED PUBLIC ACCOUNTANTS AND MANAGEMENT CONSULTANTS, PLLC

Independent Auditor's Report on
External Penetration Test of
The U.S. Equal Employment Opportunity Commission's
Office of Inspector General Network Infrastructure

Fiscal Year 2016

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

Brown & Company CPAs and Management Consultants, PLLC (Brown & Company) is pleased to submit our report of evaluation services provided pursuant to requirements of the Federal Information Security Modernization Act of 2014 (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, 2016. Our independent evaluation covered the period October 1, 2015 through September 30, 2016.

We conducted the FISMA evaluation in accordance with U.S. generally accepted government auditing standards and in compliance with 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 obtained provides a reasonable basis for our findings and conclusions based on the evaluation objectives.

Largo, Maryland
January 4, 2017

1101 MERCANTILE LANE, SUITE 122 • LARGO, MD 20774
PHONE: (240) 770-4900 • FAX: (301) 773-2090 • mail@brownco-cpas.com • www.brownco-cpas.com

Independent Auditor's Report on
External Penetration Test of
The U.S. Equal Employment Opportunity Commission's
Office of Inspector General Network Infrastructure

Fiscal Year 2016

1. Executive Summary

For Fiscal Year (FY) 2016, the U.S. Equal Employment Opportunity Commission (EEOC), Office of Inspector General (OIG) contracted with Brown & Company CPAs and Management Consultants, PLLC (Brown & Company) to conduct an independent evaluation of EEOC's compliance with the provisions of the Federal Information Security Modernization Act of 2014 (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 our evaluation, Brown & Company concluded that the EEOC continues to make 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 eleven (11) FISMA findings and eleven (11) corresponding recommendations. The FY 2016 findings are as follows:

1. EEOC OIT does not perform SCAP scanning to assess both code-based and configuration-based vulnerabilities for systems on its network.
2. EEOC OIT has not implemented secure https connections for all of its public websites.
3. EEOC's network runs software applications that exceed end-of-life maintenance support.
4. The EEOC did not fully implement multifactor authentication for logical and remote access to EEOC systems for privileged and non-privileged users.
5. EEOC does not have automated mechanisms to support the management of information system accounts.
6. EEOC did not resolve vulnerabilities within the organizational timeframe (within 30 days) for resolving known vulnerabilities.
7. PIV cards are not required for physical access for all of EEOC's offices.
8. EEOC should prepare special security controls for its district, field and area offices to ensure that information systems and information located at these offices are protected.
9. EEOC has not developed an organization-wide risk management strategy and processes to manage risk to organizational operations and assets.
10. EEOC OIT continuous monitoring processes are not effective for identifying valid a FEPA contracts and IMS accounts issued to FEPA users.
11. EEOC does not monitor physical access to EEOC local field offices.

2. Background

The Federal Information Security Modernization Act of 2014 (FISMA)

On December 18, 2014, President Obama signed the Federal Information Security Modernization Act of 2014, a bill that reformed the Federal Information Security Management Act of 2002. The new law updates and modernizes FISMA to provide a leadership role for the Department of Homeland Security (DHS), and includes security incident reporting requirements, and other key changes. The amended FISMA places greater management and oversight attention on data breaches, evaluating the effectiveness of security controls and configurations, and security control monitoring processes and procedures. This update provides several modifications to FISMA that modernize Federal security practices to current security concerns. Specifically the new bill:

- Reasserts the authority of the Director of the Office of Management and Budget (OMB) with oversight, while authorizing the Secretary of DHS to administer the implementation of security policies and practices for Federal information systems.
- Gives the delegation of OMB's authorities to the Director of National Intelligence (DNI) for systems operated by an element of the intelligence community.
- Requires agencies to notify Congress of major security incidents within seven days.
- Places more responsibility on agencies looking at budgetary planning for security management, ensuring senior officials accomplish information security tasks, and that all personnel are responsible for complying with agency information security programs.
- Changes the reporting guidance to focus on threats, vulnerabilities, incidents, and the compliance status of systems at the time of major incidents, and data on incidents involving personally identifiable information (PII).
- Calls for the revision of OMB Circular A-130 to eliminate inefficient or wasteful reporting.
- Provides for the use of automated tools in agencies' information security programs, including periodic risk assessments, testing of security procedures, and detecting, reporting, and responding to security incidents.

Furthermore, the OIG must submit to the OMB the "Inspector General FISMA Reporting Metrics" that depicts the effectiveness of the agency's information security program.

The Organization

The 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. The OIT consists of three components: Immediate Office of the Chief Information Officer; Customer Services Management Division, Infrastructure Management and Operations Division; and Enterprise Applications Innovation Division. In 2016, EEOC hired Bryan Burnett, as Chief Information Officer (CIO), and Pierrette McIntire who was acting CIO resumed her role as Deputy CIO and Chief Information Security Officer (CISO).

3. Objective

The objective of this independent evaluation is to conduct a review of EEOC's information security program and practices as required by FISMA. The objective involved reviewing the effectiveness and efficiency of the agency's information security program. Our evaluation included the following information systems:

1. DataNet System (DNS)
2. Document Management System (DMS)
3. Integrated Mission System (IMS)
4. Federal Personnel Payroll System (FPPS)
5. DOI Interior Business Center, Oracle Federal Financials (OFF)
6. EEO-1 Survey System

4. Purpose and Scope

The purpose of the independent evaluation is to determine the effectiveness and efficiency of EEOC's information security program and whether it meets the requirements of FISMA. In assessing EEOC's adherence with FISMA, the following areas were reviewed:

- Risk Management
- Contractor Systems
- Configuration Management
- Identity and Access Management
- Security and Privacy Training
- Information Security Continuous Monitoring
- Incident Response
- Contingency Planning

The period covered by this independent evaluation is October 1, 2015 to September 30, 2016. The work was performed in accordance with U.S. generally accepted government auditing standards.

