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 2015
Report Number 2015-03-EOIG

Prepared by:

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

Date: December 9, 2015

BROWN & COMPANY

CERTIFIED PUBLIC ACCOUNTANTS AND MANAGEMENT CONSULTANTS, PLLC

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

For Fiscal Year 2015

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, 2015. Our independent evaluation covered the period October 1, 2014 through September 30, 2015.

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.

Brown & Company

Largo, Maryland
December 9, 2015

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

For Fiscal Year 2015

1. Executive Summary

For Fiscal Year (FY) 2015, 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 seven FISMA findings and seven corresponding recommendations. The FY 2015 findings are as follows:

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.
2. EEOC has not developed an organization-wide risk management strategy and processes.
3. EEOC should strengthen its worksharing agreement with Fair Employment Practices Agencies (FEPAs) to include a statement that requires FEPAs to implement information security controls that ensure data and access to data are secured.
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.
5. The EEOC did not fully implement multifactor authentication to allow remote access to EEOC systems.
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.
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.

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. OMB will be responsible for developing guidance on what constitutes a major incident.
- 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. As of issuance of this report, the Agency's Chief Information Officer (CIO), Ms. Kimberly Hancher, retired from Federal service and Ms. Pierrette McIntiere, Associate CIO, was designated as Acting CIO.

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 oversight of its 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, Financial and Business Management System (FBMS)
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:

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

The period covered by this independent evaluation is October 1, 2014 to September 30, 2015. 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) 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.

6. Findings and Recommendations

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

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.**

Condition:

The EEOC does not have an approved organization-wide Information Security Program Plan that documents and enforces the implementation of common and hybrid controls amongst all EEOC IT assets. The condition is not that the agency does not have an Information Security Program Plan, but the agency's plan is:

- Missing documentation of the designed population of EEOC common, hybrid, and application specific controls.
- Missing a statement as to the party responsible for implementing the controls (EEOC, vendors, or both EEOC and vendors.)
- Missing evidence that EEOC has implemented and tested the operating effectiveness of the common and hybrid controls.
- Missing evidence that EEOC or its vendors has implemented the application specific controls of its major applications.

The related EEOC System Security Plans (SSPs) have not been updated to include all the controls and control enhancements specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4 Table D-2: *Security Control Baseline for Mod Systems*. Furthermore, EEOC should also take into consideration Table E-2: *Assurance Related Controls for Moderate Impact Systems*.

[1] FY 2015 *Inspector General Federal Information Security Modernization Act Reporting Metrics V1.2,* dated June 19, 2015 includes the ISCM maturity model for FY 2015.

Criteria:

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, PM-1 "Information Security Program Plan," states:

Control: The organization:

a. Develops and disseminates an organization-wide information security program plan that:
    1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
    2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
    3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and
    4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations and the Nation.
b. Reviews the organization-wide Information Security Program Plan;
c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and
d. Protects the information security program plan from unauthorized disclosure and modification.

Supplemental Guidance: Information security program plans can be represented in single documents or compilations of documents at the discretion of organizations. The plans document the program management controls and organization-defined common controls. Information security program plans provide sufficient information about the program management controls/common controls (including specification of parameters for any *assignment* and *selection* statements either explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plans and a determination of the risk to be incurred if the plans are implemented as intended.

The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls.

Cause:

We have determined that many elements of an EEOC organization-wide Information Security Program Plan for the agency are in design and/or development. This determination is supported by the security plans for individual EEOC information systems and applications. However, EEOC has not completed its efforts to do the following:

1. Complete the selection, design and implementation of common controls as system-specific or hybrid controls on an organization-wide basis with the involvement of EEOC's senior leadership (i.e., authorizing officials, CIO, senior information security officer, information system owners, mission/business owners, information owners/stewards, risk executive).
2. Mandate that all system staff offices (S/SO), federally- and contractor-managed, identify within their system security plans which controls are inherited as common controls, which are shared responsibilities as hybrid controls, and which are S/SO application-specific.
3. Hold OIT accountable and monitor their performance and compliance through the Chief Information Systems Officer's (CISO), and Information System Security Officer (ISSO) monitoring and reporting channels and processes.
4. Ensure that compliance with the organization-wide implementation of common, hybrid, and application-specific controls is made a requirement and included in the standard language of all contracting vehicles.
5. Develop and document an EEOC agency-wide Information Security Program Plan that describes the program management controls and common controls in place or planned for meeting the security requirements for individual information systems and the totality of all information technology assets, data, and security controls that support EEOC's organizational mission.

