

**U.S. Equal Employment Opportunity Commission
Federal Information Security Modernization Act of 2014 (FISMA)
Fiscal Year 2019 Performance Audit**

**For Fiscal Year 2019
2019-04-AOIG**

Prepared by:

**Brown & Company
Certified Public Accountants and Management Consultants, PLLC
6401 Golden Triangle Drive, Suite 310
Greenbelt, Maryland 20770
(240) 770-4903**

February 20, 2020

Proprietary and Confidential

**U.S. Equal Employment Opportunity Commission
Federal Information Security Modernization Act of 2014 (FISMA)
Fiscal Year 2019 Performance Audit**

Table of Contents

Independent Auditor’s Report	1
1. Executive Summary	3
2. Background	3
3. Summary of Results	5
4. Findings and Recommendations	6
Appendix A – Scope, Objective, Methodology and Criteria	16
Appendix B - Status of Prior Findings.....	19
Appendix C – EEOC Management’s Comments.....	21



Independent Auditor's Report

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

This report presents the results of our independent performance audit of the U.S. Equal Employment Opportunity Commission's (EEOC) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires Federal agencies, including EEOC, to have an annual independent evaluation performed of their information security programs and practices to determine the effectiveness of such programs and practices, and to report the results of the evaluation to the Office of Management and Budget (OMB) and the U.S. Department of Homeland Security (DHS). The EEOC Office of Inspector General (OIG) contracted with Brown & Company CPAs and Management Consultants, PLLC (Brown & Company) to conduct an audit of EEOC's information security program and practices for Fiscal Year (FY) 2019.

FISMA requires EEOC to develop, document, and implement an agency-wide information security program to protect its information and information systems, including those provided or managed by another agency, contractor, or other source. FISMA also clearly places responsibility on each agency program office to develop, implement, and maintain an information security program that assesses risk and provides adequate security for the operations and assets of programs and systems under its control.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objective of this performance audit was to assess the effectiveness of the EEOC's information security program and practices. To address our audit objective, we assessed the effectiveness of the EEOC information system program and practices for six information systems. As part of our audit, we responded to the DHS's *FY 2019 Inspector General FISMA Reporting Metrics V 1.3*, dated April 9, 2019, and assessed the maturity levels on behalf of the EEOC OIG.

Our methodology for the FY 2019 FISMA performance audit included testing the EEOC's systems for compliance with selected security controls covered by the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations* and *NIST Cybersecurity Framework (version 1.1)*.

We considered the internal control structure for selected EEOC systems in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives. Accordingly, we obtained an understanding of the internal controls for these various systems through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures.

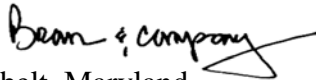
We determined EEOC generally had sound information security controls for its information security program and has implemented security controls in all eight DHS Inspector General (IG) FISMA Reporting Metrics. Based on our audit work, we concluded that the EEOC's information security program is substantially compliant with the FISMA legislation and applicable OMB guidance and the security controls tested demonstrated operating effectiveness.

Our report identifies the following four findings where the EEOC Office of Information Technology's (OIT) information security program can better protect the confidentiality, integrity, and availability of its information and information systems:

1. EEOC OIT needs to monitor security controls over SharePoint.
2. EEOC OIT needs to remediate internal vulnerabilities on its network.
3. EEOC OIT needs to enforce its mobile device management compliance policies.
4. EEOC OIT needs to develop an action plan to address the SECURE¹ Technology Act requirements.

Addressing these identified findings strengthens the EEOC's information security program, and contributes to ongoing efforts to maintain reasonable assurance of adequate security over information resources.

In closing, we appreciate the courtesies extended to Brown & Company by EEOC and EEOC OIG during this engagement.



Greenbelt, Maryland
January 28, 2020

¹ Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act.

1. Executive Summary

For Fiscal Year (FY) 2019, 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 a performance audit 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 performance audit, Brown & Company concluded that EEOC's information security program is substantially compliant with the FISMA legislation and applicable Office of Management and Budget (OMB) guidance. We determined EEOC's information security programs are effective and provide reasonable assurance of adequate security.

In conducting our audit work, we identified the following four findings related to EEOC's security practices that can be improved.