5. Testing Methodology

Brown & Company's testing methodology included: interviews with EEOC management and staff; review of legal and regulatory requirements; and review of documentation relating to EEOC's information security program. We utilized the Information Security Continuous Monitoring (ISCM) and Incident Response maturity model[1] to assess the maturity of the organization's ISCM program.

Brown & Company also contracted with Digital Defense, Inc. (DDI), a premier provider of managed security risk assessment solutions, to conduct the internal vulnerability assessment and penetration testing to determine the exploitability of identified vulnerabilities.

[1] FY 2016 *Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics (for Offices of the Inspectors General) V1.1.3*, dated September 26, 2016 includes the Maturity Models for Information Security Continuous Monitoring and Incident Response.
https://www.dhs.gov/sites/default/files/publications/FY%202016%20IG%20FISMA%20Metrics%20508%20compliant%20.pdf

6. Findings and Recommendations

The results of our independent evaluation identified areas in EEOC's information security program that need improvement. The eleven (11) findings and recommendations are discussed below.

Finding 1	**EEOC OIT does not perform SCAP scanning to assess both code-based and configuration-based vulnerabilities for systems on its network.**

Condition:

EEOC OIT does not perform Security Content Automation Protocol (SCAP) scanning to assess both code-based and configuration-based vulnerabilities for systems on its network. OIT scans with SCAP-enabled tools; however it does not currently employ any SCAP scanning capabilities.

Criteria:

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, SI-2 "Flaw Remediation," states:

Control: The organization:

a. Identifies, reports, and corrects information system flaws;
b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and
d. Incorporates flaw remediation into the organizational configuration management process.

OMB *Guidance on the Federal Desktop Core Configuration* (FDCC), M-08-22 memorandum, dated August 11, 2008, states:

> Both industry and government information technology providers must use SCAP validated tools with FDCC Scanner capability to certify their products operate correctly with FDCC configurations and do not alter FDCC settings.

Cause:

OIT uses DHS and Tenable Security Center tools to scan its external and internal networks for vulnerabilities. OIT scans with SCAP-enabled tools; however it does not currently employ any SCAP scanning capabilities. OIT expects this situation to change when the Department of Homeland Security (DHS) implements its Continuous Diagnostics and Mitigation (CDM) deliverables for TO-2F participants.[2]

Effect:

If EEOC/OIT does not perform SCAP scanning, information systems face the significant likelihood of being compromised.

Recommendation 1:

We recommend that EEOC OIT perform SCAP scanning to identify vulnerabilities in all systems on the network to assess both code-based and configuration-based vulnerabilities.

Management's Response:

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

> *OIT concurs with the finding and recommendation and plans to obtain assistance through the Department of Homeland Security in performing and assessing code-based and configuration-based vulnerability scans.*

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. SCAP scanning will reduce the likelihood of information systems being compromised.

Management's full response is provided in **Appendix A.**

[2] DHS Task Order for Continuous Diagnostics and Mitigation (CDM), Tools and Continuous Monitoring as a Service (CMaaS) for Group F Phases 1 and 2 Implementation, http://1yxsm73j7aop3quc9y5ifaw3.wpengine.netdna-cdn.com/wp-content/uploads/2015/12/CDM-task-order-2F.pdf

Finding 2	**EEOC OIT has not implemented secure https connections for all of its public websites.**

Condition:

EEOC OI) has not implemented secure https connections for all of its public websites. The OIT has implemented https connections for many of its public websites; however it has not implemented https for its [redacted]

Criteria:

OMB M-15-13: ***Policy to Require Secure Connections across Federal Websites and Web Services:***

> The Memorandum requires that all publicly accessible Federal websites and web services only provide service through a secure connection.

Cause:

The third-party contractor that developed EEOC's training website did not implement https secure connections to protect data traveling between the web browser and the server.

Effect:

The unencrypted http protocol does not protect data from interception or alteration, which can subject users to eavesdropping, tracking, and modification of received data.

Recommendation 2:

We recommend OIT ensure all publicly-accessible systems are HTTPS compliant.

Management's Response:

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

> *OIT concurs with the finding and recommendation and is working to obtain HTTPS compliance with the one remaining non-compliant site.*

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation and will make all public facing websites HTTPS compliant.

Management's full response is provided in **Appendix A.**

Finding 3	**EEOC's network runs software applications that exceed end-of-life maintenance support.**

Condition:

EEOC's network runs software applications that exceed end-of-life maintenance support. EEOC hosts a number of applications through its Salient/Enterprise Hosting Managed Cloud Services (EHMCS) shared resources. [redacted]

[3] MS Windows Server 2003 R2 Standard vendor support, https://support.microsoft.com/en-us/lifecycle/search?sort=PN&alpha=Microsoft%20Windows%20Server%202003%20R2&Filter=FilterNO

[4] Oracle Lifetime Support Policy, http://www.oracle.com/us/support/library/lifetime-support-technology-069183.pdf

[5] Microsoft SQL Server 2005 Standard Edition. https://support.microsoft.com/en-us/lifecycle/search?sort=PN&alpha=sql&forceorigin=esmc

Criteria:

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, SA-22 "Unsupported System Components," states:

> Control: The organization:
>
> a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and
>
> b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

Cause:

EEOC OIT has delayed application updates because of non-compatibility with legacy systems (i.e., DMS) and testing environments were not available to test the software updates. OIT has identified network vulnerabilities in its Plan of Action and Milestones with targeted dates for remediation.