Effect:

The lack of organization-wide security program management controls results in the risk that there is inconsistency in the design and implementation of the enterprise-wide security program. The risk of inconsistency in the implementation of security program management controls increases exposure that FISMA controls are either over applied or under applied. This may result in potential gaps (vulnerabilities) in EEOC's security posture. Gaps within the controls over federally-managed and/or contractor managed information systems could provide additional vectors for threat agents to exploit.

Recommendation 1:

1. We recommend that EEOC fully document, publish and enforce a CIO-approved organization-wide Information System Program Plan for common controls and hybrid controls across all systems and applications.
2. We recommend the EEOC organization-wide Information System Program Plan include:

- Names and contact information for the government and vendor partner personnel who are sharing responsibility for the definition and implementation of the EEOC common, hybrid, and application-specific controls.
- An EEOC defined and approved population of common, hybrid and application controls.
- A Memorandum of Understanding (MOU), or similar document, that acknowledges the government's and vendor's responsibility for designing and implementing their assigned portions of the population of EEOC NIST 800-53 Revision 4 controls.

3. We recommend that EEOC complete this organization-wide security program objective by publishing its approved organization-wide Information Security Program Plan population of common, hybrid, and application controls and continuously monitoring its approved common controls and hybrid controls.

Management's Response:

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

"Management concurs with this finding. While EEOC maintains spreadsheets which identify and outline compliance of NIST SP 800.53 rev. 4 system-specific and common controls for our major systems, our Information Security Program Plan (EEOC Order 240.005) and individual System Security Plans (SSPs) do not include the governance elements outlined within the recommendation. OIT will update EEOC Order 240.005 and the related SSPs to include this governance."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation ensures the organization-wide Information Security Program Plan and related SSPs are updated and comprehensive and will resolve the reported condition.

Finding 2	**EEOC has not developed an organization-wide risk management strategy and processes.**

Condition:

The EEOC conducted risk assessments against the major applications and the 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.

The organization-wide risk management strategy provides the objectives and action statements needed to:

- Analyze individual risk management plans and assessment results for FISMA reportable systems (general support systems, major and minor applications),
- Determine the potential adverse impacts on the EEOC organization, mission/business processes, and information system-level components, and
- Develop and implement organization-wide risk management processes 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 SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*. Risk management processes include framing risk; assessing risk; responding to risk; and monitoring risk.

Criteria:

NIST SP 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:

The EEOC's risk assessments did not include conducting and completing an agency-wide risk assessment at the Tier1 Organization level, in accordance with NIST SP 800-30, *Guide for Conducting Risk Assessments*, Revision 1, Section 2.4 "Application of Risk Assessments."

The EEOC-wide risk management process was not documented in accordance with:

- NIST SP-800-30, *Guide for Conducting Risk Assessments*, Revision 1, Section 2.1 "Risk Management Process," and
- NIST SP 800-39, *Managing Information Security Risk,* Appendix E, "Risk Management Process Tasks."

Effect:

Without designing and implementing an EEOC-wide (enterprise-wide) Risk Management Strategy and Process, responsible personnel may not be kept abreast adequately of enterprise-wide and general support system/application-specific threats, vulnerabilities, and attack vectors.

Recommendation 2:

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:

"Management concurs with this finding. EEOC has documented a risk-management strategy as a component of our Information Security Continuous Monitoring program, however we concur that 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."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation ensures an enterprise-wide risk management process that is in compliance with NIST and OMB Circular A-123, as revised, and resolves the reported condition.