1. EEOC OIT needs to monitor security controls over SharePoint.
2. EEOC OIT needs to remediate internal vulnerabilities on its network.
3. EEOC OIT needs to enforce its mobile device management compliance policies.
4. EEOC OIT needs to develop an action plan to address the SECURE Technology Act requirements.

In addition, as illustrated in **Appendix A**, seven findings reported in prior years' audits have not been fully implemented, and therefore, new recommendations were not made regarding these findings.

2. Background

The Federal Information Security Modernization Act of 2014

On December 18, 2014, President Obama signed the FISMA, a bill that reformed the FISMA of 2002. The law updates and modernizes FISMA to provide a leadership role for the U.S. 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 bill:

- Reasserts the authority of the Director of the 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's 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, OIG must submit to DHS the "Inspector General FISMA Reporting Metrics" that depicts the effectiveness of the agency's information security program.

The EEOC Overview

The EEOC is a bipartisan Commission comprised of five presidentially appointed members, including the Chair, Vice Chair, and three Commissioners. The Chair is responsible for the administration and implementation of policy for and the financial management and organizational development of the Commission. The Vice Chair and the Commissioners participate equally in the development and approval of Commission policies, issue charges of discrimination where appropriate, and authorize the filing of suits. In addition to the Commissioners, the President appoints a General Counsel to support the Commission and provide direction, coordination, and supervision to the EEOC's litigation program.

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, gender identity, and sexual orientation), 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. EEOC provides services at the headquarters offices in Washington, D.C. and through 53 field offices.

The 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 the following components: Immediate Office of the Chief Information Officer (OCIO); Customer Services Management Division; Infrastructure Management and Operations Division; and Enterprise Applications Innovation Division.

3. Summary of Results

We determined EEOC’s information security program is substantially in compliance with FISMA legislation and OMB guidance, and provides reasonable assurance of adequate security.

We also assessed EEOC’s maturity levels for the National Institute of Standards and Technology (NIST) Cybersecurity Framework function areas within the range of: ad hoc, defined, consistently implemented, managed and measurable, or optimized.

Exhibit 1 details the five maturity model levels: ad hoc, defined, consistently implemented, managed and measurable, and optimized.

Exhibit 1– DHS Maturity Level Criteria

Maturity Level Criteria	Maturity Level Description
Level 1: Ad hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented, but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Exhibit 2 presents the assessment results for EEOC maturity level assessment by function areas.

Exhibit 2 – EEOC Maturity Level Assessment by Function Areas

NIST Cybersecurity Framework Function Areas (Domains)	Overall Maturity Level
Function 1: Identify (Risk Management)	Consistently Implemented
Function 2: Protect (Configuration Management)	Managed and Measureable
Function 2: Protect (Identity and Access Management)	Managed and Measureable
Function 2: Protect (Data Protection and Privacy)	Consistently Implemented
Function 2: Protect (Security Training)	Consistently Implemented
Function 3: Detect (Information Security Continuous Monitoring (ISCM))	Managed and Measureable
Function 4: Respond (Incident Response)	Managed and Measureable
Function 5: Recover (Contingency Planning)	Consistently Implemented

Ratings throughout the domains are determined by a simple majority, where the most frequent level across the questions will serve as the overall maturity level.

4. Findings and Recommendations

We assessed the effectiveness of EEOC’s information system security controls and identified weaknesses. As a result, we identified four findings and made five recommendations to assist EEOC in strengthening its information security program.

Finding 1: EEOC OIT needs to monitor security controls over SharePoint.

Condition

EEOC’s SharePoint system is used as a repository to allow EEOC’s users across the agency to store and share files. EEOC’s SharePoint system is an application under the general support systems. EEOC’s SharePoint access security controls are configured to allow EEOC’s users to create sites. When a site is created in SharePoint, the settings are set as “private” by default, granting access to a selected group of individuals. Owners have the ability to change the settings to “public”, granting access to all approved SharePoint users within EEOC.

During our testing, we discovered one instance where an owner granted “public” access to their Chicago EEOC SharePoint site containing sensitive and PII information, granting access to all EEOC approved SharePoint users.

Criteria:

EEOC Policy on the Protection of Sensitive Information, states:

Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII) shall be stored on network drives and/or in EEOC systems with proper access controls – e.g., user IDs/passwords, with rights limited to only those individuals authorized to access the data.