Effect:

Continuing to use unsupported software beyond the end-of-support dates present security and business risks to EEOC. Any newly found vulnerabilities for unsupported software places EEOC at risk for cyber-attacks.

Recommendation 3:

We recommend that EEOC OIT update or replace software that is no longer supported by vendors and manufacturers.

Management's Response:

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

> *OIT concurs with the finding and recommendation and is moving toward subscription-based cloud platforms and applications, which will help ensure EEOC software is current.*

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Current version of supported software applications help reduce risk of cyber attack.

Management's full response is provided in **Appendix A.**

Finding 4	The EEOC did not fully implement multifactor authentication for logical and remote access to EEOC systems for privileged and non-privileged users.

Condition:

The OIT did not fully implement multifactor authentication for logical and remote access to EEOC systems for privileged and non-privileged users.

EEOC OIT requires only a user ID and password to access EEOC information systems and does not require the use of an authentication device, such as a token or Homeland Security Presidential Directive 12 (HSPD-12) Personal Identity Verification (PIV) card for remote or network (logical) authentication.

Criteria:

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, IA-2 "Identification and Authentication" (Organizational Users), states:

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

> Identification and Authentication/Acceptance of PIV Credentials
> The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.
>
> Supplemental Guidance: This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials."

OMB M-07-16: *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, states:

> Control Remote Access. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;

Cause:

The legacy Novell system does not support multifactor authentication. EEOC OIT is in the process of transitioning from the Novell system to Microsoft network technology and use of Active Directory, which will be configured to support PIV use for all standard functions.

Effect:

Lack of a fully implemented multifactor authentication process increases the risk of unauthorized access.

Recommendation 4:

We recommend EEOC Office of Information Technology implement multifactor authentication for logical and remote access for system users. Furthermore, we recommend EEOC use multifactor authentication where one of the factors is provided by a device separate from the computer gaining access.

Management's Response:

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

> *OIT concurs with the finding and recommendation and is migrating to Active Directory and configuring its identity service to support two-factor authentication using Personal Identification Verification (PIV) cards.*

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Implementing multifactor authentication will reduce the risk of unauthorized access.

Management's full response is provided in **Appendix A.**

Finding 5:	**EEOC does not have automated mechanisms to support the management of information system accounts.**

Condition:

EEOC OIT does not have automated mechanisms to support the management of information system accounts. OIT's Account Management Policy defines how accounts are identified, authorized and assigned to users. Office Directors are responsible for authorizing account creation and determining the appropriate level of system access for each user. User accounts are

monitored for inactivity and are integrated with the on-boarding and off-boarding processes. OIT conducts manual account reviews; monthly network account review; quarterly review of separated employees and annual account certification.

Criteria:

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, AC-2(1) "Account Management - Automated System Account Management," states:

> Control: Determine if the organization employs automated mechanisms to support the management of information system accounts.

AC-2(4) "Account Management-Automated Audit Actions," states:

> Control: The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].

Cause:

The legacy Novell system does not support account management. The OIT plans to implement an access and authorization management under TO-2F of the Department of Homeland Security Continuous Diagnostics and Mitigation (CDM) program.

Effect:

The implementation of automated mechanics to manage information system accounts will improve OIT's ability to proactively detect unauthorized or malicious modifications of accounts.

Recommendation 5:

We recommend OIT implement an automated mechanics to manage information system accounts.

Management's Response:

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

> *OIT concurs with the finding and recommendation and is proactively improving and automating account access and authorization management*

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Automated mechanics to manage information system accounts will improve OIT's ability to proactively detect unauthorized or malicious modifications of accounts.

Management's full response is provided in **Appendix A.**

Finding 6:	**EEOC did not resolve vulnerabilities within the organizational timeframe (within 30 days) for resolving known vulnerabilities.**

Condition:

EEOC OIT did not resolve vulnerabilities within the organizational defined timeframe for resolving known vulnerabilities; which is 30 days. [redacted]

List of Critical Vulnerabilities

Plugin Name	Description
[redacted]	[redacted]

Criteria:

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, SI-2 "Flaw Remediation," states:

Control: The organization:

a. Identifies, reports, and corrects information system flaws;
b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and
d. Incorporates flaw remediation into the organizational configuration management process.

Cause:

Software patches were delayed because of non-compatibility with legacy systems (i.e., DMS file server) and testing environments were not available to test the software updates.

Effect:

The effects of critical and high 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 that 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 6:

We recommend EEOC OIT review and analyze critical, high, and medium vulnerabilities. These vulnerabilities should be resolved to avoid compromise of 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 concurs with the finding and recommendation and will be retiring legacy applications over the next two fiscal years. In the interim, compensating controls will be put in place to mitigate and reduce related risk.*

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Maintaining current versions of supported software applications help reduce risk of cyber attack.