Finding 3	**EEOC should strengthen its worksharing agreement with FEPAs to include a statement that requires FEPAs to implement information security controls that ensure data and access to data are secured.**

Condition:

The EEOC has worksharing agreements with FEPAs for processing charges of employment discrimination within their geographic boundaries. The EEOC and FEPA each designate the other as its agent for the purpose of receiving and drafting charges, including those that are not jurisdictional with the agency that initially receives the charges. The FEPA Gateway Oracle Forms application provides users external to the EEOC network the ability to upload data through data files into the IMS application located at EEOC headquarters. FEPAs collect and transmit charge data, charging party, and respondent records. The workshare agreements between EEOC and FEPA do not include a security clause requiring FEPAs to implement information security controls that ensure that data and access to data are secure.

Criteria:

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

OMB M-10-15 Memo section "Contractor Monitoring and Controls," states the following:

"Agency must ensure their contractors are abiding by FISMA requirements. Section 3544(a)(1)(A)(ii) describes Federal agency security responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." Section 3544(b) requires each agency 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." This includes services which are either fully or partially provided, including agency hosted, outsourced, and software-as-a-service (SaaS) solutions."

"Because FISMA applies to both information and information systems used by the agency, contractors, and other organizations and sources, it has somewhat broader applicability than prior security law. That is, agency information security programs apply to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems (whether automated or manual) – on behalf of a Federal agency. Such other organizations may include contractors, grantees, State and local Governments, industry partners, providers of software subscription services, etc. FISMA, therefore, underscores longstanding OMB policy concerning sharing Government information and interconnecting systems."

Cause:

EEOC has developed a worksharing agreement to allow FEPAs to collect and transmit data to its IMS system; however, the agreement does not require FEPAs to implement information security controls to protect data and the ISM system from unauthorized access.

Effect:

The lack of a security policy for FEPAs increases the risk of unauthorized access to information and information systems. Devices used by external parties are at a higher risk of threat than client devices that are issued and controlled by EEOC's OIT office. If a FEPA has not implemented proper information security controls to protect devices and data, an unauthorized person could gain access to the IMS system and gain unauthorized access to charges data. In addition, a device that does not have the latest security patches could be infected with malicious viruses or worms, which can easily spread to interconnected systems.

Recommendation 3:

We recommend EEOC develop, document, and implement a policy requiring FEPAs that collect, store, process, use and transmit EEOC data to implement information security controls that ensure data and access to data are secured. For example, the worksharing agreement should include a clause that requires only authorized individuals access to the IMS system and that devices are updated with current system security patches and antivirus signatures before users connect to the system.

Management's Response:

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

"Management concurs that FEPA contracts should include wording that outlines security control requirements to better protect EEOC systems and data. OIT and OFP will work with the Office of Legal Counsel to prepare language for incorporation into the FEPA contracts."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation ensures that future FEPA contracts require FEPAs to implement information security controls that better protect EEOC systems and data and resolves the reported condition.

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.**

Condition:

Security control assessments of its District, Field and Area Offices have not been performed to ensure that security controls previously put in place are operating as designed.

We reviewed information system security controls at four EEOC offices— Birmingham District Office and Philadelphia District Office, Baltimore Field Office and Albuquerque Area Office— and made the following observations:

- Segregation of duties. Security procedures can be improved by ensuring that managers do not have the responsibility of both granting and approving access rights.
- Segregation of duties. Security procedures can be improved by ensuring that managers do not have the responsibility of both receiving and storing equipment.
- System monitoring. Performance can be improved if OIT ensures that IT staff have adequate training and skillsets for monitoring information systems.
- Continuity of Operations (COOP) and Disaster Recovery (DR). The IT staff could benefit from training in continuity of operations and disaster recovery.
- Confidentiality. Security could be improved if the IT staff ensures confidentiality of information, to include password protection.
- Network security. The offices could better protect the network by installing monitoring devices on the network and implementing port security.
- Safeguarding. Investigators can improve safeguarding of case files by locking investigator's office doors after hours and when no one is present in the office attending to the files.
- Physical security (Baltimore). Third-party contracting security officers do not consistently enforce the barring notices or the ID verification procedures that are requested by EEOC or mandated by Federal Protective Service (FPS) requirements. For instance, a recent security incident resulted in personnel being barred by EEOC for disorderly conduct; however, a contracting security officer allowed the barred personnel to enter the premises, despite having their pictures and barring notices posted at the security officer's desk.
- Physical Security to Baltimore EEOC's IT room. The field office is located in a multi-tenant, privately-managed building. The EEOC leasing agent for the building, as well as other tenants in the building have keys to EEOC's IT facilities. Only authorized EEOC personnel should have access to EEOC's field office IT facilities.

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:

The 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 controls 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 increase the risk of organization-wide security vulnerabilities.

Recommendation 4:

We recommend that the EEOC develop special security controls for Field Offices that align with the Federal Managers' Financial Integrity Act of 1982. In addition, we recommend the following improvements:

1. Assess the information systems security controls at the district, field and area offices.
2. Segregation of duties – Implement policies and procedure to ensure that managers do not have granting and approval rights for providing access to systems.
3. Segregation of duties – Implement policies and procedure to ensure managers do not have rights to both receive and store equipment.
4. System monitoring – Implement policies and procedure to ensure that IT staff have adequate skillsets to monitor information systems. In addition, provide annual network training.
5. COOP and DR – Provide IT staff COOP and DR training.
6. Confidentiality – Implement policies and procedures to ensure that the IT staff maintain confidentiality of sensitive data.
7. Network security – Install network monitoring devices and port security.
8. Safeguarding – Lock investigator's office doors after hours and when the office is vacant.
9. Physical security (Baltimore) – Ensure that third-party security officer contractors enforce the barring notices and the ID verification procedures; and
10. Physical Security to Baltimore EEOC's IT room – Ensure that only authorized EEOC personnel has access to EEOC's field office IT facilities.

Management's Response:

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

"Management concurs with this finding. 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."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation, recommended improvements and plan to identify, document and provide training on security controls for information systems at the District, Field and Area Offices will resolve the reported condition.

Finding 5: The EEOC did not fully implement multifactor authentication to allow remote access to EEOC systems.

Condition:

The EEOC has not implemented multifactor authentication where one of the factors is provided by a device separate from the computer gaining remote access. EEOC requires only a user ID and password to access EEOC information systems and does not require the use of an authentication device, such as a token or Homeland Security Presidential Directive 12 Personal Identity Verification (HSPD-12 PIV) card for remote or network 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).

Control Enhancement:

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

Effect:

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

Recommendation 5:

We recommend EEOC OIT implement multifactor authentication for remote access. Furthermore, we recommend EECO 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:

"*Management concurs with this finding, but implementation continues to be constrained by resource availability. EEOC understands that the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program, Task Order 2, may be able to provide agencies with support and services in this area; therefore, EEOC is actively pursuing funding of this technology through the DHS CDM program.*"

Auditor's Evaluation of Management's Response:

Management's response does not implement the recommendation. We recommend management develop a corrective action plan, including funding, resources, and milestone requirements, and implement two-factor authentication to resolve the finding.

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.**

Condition:

Through inquiry of personnel, inspection of documentation, and observation of operational and process walkthroughs, we determined that EEOC has not developed a comprehensive strategy for:

- Test, training and exercise (TT&E) programs to test or exercise the EEOC Business Continuity Plan (BCP) and IT Disaster Recovery Plan (IT DRP) and determine their operational effectiveness in both Headquarters (HQ), as well as in the Field Offices
- Performing after-action reporting that addresses issues identified during contingency/disaster recovery exercises and incorporates them into HQ and field office plan updates.
- Coordinating the HQ OIT BCP and IT DRP TT&E programs with the 53 EEOC Field Offices to ensure adequate levels of emergency preparedness and IT disaster recovery capability across all of the EEOC.