NIST SP 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, AR-2 Privacy Impact and Risk Assessment, states:

The organization:

- a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and
- b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, AT-3 Role-Based Security Training, states:

The organization provides role-based security training to personnel with assigned security roles and responsibilities:

- a. Before authorizing access to the information system or performing assigned duties;
- b. When required by information system changes; and
- c. [Assignment: organization-defined frequency] thereafter.

Cause:

EEOC OIT did not monitor security controls over the SharePoint system to ensure that operational and security controls are in place and operating effectively to protect sensitive and PII information maintained at the owner's SharePoint sites.

Effect:

The effect of not monitoring security controls over SharePoint increases the risk of unauthorized use, disclosure, disruption, modification, or destruction of EEOC's data, causing EEOC to lose the ability to provide confidentiality, integrity, and availability of data.

Recommendation 1:

We recommend EEOC OIT conduct a privacy impact assessment of the SharePoint system to identify privacy issues and risks associated with the security settings; and to provide recommendations to mitigate potential privacy risk.

Recommendation 2:

We recommend EEOC OIT provide specialized training for SharePoint administrators and users to reduce the risk of exposing sensitive information and PII.

Management's Response:

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

OIT acknowledges this finding and recommendation. OIT has implemented technical and managerial controls to limit data exposure thus also preventing users from storing unencrypted sensitive and PII data (SPII) on untrusted public SharePoint locations. OIT intends to further implement the data loss prevention (DLP) controls within its Office 365 subscriptions, bolstered by the FY 2020 deployment of AvePoint as an operational governance toolset. Once implemented, OIT will update policy documents and provide training to administrators and end-users who manage SPII on the new governance process and protections.

Additionally, OIT is further implementing secure repositories for sensitive data within SharePoint, including for the purposes of receiving and sharing this data with external

parties. These repositories include DLP policies to monitor and automatically protect sensitive information, including implementing controls that regulate the download of sensitive data. The use of secured SharePoint repositories will significantly diminish the risk of exposure of sensitive data.

By improving data safeguards and reducing the need to use removable media, OIT believes it can resolve the finding and improve the services provided to the program offices.

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

Auditor's Evaluation of Management's Response

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

However, management's response did not address Recommendation 1 to conduct a privacy impact assessment of the SharePoint system. A Privacy Impact Assessment will address the general privacy risks involved in using SharePoint.

Also, management's response did not address Recommendation 2 to provide specialized training for SharePoint administrators and users. Before gaining access to the system, agency staff should complete a SharePoint training. The training regarding privacy and security may also train staff on how to use SharePoint's access controls to restrict access, on a group or user-level, to SharePoint sites, document libraries, and specific documents.

Finding 2: EEOC OIT needs to remediate internal vulnerabilities on its network.
--

Condition

We performed an internal vulnerability assessment on EEOC's internal computer networks on August 19, 2019. The internal vulnerability assessment consisted of an automated assessment of 3,275 Internet or Intranet connected assets, including firewalls, routers, web and mail servers and other hosts residing within the provided IP address range. The assets scanned had 207 occurrences of 17 critical-severity vulnerabilities, 102 occurrences of 20 high-severity vulnerabilities, and 266 occurrences of 24 medium-severity vulnerabilities. From a scale of 0 to 4.0, with 4.0 being the highest, the overall assessment of EEOC's network security posture for all assets was 2.64 (B-). The overall rating was based on the average rating values of each asset scanned. The result of the vulnerability assessment indicates that EEOC controls were not consistently implemented to remediate internal vulnerabilities on its network.

Criteria:

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

The organization:

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

Cause:

EEOC's lacks remediation controls to address known vulnerabilities.

The results of the 17 critical-severity vulnerabilities include, but are not limited to, the result of: (1) default passwords; (2) unpatched systems; (3) no passwords; (4) guessable credentials; (5) no authentication; and (6) default credential.

The results of the 20 high-severity vulnerabilities include, but are not limited to, the result of: (1) no password; (2) end-of-life applications; (3) weak configurations; (4) trust authentication; (5) debugging agent accessible; and (6) SQL credentials.