Management's full response is provided in **Appendix A.**

Finding 7:	**PIV cards are not required for physical access for all of EEOC's controlled space.**

Condition:

PIV cards are not required for physical access for all of EEOC's controlled space. During our review of physical access controls at the EEOC's field offices (Charlotte, Baltimore, Detroit and Milwaukee), we observed EEOC personnel entering and exiting EEOC controlled space (i.e., offices, in-take room and waiting areas) without being required to scan their EEOC PIV cards. Employees used other security controls such as keys and cypher locks at these locations. At federally- controlled buildings, individuals are screened for facility entrance; however PIV cards are not used to enter the building or EEOC's controlled space. At the commercial buildings, PIV cards are not required for facility entrance or access to EEOC's controlled space.

The EEOC HQ and Washington Field offices utilize PIV cards to enter the facility and EEOC controlled space. However, EEOC has not fully implemented PIV card controlled access for 52 field offices that are located in other federally-controlled and commercial buildings.

Criteria:

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, PE-2 "Physical Access Authorizations," states:

Control: The organization:

a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;

b. Issues authorization credentials for facility access;

c. Reviews the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and

d. Removes individuals from the facility access list when access is no longer required.

AC-2 "Identification and Authentication" (Organizational Users), states:

> Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).
>
> Identification and Authentication/Acceptance of PIV Credentials.
>
> The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.
>
> Supplemental Guidance: This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials."

Cause:

EEOC relies on the federal government or leaser to provide and monitor physical security at 52 EEOC field offices.

Effect:

Lack of a fully implemented PIV card access program increases the risk of unauthorized access to EEOC facilities, office and information systems.

Recommendation 7:

We recommend EEOC Office of the Chief Financial Officer (CFO) implement PIV card readers for physical access for all EEOC's controlled space.

Management's Response:

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

> *Management concurs with the finding and recommendation and is actively pursuing opportunities to implement with field office relocation/renovation efforts.*

Auditor's Evaluation of Management's Response:

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

Management's full response is provided in **Appendix A.**

Finding 8:	EEOC should prepare special security controls for its district, field and area offices to ensure that information systems and information located at these offices are protected.

Condition:

EEOC should prepare special security controls for its district, field and area offices to ensure that information systems and information located at these offices are protected.

Information security policies and procedures at the district, field and area offices are inherited from the EEOC OIT headquarters. In addition, security controls assessments of its district, field, and offices have not been performed to ensure that security controls that were put in place are operating as designed.

Based on our review of information system security controls at four offices—Charlotte District Office, Detroit Field Office, Milwaukee Area Office and Baltimore Field Office—the following security controls can be improved:

- Data protection and access control. Security procedures can be improved by removing unsecured recycle bins and securing case files at the end of the day.
- Data protection. Security procedures can be improved by ensuring personally identifiable information (PII), sensitive and classified data is not stored on unsecured USB thumb drives.
- Confidentiality. Security procedures can be improved by reviewing access accounts for Fair Employment Practices Agencies (FEPA) users more frequently than annually and by ensuring the FEPA users can only access information on a need to know basis.
- Physical security. Security procedures can be improved by surveying field offices to ensure the network equipment is not stored/secured in employee offices.
- Physical security. Security procedures can be improved by maintaining temperature and humidity levels within the facility where the information system resides and to avoid IT staff from keeping doors ajar for ventilation.
- Physical security. Security procedures can be improved by implementing a surveillance system to monitor or document unauthorized access after business hours and locking offices (i.e., intake interview offices) that are accessible to the public.
- Segregation of duties. Security procedures can be improved by ensuring that Directors do not receive a copy of users' temporary login credentials.
- Segregation of duties. Security procedures can be improved by ensuring that IT Specialists (ITS) or other employees do not have the responsibility of both receiving and storing equipment.

- Unsupported software. Security procedures can be improved by ensuring that backup images provided to field offices contain the latest software versions and vendor supported software.
- Network monitoring. Baltimore, MD Field Office: we noted the following exceptions to the network security monitoring controls: no network monitoring and no network sensor recording or analysis is being conducted. The Baltimore Field Office could better protect its network by installing monitoring devices on the network and installing security controls on network ports. Furthermore, the Baltimore Field Office needs to develop and implement monitoring procedures or train Field Office personnel to follow EEOC's OIT Headquarters' monitoring procedures.
- Physical security. Baltimore Field Office: the Field Office is located in a multi-tenant, privately-managed building. We noted the following exceptions to the Baltimore, MD Field office's physical security controls for its server room:
  - no environmental sensor or surveillance controls;
  - no sign-in sheet to track visitors; and
  - insufficient temperature and humidity controls to keep the servers and other computer equipment from overheating.

Criteria:

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, PL-1 "Security Planning Policy and Procedures," states:

Control: The organization:

a. Develops, documents, and disseminates to *organization-defined personnel or roles*:
   1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and

b. Reviews and updates the current:
   1. Security planning policy; and
   2. Security planning procedures.

Cause:

EEOC does not have policies and procedures specific to the district, field and area offices. In addition, the EEOC OIT does not perform frequent security control reviews or assessments of its district, field and area offices to uncover weaknesses.

Effect:

The lack of security controls, policies and procedures, reviews and assessments increases the risk of organization-wide security vulnerabilities.