Criteria:

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* CP-4 "Contingency Plan Testing," states:

Control: The organization:

a. Tests the contingency plan for the information system at least annually using organization-defined tests, to determine the effectiveness of the plan and the organizational readiness to execute the plan;
b. Reviews the contingency plan test results; and
c. Initiates corrective actions, if needed.

Control Enhancements:

Contingency Plan Testing/Coordinate with Related Plans

(1) The organization coordinates contingency plan testing with organizational elements responsible for related plans.

Cause:

While performing the FY 2015 EEOC FISMA procedures, we determined that the agency conducts contingency plan testing at the enterprise-wide level. However, the agency did not provide the results of testing for the following system-specific contingency plans: DNS; EEO-1 Survey System; DMS; and IMS.

However, at the Philadelphia and Baltimore field office levels, management and operational and technical personnel were unable to demonstrate knowledge of, or proficiency in, performing the duties and tasks described within the EEOC HQ and Field Office Contingency Plan.

Effect:

Without designing and implementing contingency planning and testing strategies at EEOC HQ and field offices, responsible personnel may not be kept abreast adequately and trained in a timely manner to have the knowledge, skills, and abilities needed to protect its people and assets, continue essential support tasks, and minimize any adverse consequences of disruption resulting from a disaster or catastrophic event, in accordance with Federal Continuity Directive 1 (FCD-1).

Recommendation 6:

We recommend the EEOC:

- Develop TT&E programs to test or exercise the EEOC BCP and IT DRP at the HQ and field office levels and determine their operational effectiveness.
- Conduct after-action reporting that addresses issues identified during contingency/disaster recovery exercises and incorporates them into HQ and field office plan updates.

- Coordinate the HQ OIT BCP and IT DRP TT&E programs with the 53 EEOC field office's programs to ensure adequate levels of emergency preparedness and IT disaster recovery capability across EEOC. Develop and perform testing of system-specific contingency plans for the following EEOC General Support Systems and major applications: DNS; EEO-1 Survey System; DMS; and IMS.

Management's Response:

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

"Management concurs that IT continuity/disaster recovery program could be improved through increased participation by field offices. OIT, OFP, and OCFO will collaborate with system sponsors to better incorporate field participation in the planning, testing and after-action response."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation and incorporating Field Offices' participation in the planning, testing and after-action response will resolve the reported condition.

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.**

Condition:

EEOC currently does not define policy or provide automated tools and processes to:

- Detect the presence of unauthorized hardware, software, and firmware components within the information system inventory; and
- Take the following actions when unauthorized components are detected:
  i. Disable network access by such components;
  ii. Isolate the components; and
  iii. Notify EEOC-defined personnel or roles with the responsibility to remediate the unauthorized components detected.

Specifically, we did not observe EEOC tools in place to detect and report on unauthorized IT component inventory for DNS, EEO-1 Survey System, DMS, and IMS. These monitoring, detection, and correction activities, include, but are not limited to the following:

- Network enumeration for all IT assets connected to the HQ and field offices' Wide Area Networks (WANs) and Local Area Networks (LANs).

- Baseline configuration definition and enforcement for all IT components' hardware and software inventories deployed on the network.
- Monitoring and approval for the implementation of authorized changes to the configuration baselines.
- Monitoring, prevention, detection, and correction of unauthorized changes to the configuration baselines for all IT assets connected to HQ and Field Offices' WANs and LANs.

EEOC currently does not provide policy and procedures to verify that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

Criteria:

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* CM-8 "Information System Component Inventory," states:

Control Enhancements**:**

(1) Information System Component Inventory | Updates During Installations / Removals

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

(3) Information System Component Inventory | Automated Unauthorized Component Detection

The organization:

(a) Employs automated mechanisms [*on an organization-defined frequency*] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and

(b) Takes the following actions when unauthorized components are detected: [*Selection (one or more): disables network access by such components; isolates the components; notifies* [*organization-defined personnel or roles with the responsibility to remediate the unauthorized components detected.*]].