The results of the 24 medium-severity vulnerabilities include, but are not limited to, the result of: (1) default communities; (2) password hash disclosures; (3) header using user supplied values; (4) unpatched systems; and (5) parsing vulnerability.

Effect:

Unmitigated vulnerabilities on EEOC's network compromise the confidentiality, integrity, and availability of EEOC's data. For example:

- an attacker may leverage known issues to execute arbitrary code;
- agency employees may be unable to access systems; and
- agency data may be compromised.

Recommendation 3:

We recommend EEOC OIT review and remediate critical-risk, high-risk and medium-risk vulnerabilities in accordance with EEOC OIT's assessment of risk. If the risk is not remediated then we recommend EEOC OIT document the acceptance of the risk.

Management's Response:

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

OIT concurs with this finding and recommendation. OIT has made progress in remediating vulnerabilities, and will investigate options to further validate and remediate these findings using technology. As an example, OIT is planning to implement a Governance, Risk and Compliance (GRC) solution to improve risk monitoring, as well as documenting risk decisions to include acceptance.

OIT will seek to increase efficiencies in (1) evaluating current vulnerability remediation lifecycles as well as scenarios which affect these lifecycles; (2) exploring vulnerability management timelines and remediation procedures; and (3) drafting, approving and implementing improved vulnerability management standard operating procedures (SOP) within the GRC solution.

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

Auditor's Evaluation of Management's Response

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

Finding 3: EEOC OIT needs to enforce its mobile device management compliance policies.

Condition:

EEOC OIT uses Microsoft Intune cloud-based mobile device management tool to allow enrolled mobile devices access to certain applications. Intune provides secure, real-time synchronization of emails, calendars, and contacts to and from mobile devices. Intune allows mobile devices (e.g. cell phones and tablets) to download and store data from agency's emails and applications. EEOC OIT has configured Intune to check security requirements based on a specified time (30 days) in which devices must report the status for all received compliance policies. Mobile devices that do not return status within this time period are treated as noncompliant. During our testing, the OIT identified 332 of 1,323 enrolled mobile devices that were noncompliant.

Criteria:

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

All components should be updated with the latest available patches and configured following sound security practices. The organization should also take basic measures to prevent the user from circumventing the device's security features. Also, jailbroken or rooted mobile devices should be automatically detected to prohibit their use, for cases in which detection is feasible.

Cause:

EEOC OIT lacks a process for enforcing its mobile device management compliance policies and reporting noncompliance to the user and OIT senior management.

Effect:

The effect of EEOC OIT not enforcing its mobile device management compliance policies increases the risk of unauthorized access to EEOC's information and information systems.

Recommendation 4:

We recommend EEOC OIT enforce its mobile device management compliance policies for all enrolled mobile devices and report noncompliance to the user and OIT senior management for corrective action.

Management's Response:

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

OIT concurs with and acknowledges this finding and recommendation. OIT has made significant progress in resolving this finding and will continue forward until it is resolved. During the observation portion of the assessment, auditors viewed mobile device

management (MDM) settings that could be secured further, which OIT has executed. The corrective actions resulted in an over 85% reduction in non-compliant devices. Of the non-compliant devices secured, they were largely either: lacking a compliant password; had not been used within the last 90 days; or the device operating system and/or patch level was below the minimum compliance level.

Supplementary managerial policies which affect control settings will be explored with Agency leadership. Government furnished equipment (GFE) which has been unused within reasonable use periods will be retrieved from users while personal electronic devices (PED) accessing Agency data has already been restricted to assets meeting compliance criteria.

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

Auditor's Evaluation of Management's Response:

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

<p>Finding 4: EEOC OIT needs to develop an action plan to address the SECURE Technology Act requirements.</p>
--

Condition:

EEOC OIT has developed an Enterprise Risk Management (ERM) Policy Handbook that provides processes and steps toward a mature ERM program, but does not address supply chain risk management. EEOC OIT has not developed an action plan and outlined its processes to address a supply chain risk management strategy and related policy and procedural requirements of the SECURE Technology Act.

Criteria:

Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act or the SECURE Technology Act, states:

Title II--Federal Acquisition Supply Chain Security
SEC. 204. FISMA Act, (a) (2) (c) adds agency responsibilities relating to assessing and avoiding, mitigating, transferring, or accepting supply chain risks and complying with exclusion and removal orders.