Recommendation 8:

We recommend that the EEOC develop specialized security training and survey field offices to ensure security control align with the Federal Managers' Financial Integrity Act. In addition, we recommend the following improvements:

1. Assess the information systems security controls at the district, field and area offices;
2. Data protection and access control – Implement access controls to disallow unsecured recycle bins, secure case files, and require login credentials for devices that store and receive sensitive information (i.e., network printers and faxes);
3. Network monitoring – Implement policies and procedures to prevent PII and sensitive data from being stored on unsecured USB thumb drives;
4. Physical security – Survey network equipment for secured locations and ensure network equipment is installed in secured areas with controlled access;
5. Physical Security – Lock in-take offices containing computer equipment that are accessible to the general public;
6. Segregation of duties – Implement policies and procedure to ensure Director do not receive users' temporary login credentials;
7. Segregation of duties – Implement policies and procedure to ensure IT Specialists do not have rights to both receive and store equipment when off-boarding employees/contractors;
8. Segregation of duties – Review IMS role-based access to ensure users cannot access unauthorized data;
9. Information System Backup – Provide the field offices with updated PC backup images that contain the latest software versions and patches;
10. Enterprise Risk Management – Provide district, area and field offices with routine status reports on its IT security controls;

11. Network monitoring – Implement policies and procedure to ensure that ITS has adequate skillsets and training to monitor information systems. In addition, provide annual network training; and
12. Confidentiality – Implement policies and procedure to ensure that the ITS maintain confidentiality of sensitive data.

Management's Response:

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

> *OIT concurs with the finding and recommendation and will work with field offices to conduct specialized training and update policies and procedures. That and migrating data to secure cloud services will protect data and reduce organization-wide security vulnerabilities.*

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Specialized security training of personnel and secure cloud services to host data will reduce organization-wide security vulnerabilities.

Management's full response is provided in **Appendix A.**

Finding 9:	**EEOC has not developed an organization-wide risk management strategy and processes to manage risk to organizational operations and assets.**

Condition:

EEOC conducted risk assessments against the major applications and common controls. However, through inquiry of personnel, inspection of documentation, and observation of operational and process walkthroughs, we determined that EEOC has not developed an organization-wide risk management strategy and processes to manage risk to organizational operations and assets.

An organization-wide risk management strategy provides objectives and action statements to:

- Analyze individual risk management plans and assessment results for FISMA reportable systems (general support systems, major and minor applications);
- Determine potential adverse impact on the organization, mission/business processes, and information system level components; and
- Develop and implement an organization-wide risk management process for responding to, mitigating, and monitoring organization-wide risks.

Risk assessment is a key component of a holistic, organization-wide *risk management process* as defined in NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*. Risk management processes include: (i) framing risk; (ii) assessing risk; (iii) responding to risk; and (iv) monitoring risk.

Criteria:

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, PM-9 "Risk Management Strategy," states:

Control: The organization:

a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems;
b. Implements the risk management strategy consistently across the organization; and
c. Reviews and updates the risk management strategy at least annually or as required, to address organizational changes.

Supplemental Guidance: An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. The organization-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad-based and comprehensive.

Cause:

EEOC's risk assessments did not include conducting and completing an agency-wide risk assessment (at the Tier 1 Organization level), in accordance with NIST SP-800-30, *Guide for Conducting Risk Assessment*, Revision 1, Section 2.4 "Application of Risk Assessments."

The EEOC-wide risk management process was not documented in accordance with OMB Circular A-123, *"Management's Responsibility for Enterprise risk Management and Internal Control."*

Effect:

Without designing and implementing an enterprise-wide risk management strategy and processes, responsible personnel may not be kept abreast adequately of enterprise-wide and general support system application-specific threats, vulnerabilities, and attack vectors.

Recommendation 9:

We recommend EEOC develop an organization-wide risk management strategy and processes to manage risk to organizational operations and assets, in accordance with NIST guidelines.

Management's Response:

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

> *OIT concurs with the finding and recommendation and has drafted Enterprise Risk Management Policies and Plans that are being reviewed and scheduled to be finalized in fiscal year 2017.*

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. An organization-wide risk management strategy and processes to manage risk to organizational operations and assets in accordance with NIST guidelines will help keep responsible personnel abreast of enterprise-wide and general support system application-specific threats, vulnerabilities, and attack vectors.

Management's full response is provided in **Appendix A.**

Finding 10: EEOC OIT continuous monitoring processes are not effective for identifying valid FEPA contracts and IMS accounts issued to FEPA users.

Condition:

EEOC OIT continuous monitoring processes are not effective for identifying valid Fair Employment Practices Agencies (FEPA) contracts and IMS accounts issued to FEPA users. OIT should monitor FEPA agreements and user account access more frequently than annually to ensure FEPA contracts and user accounts are valid.

The EEOC contracts with various FEPA agencies nationwide for processing charges of employment discrimination within their geographic boundaries. FEPA Directors are responsible for authorizing IMS or successor system account creation and determining the appropriate level

of system access to provide each user. FEPA Directors are responsible for ensuring accounts are removed and system accounts are disabled upon a user's separation. Inactive IMS accounts (accounts that have not been logged into within 30 days) are disabled by EEOC. On an annual basis, EEOC forwards a list of active IMS accounts to FEPA Directors for their review and certification. FEPA Directors review each account to ensure that all individuals have the need and the proper level of access.

The EEOC annual certification process identified FEPA users that had an IMS account, but the specific FEPA agencies no longer had a valid contract with EEOC.

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:

OIT lacks policies and procedures to perform frequent reviews of FEPA user IMS accounts to ensure that the specific FEPA contract and user account is still valid.

Effect:

If EEOC does not implement a process to validate FEPA contracts and user accounts more frequently than annually, EEOC increases the risk of individuals gaining unauthorized access to information systems and information.

Recommendation 10:

We recommend that OIT chief information security officer develop, document, and implement a policy requiring OIT to review access logs quarterly to ensure that no one at the FEPA can contact OIT to inappropriately re-activate an account.