Supplemental Guidance: This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented within information systems or in other separate devices. Isolation can be achieved, for example, by placing unauthorized information system components in separate domains or subnets or otherwise quarantining such components. This type of component isolation is commonly referred to as sandboxing.

(5) Information System Component Inventory | No Duplicate Accounting of Components

The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

Supplemental Guidance: This control enhancement addresses the potential problem of duplicate accounting of information system components in large or complex interconnected systems.

Cause:

EEOC does not define policy and procedures and manage automated tools to:

1. Accurately reflect the current information system inventory system;
2. Include and monitor all components within the authorization boundary of the information system;
3. Provide the level of granularity deemed necessary for real-time tracking and reporting of IT assets being added, modified, or removed from the EEOC HQ and field offices' networks; and
4. Review and update the information system component inventory for authorized changes, and prevent, detect, and correct unauthorized changes.

Effect:

Without automated tools and procedures to support the configuration management process, EEOC responsible personnel may not be kept abreast adequately and informed of unauthorized changes to the EEOC systems' component inventory. Nor will responsible personnel have the capability to readily detect the presence of unauthorized hardware, software, and firmware components within the information system inventory, and take one or more of the following actions when unauthorized components are detected:

- Disable network access by such components;
- Isolate the components; and
- Notify EEOC personnel or roles with the responsibility to remediate the unauthorized components detected.

Recommendation 7:

We recommend EEOC build upon existing HQ configuration management policy and procedures to deploy automated tools and procedures that accurately and completely detect, identify, and account for changes to the information system component inventory.

Management's Response:

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

"Management concurs with this finding, however EEOC does not currently have the technology or resources available to fully automate the recommendation. OIT will build upon existing HQ configuration management policy and procedures to deploy tools and procedures that more accurately detect, identify, and account for changes to the information system component inventory, using both automated and manual processes. EEOC will additionally work with DHS to identify if additional tools and services might be available to EEOC under their CDM program to provide better automate detection and prevention."

Auditor's Evaluation of Management's Response:

Management's response is appropriate to address the finding and recommendation. Effective implementation of the recommendation and using both automated and manual processes to accurately and completely detect, identify, and account for changes to the information system component inventory will resolve the reported condition.

Appendix A – Management's Response

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

December 03, 2015

MEMORANDUM

TO: Milton Mayo, Inspector General

FROM: Pierrette McIntire, Acting Chief Information Officer
Office of Information Technology

Pierrette McIntire

SUBJECT: Management's Comments on the FY 2015 Independent Evaluation of the EEOC's Compliance with Provisions of FISMA

Below are consolidated comments from the Office of Information Technology (OIT), Office of Field Programs (OFP), and Office of the Chief Financial Officer (OCFO) regarding the findings outlined in the FY 2015 Independent Evaluation of EEOC's compliance with Federal Information Security Modernization Act (FISMA).

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.

Management concurs with this finding. While EEOC maintains spreadsheets which identify and outline compliance of NIST SP 800.53 rev. 4 system-specific and common controls for our major systems, our Information Security Program Plan (EEOC Order 240.005) and individual System Security Plans (SSPs) do not include the governance elements outlined within the recommendation. OIT will update EEOC Order 240.005 and the related SSPs to include this governance.

2. EEOC has not developed an organization-wide risk management strategy.

Management concurs with this finding. EEOC has documented a risk-management strategy as a component of our Information Security Continuous Monitoring program, however we concur that 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.

3. EEOC should strengthen its work sharing agreement with the FEPA agencies to include a statement that requires FEPA agencies to implement information security controls that ensure data and access to data is secured.

Management concurs that FEPA contracts should include wording that outlines security control requirements to better protect EEOC systems and data. OIT and OFP will work with the Office of Legal Counsel to prepare language for incorporation into the FEPA contracts.

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

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.

Management concurs with this finding. 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.