NIST SP 800-161 *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, provides:

Guidance to federal agencies on identifying, assessing, selecting, and implementing risk management processes and mitigating controls throughout their organizations to help manage Information and Communications Technology (ICT) supply chain risks.

NIST SP 800-161, states:

Federal agencies are concerned about the risks associated with information and communications technology (ICT) products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the ICT supply chain. These risks are associated with the federal agencies' decreased visibility into, understanding of, and control over how the technology that they acquire is developed, integrated and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services.

Cause:

EEOC OIT has not allocated resources to develop an action plan to address related policy and procedural requirements of the SECURE Technology Act.

Effect:

The lack of a supply chain risk management strategy increases risks associated with information and communications technology products and services.

The effect of not developing an action plan for a supply chain risk management strategy reduces management's ability to respond to supply chain needs resulting from natural disasters, counterfeit products, theft, supplier delay, production interruptions, part shortages, and cyber security events.

Recommendation 5:

We recommend EEOC OIT develop an action plan to address related policy and procedural requirements of the SECURE Technology Act.

Management's Response:

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

EEOC acknowledges that supply chain management is not specifically referenced in its Enterprise Risk Management (ERM) Handbook, nor in operational policy and procedures. However, supply chain risks have been considered when developing Agency risk registers and profiles. The Agency will address this finding by developing an action plan to specifically incorporate information and communications technology (ICT) product and service risks into current policy and procedural documents.

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

Auditor's Evaluation of Management's Response:

Management acknowledged the need for a supply chain risk management strategy. However, management did clearly address Recommendation 5 to develop an action plan to address related policy and procedural requirements of the SECURE Technology Act. SECURE Technology Act established new requirements for supply chain risk management. EEOC OIT should identify and update specific policies and procedures to gauge the agency's preparedness in addressing these new requirements.

Appendix A – Scope, Objective, Methodology and Criteria

Scope and Objective

We conducted this audit in accordance with generally accepted government auditing standards (GAGAS), as specified in the Government Accountability Office's *Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. The audit was designed to determine whether EEOC implemented selected security controls for certain information systems in support of FISMA.

Our overall objective was to evaluate EEOC's information security program and practices, as required by FISMA. Specifically, we reviewed the status of the following areas of EEOC's information security program in accordance with DHS's FISMA Inspector General reporting requirements:

- Risk Management;
- Configuration Management;
- Identity, Credential, and Access Management;
- Data Protection and Privacy;
- Security Training;
- Information Security Continuous Monitoring;
- Incident Response; and
- Contingency Planning.

In addition, we evaluated the status of EEOC's IT security governance structure and the Agency's system security assessment and authorization (SA&A) methodology. We also followed-up on outstanding recommendations from prior FISMA audits (see Appendix B), and performed audits focused on EEOC's major information systems. The audit also included a vulnerability assessment of an EEOC-managed system and an evaluation of EEOC's process for identifying and mitigating technical vulnerabilities.

The audit was conducted at EEOC's headquarters in Washington, D.C., from May 16, 2019 through September 30, 2019. It covered the period from FY 2019 October 1, 2018, through September 30, 2019.

Methodology

We reviewed EEOC's general FISMA compliance efforts in the specific areas defined in DHS's guidance and the corresponding reporting instructions. We also audited an internal system and EEOC's SA&A process. We considered the internal control structure for EEOC's systems in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives. Accordingly, we obtained an understanding of the internal controls over EEOC's systems through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and

procedures. Our understanding of these systems' internal controls was used to evaluate the degree to which the appropriate internal controls were designed and implemented. When appropriate, we conducted compliance tests using judgmental sampling to determine the extent to which established controls and procedures are functioning as required.

To accomplish our audit objective, we:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA;
- Reviewed documentation related to EEOC's information security program, such as security policies and procedures, system security plans, and risk assessments;
- Tested system processes to determine the adequacy and effectiveness of selected security controls;
- Reviewed the status of recommendations in FY 2018 and FY 2017 FISMA audit reports;
- Completed a network vulnerability assessment of EEOC's sole internal system; and
- Reviewed SSAE 18 reports for Federal Shared Service Providers to determine the effectiveness of controls.

Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the set of internal controls for EEOC's systems taken as a whole.