Management's Response:

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

> *OIT concurs with the finding and recommendation. The Agency proposes to implement an alternate solution for mitigation of the identified risk.*

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Implementation of effective continuous monitoring processes, policies and procedures will help reduce the risk of individuals gaining unauthorized access to information systems and information.

Management's full response is provided in **Appendix A.**

Finding 11: EEOC does not monitor physical access to EEOC local field offices.

Condition:

EEOC local field offices do not have surveillance cameras or proximate card readers to monitor physical access to federally-controlled facilities or offices. During our review of physical access controls at local EEOC field offices, we noted that the EEOC field offices are secured with locks and keys but do not have an automated system to identify and monitor who entered the facility. We also noted that the EEOC field offices did not have a mechanism to detect physical security incidents or monitor physical access intrusion alarms/surveillance.

Criteria:

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, PE-6 "Monitoring Physical Access," states:

Control: The organization:

a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
b. Reviews physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and
c. Coordinates results of reviews and investigations with the organizational incident response capability.

Control Enhancement: **PE-6(1) "Monitoring Physical Access Intrusion Alarm/Surveillance," states:**

The organization monitors physical intrusion alarms and surveillance equipment.

NIST Special Publication 800-116, Revision 1, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), Section 7.7* "PIV-in PACS Best Practices," states:

7.7 PIV-in-PACS Best Practices

[HSPD-12] mandates the establishment of government-wide identity credentials and the use of these credentials in gaining physical access to federally controlled facilities. This implies that a PACS application installed at these facilities should interoperate with the credential standardized by [FIPS201], the PIV Card, issued by any government agency. The PIV Card interface and data model requirements are fully specified through [FIPS201] and companion documents. For the PACS application (or PIV-enabled PACS application), the following best practices are recommended.

PACS application providers to employ products that are approved through the for relevant product categories.

For each access transaction, once the applicable authentication mechanisms are satisfied, all PACS access decisions are based on the utilization of an acceptable PIV identifier.

Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

http://www.dhs.gov/homeland-security-presidential-directive-12

HSPD-12 was issued on August 12, 2004 and calls for a mandatory, government-wide standard for secure and reliable ID for all of its employees and employees of federal contractors to access federally-controlled facilities and networks. Based upon this directive, the National Institute for Standards and Technology (NIST) developed Federal Information Processing Standards Publication (FIPS Pub) 201.

HSPD-12 established that all departments and agencies shall require the use of the PIV card (such as a proximity card) to gain access to federally controlled facilities. HSPD-12 provides for a new standardized federal identity credential that is designed to enhance security, reduce identity fraud, and protect the personal privacy of those issued government identification.

Cause:

EEOC Chief Financial Officer (CFO) lacks procedures that require EEOC field offices (other than the Washington Field Office) to have an automated surveillance and monitoring system. EEOC relies on the building facility manager to provide the physical security monitoring systems at the local EEOC field offices.

Effect:

The lack of physical surveillance and an automated monitoring system increases the risk of intruders entering the EEOC field office without being detected. In addition, EEOC does not have the ability to monitor and log suspicious activity—f or example, employees entering offices during non-work hours; non-EEOC employees attempting to access Agency spaces during non-work hours; repeated accesses to areas not normally accessed; access to controlled areas for an unusual length of time; and out-of-sequence access (i.e., there was an exit without an entry).

Recommendation 11:

We recommend EEOC CFO develop and implement policy and procedures to install surveillance technology and proximity card readers at EEOC local field offices to monitor and control physical access to EEOC controlled exterior entrances.

Management's Response:

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

> *Management concurs with comment(s) and is in the process of installing security cameras and Intrusion Detection Systems (IDS) in field offices.*

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Better physical surveillance and automated monitoring systems help reduce the risk of intruders entering EEOC the field offices without being detected.

Management's full response is provided in **Appendix A.**

Appendix A – Management's Response

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION
Washington, D.C. 20507

December 21, 2016

MEMORANDUM

TO: Milton Mayo, Inspector General

FROM: Pierrette McIntire, Chief Information Security Officer

SUBJECT: Office of Information Technology's (OIT) Response to the Draft Independent Evaluation of EEOC's Compliance with the Federal Information Security Modernization Act of 2014 (FISMA)

Below are OIT's responses to the draft findings and recommendations outlined in the above referenced evaluation. Please feel free to contact me at pierrette.mcintire@eeoc.gov or 202.663.4423 if you have any questions related to our responses.

FINDING/RECOMMENDATIONS:

1. **EEOC OIT does not perform SCAP scanning to assess both code-based and configuration-based vulnerabilities for systems on its network. We recommend that EEOC OIT perform SCAP scanning to identify vulnerabilities in all systems on the network to assess both code-based and configuration-based vulnerabilities.**

OIT concurs with the finding and recommendation. During fiscal year 2017, EEOC will obtain additional SCAP scanning and technical assistance through the Department of Homeland Security (DHS) Continuous Diagnostic and Mitigation (CDM) Program, Task Order 2F. These new tools and access to related expertise will assist OIT in performing and assessing code-based and configuration-based vulnerability scans.

2. **EEOC OIT has not implemented secure https connections for all of its public websites. We recommend OIT ensure all publicly-accessible systems are HTTPS compliant.**

OIT concurs with the finding and recommendation. OIT is working with the Revolving Fund training system vendor who supports the one remaining non-compliant site to obtain compliance.