5. The EEOC did not fully implement multifactor authentication to allow remote access to EEOC systems.

Management concurs with this finding, but implementation continues to be constrained by resource availability. EEOC understands that the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program, Task Order 2, may be able to provide agencies with support and services in this area; therefore, EEOC is actively pursuing funding of this technology through the DHS CDM program.

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 for IT.

Management concurs that IT continuity/disaster recovery program could be improved through increased participation by field offices. OIT, OFP, and OCFO will collaborate with system sponsors to better incorporate field participation in the planning, testing and after-action response.

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.

Management concurs with this finding, however EEOC does not currently have the technology or resources available to fully automate the recommendation. OIT will build upon existing HQ configuration management policy and procedures to deploy tools and procedures that more accurately detect, identify, and account for changes to the information system component inventory, using both automated and manual processes. EEOC will additionally work with DHS to identify if additional tools and services might be available to EEOC under their CDM program to provide better automate detection and prevention.

Appendix B – Status of Fiscal Year 2014 FISMA Evaluation Findings

FINDING/RECOMMENDATION	CORRECTIVE ACTION PLAN	DUE DATE	STATUS/ CERTIFICATION OF COMPLETION
FINDING 1 - EEOC Risk Management Program is not fully developed per NIST SP 800-37 Rev1.	Updated ISCM Plan to fully document EEOC's Risk Management Program. OIT will update Order 240.001, Information Security Program Directive to better incorporate Risk Management once OMB A-130 Revisions are finalized.	08/30/15	**Completed** ISCM Plan Updated 6/2015
FINDING 2 - EEOC system level risk assessment reports include outdated diagrams.	During our annual risk assessment review, OIT will update all risk assessment report and ensure diagrams are current	08/31/15	**Completed** Risk Assessment Plan and Risk Assessment Report completed with DataNet ATO
FINDING 3 - EEOC's Bring Your Own Device Program does not address all elements of NIST SP 800-124 related to operation, maintenance, & disposal.	OIT will update policy to better document operation, maintenance, and disposal of mobile devices	06/30/15	**Completed** New Policy Issued July, 2015
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.	The correction action plan was not received. The following is management's response to the recommendation: "*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*	TBD	**Open**

FINDING/RECOMMENDATION	CORRECTIVE ACTION PLAN	DUE DATE	STATUS/ CERTIFICATION OF COMPLETION
	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."		
FINDING 5 – VPN settings do not enforce strong password management rules	OIT will request funds to implement a VPN management solution that can better enforce password requirements. In the interim, OIT will issue guidance and tips to VPN participants on strong password requirements.	08/30/15	**Completed** VPN Gateways upgraded June, 2015. VPN LDAP Authentication deployed 09/27/15 to enforce strong password mgmt. rules.
FINDING 6 – Digital Backup Media is not encrypted during transport	OIT has accepted the risk associated with the finding and has implemented compensating controls. The risk acceptance will be documented for future reference.	01/30/15	**Completed** Policy updated 12/2014
FINDING 7 – Response times for security alert reviews is not clearly defined	OIT will update our Incident Response Plan to better document incident response requirements related to security alerts	08/30/15	**Completed** ISCM Plan Updated 6/2015 Incident Plan – Updated 07/15
FINDING 8 – EEOC has not implemented File Integrity Monitoring to detect unauthorized changes.	With the implementation of Windows7, OIT will implement Dynamic Local User polices to restrict the rights needed to make changes. OIT will also use software deployment tools to ensure consistent configuration and versioning.	Policy - 08/30/15 Deploy-with Win7	**Completed** New DLU Policy & SW Distribution Policies, completed June 2015 Ongoing – Implementation w/Win7 Rollout underway
FINDING 9 – Laptop computers issued for Disaster Recovery are not checked to ensure patches and updates are installed.	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. OIT will implement policies to require that workstations that do	11/30/15	D620s to be phased out with Win7 deployment (12/2015). **Completed** ZENworks used to monitor patches for all systems that attach to the network.