Criteria

The criteria used in conducting this audit included:

- P.L. 113-283, FISMA;
- FY 2019 Inspector General FISMA Act of 2014 Reporting Metrics;
- NIST Cybersecurity Framework (version 1.1)
- NIST SP 800-12, Rev. 1, *An Introduction to Computer Security: The NIST Handbook*;
- NIST SP 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*;
- NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments*;
- NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*;
- NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*;
- NIST SP 800-39, *Managing Information Security Risk Organization, Mission, and Information System View*;
- NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*;
- NIST SP 800-124 Rev.1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*;
- NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*;

Criteria continued.

- Federal Cybersecurity Workforce Assessment Act of 2015;
- Federal Identity, Credential, and Access Management Roadmap Implementation Guidance;
- Federal Information Processing Standard (FIPS) Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*;
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*;
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*;
- OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*;
- SECURE Technology Act; and
- Other criteria as appropriate.

Appendix B - Status of Prior Findings

No.	Prior Year Audit Recommendations for FY 2018 ² and FY 2017 ³	Status	Auditor's Position on Status
1	FY 2018-01 FISMA audit recommendation No. 1: <i>We recommend the OIT employed an automated mechanism that ensures sensitive PII is encrypted on removable mobile media.</i>	Open	Agree
2	FY 2018-02 FISMA audit recommendation No. 2: <i>We recommend the OCHCO and OIT define and implement a process for conducting assessment of the knowledge, skills, and abilities of EEOC's cybersecurity workforce.</i>	Open	Agree
3	FY 2018-03 FISMA audit recommendation No. 3: <i>We recommend the OCHCO and OIT conduct a baseline assessment of the EEOC's cybersecurity workforce that includes (1) the percentage of personnel with IT, cybersecurity, or other cyber-related job functions who hold certifications; (2) the level of preparedness of other cyber personnel without existing credentials to take certification exams; and (3) a strategy for mitigating any gaps identified with appropriate training and certification for existing personnel.</i>	Open	Agree
4	FY 2018-03 FISMA audit recommendation No. 4: <i>We recommend the OIT review and remediate critical-risk, high-risk and moderate-risk vulnerabilities. These vulnerabilities should be resolved to avoid compromise to EEOC's systems; or the Agency should document acceptance of the risk or reclassification of the risk.</i>	Open	Agree
5	FY 2017 FISMA audit recommendation No. 1: <i>We recommend the OIT implement an automated solution to provide a centralized, enterprise-wide view of risk across the agency.</i>	Open	Agree

² The 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 2018 (report no. 2018-04-AOIG).

³ The 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 2017 (report no. 2017-07-AOIG).

No.	Prior Year Audit Recommendations for FY 2018 ² and FY 2017 ³	Status	Auditor's Position on Status
6	FY 2017 FISMA audit recommendation No. 2 <i>We recommend the EEOC Office of Information Technology develop and implement a Trusted Internet Connection (TIC) program in accordance with Office of Management and Budget (OMB) requirements to assist in protecting the Agency's network from cyber threats.</i>	Open	Agree
7	FY 2017 FISMA audit recommendation No. 3: <i>We recommend the OIT conduct an e-authentication risk assessment based on NIST SP 800-63-3 Digital Identity Guidelines suite, for EEOC's digital services, and fully implement multifactor authentication for logical and remote access enterprise-wide.</i>	Open	Agree

Appendix C – EEOC Management’s Comments




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

January 24, 2019

MEMORANDUM

TO: Milton Mayo, Inspector General

FROM: Jamell Fields, Chief Information Security Officer (CISO) 

SUBJECT: Office of Information Technology’s (OIT) Response to the FY 2019 Independent Evaluation of the EEOC’s Compliance with Provisions of the Federal Information Security Modernization Act (FISMA)

Digitally signed by JAMELL FIELDS
DN: cn=J.F., o=U.S. Government, ou=Equal
Employment Opportunity Commission,
cn=JAMELL FIELDS,
0.9.2342.19200300.100.1.1=45001003673096
Date: 2020.01.24 15:22:12 -0500

Below are OIT’s responses to the draft findings and recommendations outlined in the above referenced evaluation. Please feel free to contact me at jamell.fields@eeoc.gov or 202.663.4446 if you have any questions related to our responses.