3. **EEOC's network runs software applications that exceed end-of-life maintenance support. We recommend that EEOC OIT update or replace software that is no longer supported by vendors and manufacturers.**

OIT concurs with the finding and recommendation. In general, the move to subscription-based cloud platforms and applications will ensure that the Agency's software is current. Specifically:

Office of Information Technology
Phone (202) 663-4447 | FAX (202) 663-4451 | TTY (202) 663-7193 | Help Desk (202) 663-4767

- OIT currently is working to replace the Agency's legacy scanning service with a new cloud-based enterprise scanning solution.
- EEOC's Open Text Document Management System (DMS) will be retired as the Agency completes its migration to Alfresco for mission-system support and utilizes its Office 365 SharePoint subscription for other document management needs.
- The Common Spot content management software powering both inSite and www.eeoc.gov will be replaced by SharePoint and a to-be-determined solution, respectively and depending on the availability of funds.

In the interim, the Agency has implemented compensating controls to mitigate risks associated with these legacy applications.

4. **The EEOC did not fully implement multifactor authentication for logical and remote access to EEOC systems for privileged and non-privileged users. We recommend EEOC Office of Information Technology implement multifactor authentication for logical and remote access for system users. Furthermore, we recommend EEOC use multifactor authentication where one of the factors is provided by a device separate from the computer gaining access.**

OIT concurs with the finding and recommendation. EEOC presently is migrating to Active Directory, and its identity service is being configured to support two-factor authentication using Agency Personal Identification Verification (PIV) cards. OIT is partnering with GSA, the Office of Chief Financial Officer (OCFO), and the Office of Field Programs (OFP) on this effort, with kick-off meetings and initial planning completed during fiscal year 2016. The initial fiscal year 2017 focus for PIV authentication will be for privileged users and remote logical access. EEOC expects full PIV two-factor authentication for non-privileged users during fiscal year 2018.

5. **EEOC does not have automated mechanisms to support the management of information system accounts. We recommend OIT implement an automated mechanics to manage information system accounts**.

OIT concurs with the finding and recommendation. EEOC's legacy Novell directory services does not support automated account management. During fiscal year 2017, EEOC is implementing Active Directory, Exchange, and Office 365 which will support automated account management. In addition, EEOC's participation in the DHS CDM Program, Task Order 2F, will include fiscal year 2017 implementation of new tools and services that will also proactively improve and automate access and authorization management.

6. **EEOC did not resolve vulnerabilities within the organizational timeframe (within 30 days) for resolving known vulnerabilities. We recommend EEOC OIT review and analyze critical, high, and medium vulnerabilities. These vulnerabilities should be resolved to avoid compromise of EEOC's systems; or the agency should document acceptance of the risk or reclassification of the risk.**

All of the vulnerabilities identified in finding #6 relate to the legacy applications and "end-of-life" software issues identified in finding #3; therefore, OIT recommends that finding #6 be

merged into finding #3. As outlined in response to finding #3, EEOC will be retiring these legacy applications during fiscal years 2017 and 2018. In the interim, compensating controls are in place to mitigate and reduce related risk.

7. **PIV cards are not required for physical access for all of EEOC's offices. We recommend EEOC Office of the Chief Financial Officer (CFO) implement PIV card readers for physical access for all EEOC's controlled space.**

OCFO will respond to this finding and recommendation.

8. **EEOC should prepare special security controls for its district, field and area offices to ensure that information systems and information located at these offices are protected. We recommend that the EEOC develop specialized security training and survey field offices to ensure security control aligns with the Federal Management Financial Integrity Act.**

OIT concurs with the finding and recommendation. OIT will work with OCFO to survey field offices, conduct specialized security training as outlined in the recommendation, and update policies and procedures where needed. Additionally, the Agency's information technology plans include migrating data from Field Offices to secure cloud services, such as with the current GroupWise email migration.

9. **EEOC has not developed an organization-wide risk management strategy and processes to manage risk to organizational operations and assets. We recommend EEOC develop an organization-wide risk management strategy and processes to manage risk to organizational operations and assets, in accordance with NIST guidelines.**

OIT concurs with the finding and recommendation. Both OIT and OCFO drafted Enterprise Risk Management Policies and Plans at the end of fiscal year 2016. OIT, OCFO, the Office of Research Information and Planning (ORIP), the Office of Legal Counsel (OLC), and the Office of the Chair, are currently reviewing and consolidating these plans for finalization during fiscal year 2017.

10. **EEOC OIT continuous monitoring processes are not effective for identifying valid FEPA contracts and IMS accounts issued to FEPA users. We recommend that OIT chief information security officer develop, document, and implement a policy requiring OIT to review access logs quarterly to ensure that no one at the FEPA can contact OIT to inappropriately re-activate an account.**

OIT concurs with the finding. The Agency proposes to implement an alternate solution for mitigation of the identified risk, however. The recommendation focuses on the risk related to ensuring that IMS user accounts are disabled and cannot be reactivated when a Fair Employment Practices Agency (FEPA) no longer has a valid contract with the EEOC. The process of authorizing contracts is completed once a year by OFP. OIT and OFP will implement policies and procedures to require that OFP formally notify OIT if a FEPA office no longer has an active contract with the EEOC. OIT will then automatically disable all related user accounts for that

office, reassigning any open charges to other authorized offices/users, as directed by OFP. OIT will also set permissions so that user accounts related to the FEPA office may not be reactivated unless the contract with the FEPA is reinstituted.

11. EEOC does not monitor physical access to EEOC local field offices. We recommend EEOC CFO develop and implement policy and procedures to install surveillance technology and proximity card readers at EEOC local field offices to monitor and control physical access to EEOC controlled exterior entrances.