FINDING/RECOMMENDATION	CORRECTIVE ACTION PLAN	DUE DATE	STATUS/ CERTIFICATION OF COMPLETION
	now show on the reports as being updated are brought into the office for connection to the network and update, as required.		
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.	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	TBD	**Open**
FINDING 11 – EEOC offices did not all achieve 95% compliance with completion of annual security awareness training.	OIT will update policy and implement procedures to better enforce SAT compliance and communicate deficiencies to management, as required.	09/30/15	Improved SAT Offerings and communications **Completed** Overall Agency compliance rate for both HQ and Field increased to 98%.
FINDING 12 – EEOC does not have policies and procedures to properly manage HQ physical security access cards.	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.	TBD	**Open**
FINDING 13 – EEOC does not employ full-device or container encryption to protect agency laptops.	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.	Image Completed Deploy w/Win7	**Completed** New Win7 image uses ZENworks Full Disk Encryption Ongoing – Implementation w/Win7 Rollout underway
FINDING 14 – EEOC has not developed COOP Implementation Plans for its respective field offices.	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%	TBD	**Open**

FINDING/RECOMMENDATION	CORRECTIVE ACTION PLAN	DUE DATE	STATUS/ CERTIFICATION OF COMPLETION
	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.		
FINDING 15 – EEOC's telecommuting policy does not address all NIST SP800-46 Rev 1 requirements.	OIT and OHR will update Telework Security Policy to meet requirements.	09/30/15	**Completed** New Telework policies issued in late 2014 address various components of telework requirements. **Completed** Created Telework Security Addendum to consolidate the telework security requirements into a single document.
FINDING 16 – EEOC does not have policies and procedures for managing shared group accounts.	With the deployment of Windows 7, EEOC will be using Novell DLU policies to control the issuance of persistent local admin rights to IT support staff (over specific domains) and to individuals (for specific computers). In these ways, the use of the installer account will be drastically minimized, and retained primarily for selected Help Desk 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).	07/30/15 – policy Deploy w/Win7	**Completed** New DLU policies issued in June 2015. Ongoing – Implementation w/Win7 Rollout underway
FINDING 17 – EEOC needs to improve account management procedures that include disabling inactive accounts as required.	OIT will update EEOC's Account Management Policy to enforce the use of Service Now for off-boarding users. As users are off-boarded via Service Now, tickets are automatically created and assigned to system administrators for disabling or deleting the various related accounts. Task completion will be automatically tracked, with non-compliance with service level agreements reported daily to supervisors.	08/30/15	**Completed** Provided guidance and training on On-Boarding and Off-Boarding in 2Qtr 2015. **Completed** Updated Account Mgmt Policy – July 2015

FINDING/RECOMMENDATION	CORRECTIVE ACTION PLAN	DUE DATE	STATUS/ CERTIFICATION OF COMPLETION
FINDING 18 – EEOC needs to control physical access to controlled and sensitive areas.	OIT and OCFO will review access procedures and authorizations and will better enforce existing policy.	03/31/15	Met with OCFO to discuss. Still have issues when CRAC units fail which requires that doors be kept open to keep equipment from overheating. **Completed** Meetings with OCFO/OIT/JLL to address CRAC unit issues 09/2015
FINDING 19 – EEOC's internal vulnerability assessment (scans) identified risks that should be analyzed and resolved.	OIT will update scan policy and implement procedures to ensure risks are analyzed and resolved or accepted.	06/30/15	**Completed:** Enhanced mitigation is addressed by policy change per ISCM (8/2015) pgs 30-33 and 47-50; findings distributed through managers (not system admins) and tracked by POA&M and ServiceNow. External scans are distributed through supervisory channels also, to facilitate mitigation tracking. Open: The FY 2015 Internal Vulnerabilities results rated the agency posture as Fair, which is the same rating for FY 2014. OIT is obtaining professional assistance in implementing PVS scanning in addition to active vulnerability scans, to begin by late October 2015. This will assist the agency in identifying and remediating internal vulnerabilities sooner.