FINDING/RECOMMENDATIONS:**1. Finding: EEOC OIT needs to check security controls over SharePoint.**

Recommendation 1: We recommend EEOC OIT conduct a privacy impact assessment of the SharePoint system to identify privacy issues and risks associated with the security settings; and to provide recommendations to mitigate potential privacy risk.

Response: OIT acknowledges this finding and recommendation. OIT has implemented technical and managerial controls to limit data exposure thus also preventing users from storing unencrypted sensitive and PII data (SPII) on untrusted public SharePoint locations. OIT intends to further implement the data loss prevention (DLP) controls within its Office 365 subscriptions, bolstered by the FY 2020 deployment of AvePoint as an operational governance toolset. Once implemented, OIT will update policy documents and provide training to administrators and end-users who manage SPII on the new governance process and protections.

Additionally, OIT is further implementing secure repositories for sensitive data within SharePoint, including for the purposes of receiving and sharing this data with external parties. These repositories include DLP policies to monitor and automatically protect sensitive information, including implementing controls that regulate the download of sensitive data. The use of secured SharePoint repositories will significantly diminish the risk of exposure of sensitive data.

By improving data safeguards and reducing the need to use removable media, OIT believes it can resolve the finding and improve the services provided to the program offices.

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

SUBJECT: OIT's Response to the FY 2019 Independent Evaluation of the EEOC's Compliance with Provisions of the Federal Information Security Modernization Act (FISMA)

2. Finding: The OIT needs to analyze and resolve internal vulnerabilities.

Recommendation 2: We recommend EEOC OIT review and remediate critical-risk, high-risk and medium-risk vulnerabilities by EEOC OIT's assessment of risk. If the risk is not remediated, then we recommend EEOC OIT document the acceptance of the risk.

Response: OIT concurs with this finding and recommendation. OIT has made progress in remediating vulnerabilities, and will investigate options to further validate and remediate these findings using technology. As an example, OIT is planning to implement a Governance, Risk and Compliance (GRC) solution to improve risk monitoring, as well as documenting risk decisions to include acceptance.

OIT will seek to increase efficiencies in (1) evaluating current vulnerability remediation lifecycles as well as scenarios which affect these lifecycles; (2) exploring vulnerability management timelines and remediation procedures; and (3) drafting, approving and implementing improved vulnerability management standard operating procedures (SOP) within the GRC solution.

3. Finding: EEOC OIT needs to enforce its mobile device management (MDM) compliance policies.

Recommendation 3: We recommend EEOC OIT enforce its mobile device management compliance policies for all enrolled mobile devices and report noncompliance to the user and OIT senior management for corrective action.

Response: OIT concurs with and acknowledges this finding and recommendation. OIT has made significant progress in resolving this finding and will continue forward until it is resolved. During the observation portion of the assessment, auditors viewed mobile device management (MDM) settings that could be secured further, which OIT has executed. The corrective actions resulted in an over 85% reduction in non-compliant devices. Of the non-compliant devices secured, they were largely either: lacking a compliant password; had not been used within the last 90 days; or the device operating system and/or patch level was below the minimum compliance level.

Supplementary managerial policies which affect control settings will be explored with Agency leadership. Government furnished equipment (GFE) which has been unused within reasonable use periods will be retrieved from users while personal electronic devices (PED) accessing Agency data has already been restricted to assets meeting compliance criteria.

SUBJECT: OIT's Response to the FY 2019 Independent Evaluation of the EEOC's Compliance with Provisions of the Federal Information Security Modernization Act (FISMA)

4. Finding: EEOC OIT needs to develop an action plan to address the SECURE, Technology Act requirements.

Recommendation 4: We recommend EEOC OIT develop an action plan to address related policy and procedural requirements of the SECURE Technology Act.

Response: EEOC acknowledges that supply chain management is not specifically referenced in its Enterprise Risk Management (ERM) Handbook, nor in operational policy and procedures. However, supply chain risks have been considered when developing Agency risk registers and profiles. The Agency will address this finding by developing an action plan to specifically incorporate information and communications technology (ICT) product and service risks into current policy and procedural documents.

cc: Bryan Burnett, CIO
Pierrette McIntire, DCIO
Greg Frazier, OIG