OCFO will respond to this finding and recommendation.

OCFO's full response to Findings 7 and 11:

7. PIV cards are not required for physical access for all of EEOC's offices. We recommend EEOC Office of the Chief Financial Officer (CFO) implement PIV card readers for physical access for all EEOC's controlled space.

Management's Comment:

Management concurs with comment; implementation continues to be constrained due to resource availability and operational administration. EEOC is actively pursuing opportunities to implement with field office relocation/renovation efforts with GSA assistance.

11. EEOC does not monitor physical access to EEOC local field offices. We recommend EEOC CFO develop and implement policy and procedures to install surveillance technology and proximity card readers at EEOC local field offices to monitor and control physical access to EEOC controlled exterior entrances.

Management's Comment:

Management concurs with comment(s):

Security Cameras: EEOC began implementation of IP security cameras for all field office location intake waiting room areas in FY2016. As of December 2016: two (2) field office locations have IP security cameras installed; one (1) field office location IP security camera is being installed. Current plan is to complete all field office intake waiting room area IP security camera installations by the end of FY2017. Phase II, FY2018, will expand to IP security camera installation in ADR waiting rooms and additional high priority locations.

Intrusion Detection Systems (IDS): EEOC installation of IDS is handled on a case-by-case after reviewing the Federal Protective Service Facility Security Assessment (FSA) recommendations; and examining Security-in-Depth (layers).

HSPD-12 PACS: refer to Finding 7: PIV cards are not required for physical access for all of EEOC's controlled space.

Appendix B – Status of Fiscal Year 2015 FISMA Evaluation Findings

FINDING/RECOMMENDATION	CORRECTIVE ACTION PLAN	DUE DATE	STATUS/ CERTIFICATION OF COMPLETION
FINDING 1: EEOC has no organization-wide Information Security Program Plan that documents and enforces implementation of common and hybrid controls amongst all EEOC IT assets.	EEOC maintains spreadsheets which identify and outline compliance with NIST SP800.53 rev 4 system-specific and common controls. We will update System Security Plans to ensure that these control spreadsheets, along with ownership, are properly referenced. We will also update EEOC Order 240.005, EEOC Information Security Program to outline governance related to common and hybrid controls.	12/2016	Updates to A-123 and A-130 were finalized in late FY 2016. A draft update to 240.005 was completed in September and is currently in review for circulation and finalization during the first quarter of FY 2017.
FINDING 2: EEOC has not developed an organization-wide risk management strategy and processes.	EEOC has documented a risk-management strategy as a component of our Information Security Continuous Monitoring program, however this focus does not address all elements outlined within the recommendation. OIT will work with program offices and the Office of the Chair to develop and document an Enterprise Risk-Management Process in compliance with NIST SPs 800-30 and 800-39. EEOC will also incorporate requirements outlined in the pending update to OMB Circular A-123, once released.	12/2016	A-123 released in late FY 2016. Draft EEOC ERM completed, currently in review
FINDING 3: EEOC should strengthen its contracts with FEPAs to include a statement that requires FEPAs to implement information security controls that ensure data and access to data are secured.	OIT will outline security control requirements and will work with OFP and OLC to incorporate this language into the FEPA contracts.	03/2016	Completed. New language approved by OLC and incorporated into FEPA contracts by OFP
FINDING 4: EEOC should prepare special security controls for its District, Field, and Area Offices to ensure that information systems and information located at these offices are protected.	OIT will collaborate with OFP and OCFO to identify, document, and provide field offices with training on specific security controls that will address the recommended improvements.	09/2016 12/2016	Provided role-based training to Field ITS specific to their 800.53 responsibilities. <Completed> Complete documentation of field responsibilities related to 800.53

FINDING/RECOMMENDATION	CORRECTIVE ACTION PLAN	DUE DATE	STATUS/ CERTIFICATION OF COMPLETION
FINDING 5: The EEOC did not fully implement multifactor authentication to allow remote access to EEOC systems.	EEOC will develop a corrective action plan, including funding, resources, and milestone requirements to resolve this finding. EEOC will also work with DHS to determine if solutions are available under CDM Task Order #2.	FY 2017	Update: EEOC is migrating to Active Directory/Azure Government in CY 2016. The configuration is being set to support PIV 2-factor. Preparatory action taking place in 2016 for 2-factor PIV rollout in FY 2017.
FINDING 6: The EEOC enterprise-wide Information Technology continuity/disaster recovery program that is established and operational at EEOC HQ is not implemented and enforced at the EEOC Field Offices.	OIT, OFP, and OCFO will collaborate with system sponsors to better incorporate field participation in the planning, testing and after-action response.	09/2016	Completed. Field participants were incorporated into DR testing (Caseworks and IMS) and DR requirements were reviewed during Field ITS role-based training.
FINDING 7: EEOC configuration management policy and procedures are not currently supported by automated tools and procedures to accurately and completely detect, identify, and account for changes to the information system component inventory.	OIT will automate our change management processes, utilizing the Change component of Service Now. Implement Change Management System Update Change Management policy documents OIT will automate asset management processes, utilizing the Asset component of Service Now. Phase 1: Non-standard SW and Mobile Devices Phase 2: Implement ServiceNow Discovery OIT will work with DHS to determine if additional automated monitoring tools are available through the CDM program.	 02/2016 08/2016 03/2016 12/2016	 Completed Completed. Completed Implemented in development environment August 2016. Preparing for production deployment, 1Q17