U.S. Equal Employment Opportunity Commission
Federal Information Security Modernization Act of 2014 (FISMA)
Fiscal Year 2018 Independent Evaluation

For Fiscal Year 2018
2018-004-AOIG

Prepared by:

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

March 6, 2019

U.S. Equal Employment Opportunity Commission
Federal Information Security Modernization Act of 2014 (FISMA)
Fiscal Year 2018 Independent Evaluation

Table of Contents

BROWN & COMPANY

CERTIFIED PUBLIC ACCOUNTANTS AND MANAGEMENT CONSULTANTS, PLLC

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). The EEOC Office of Inspector General (OIG) contracted with Brown & Company CPAs and Management Consultants, PLLC's (Brown & Company) to conduct an audit of EEOC's information security program and practices.

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 a 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 6 information systems. As part of our audit, we responded to the Department of Homeland Security's (DHS) *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics V 1.0,* dated April 11, 2018, and assessed the maturity levels on behalf of the EEOC OIG.

Brown & Company's methodology for the FY 2018 FISMA performance audit included testing the EEOC's systems for compliance with selected 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.*

We considered the internal control structure for various 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 found that 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 generally compliant with the FISMA legislation and applicable Office of Management and Budget (OMB) guidance and the security controls tested demonstrated operating effectiveness.

Our report identifies the following three findings where the EEOC's information security program can better protect the confidentiality, integrity, and availability of its information and information systems:

1. The Office of Information (OIT) has not employed an automated mechanism that ensures full-encryption of sensitive data and Personally Identifiable Information (PII) on mobile devices.
2. The Office Chief Human Capital Officer (OCHCO) and OIT need to conduct a baseline assessment of the EEOC's cybersecurity workforce.
3. The OIT needs to analyze and resolve internal vulnerabilities.

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

This performance audit did not constitute an audit of financial statements in accordance with GAGAS. Brown & Company was not engaged to, and did not, render an opinion on EEOC's internal controls over financial reporting or financial management systems. Furthermore, the projection of any conclusions based on our findings to future periods is subject to the risk that controls may become inadequate due to changes in conditions or the deterioration of compliance with controls.

This report is intended solely for the information and use of the management of EEOC, EEOC OIG, and the U.S. Congress, and is not intended to be, and should not be, used by anyone other than these specified parties.

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

Greenbelt, Maryland
February 27, 2019

1. Executive Summary

For Fiscal Year (FY) 2018, 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.

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

Overall Assessment of EEOC's Information Security Program

Based on the results of our audit, Brown & Company concluded that EEOC's information security program is generally compliant with the FISMA legislation and applicable Office of Management and Budget (OMB) guidance. EEOC continues to make positive strides in addressing information security weaknesses. We found that EEOC's information security programs is effective and provide reasonable assurance of adequate security.

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

1. The OIT has not employed an automated mechanism that ensures full-encryption of sensitive data and Personally Identifiable Information (PII) on mobile devices.
2. The OCHCO and OIT need to conduct a baseline assessment of the EEOC's cybersecurity workforce.
3. The OIT needs to analyze and resolve internal vulnerabilities.

In addition, as illustrated in **Appendix A**, three findings reported in last year's audit have not been fully implemented, and therefore, new recommendations were not made regarding these findings.

2. Background

The EEOC Overview

The U.S. Equal Employment Opportunity Commission (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 Federal Information Security Modernization Act of 2014

On December 18, 2014, President Obama signed the Federal Information Security Modernization Act (FISMA) of 2014, a bill that reformed the FISMA of 2002. The 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 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 7 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 OMB the "Inspector General FISMA Reporting Metrics" that depicts the effectiveness of the agency's information security program.

On July 27, 2016, OMB released a revised Circular A-130, *Managing Federal Information as a Strategic Resource*. This revised circular continues to establish minimum requirements for federal information security programs, assigns responsibilities for the security of information, and information systems to the agency's CIO and others. The revised Circular A-130 adopts the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and the NIST Cybersecurity Framework, requiring agencies to perform ongoing re-authorizations of systems and replace the triennial reauthorization process to better protect agency information and information systems. In certain areas, the revised Circular A-130 expands upon a minimum set of security controls required in NIST Special Publication (SP) 800-53, Revision (Rev.) 4. Specifically, the revised Circular A-130 adds requirements for moderate and high-impact systems to have PII encrypted at rest and in transit and instructs federal agencies to periodically test response procedures and document lessons-learned to improve incident response.

3. 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 6 information systems. As part of our audit, we responded to the Department of Homeland Security's (DHS) FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics V 1.0, dated April 11, 2018, and assessed the maturity levels on behalf of the EEOC OIG.

4. Audit Scope

The scope of this performance audit is to determine the effectiveness and efficiency of EEOC's information security program and practices, and whether EEOC meets the requirements of FISMA. In assessing EEOC's adherence with FISMA, the following **Exhibit 1** NIST cybersecurity framework function areas and domains[1] were reviewed:

Exhibit 1 – FY 2018 IG FISMA Reporting Metrics

NIST Cybersecurity Framework Functions	**NIST Cybersecurity Framework Domains**
Identify Function Area	Risk Management
Protect Function Area	Configuration Management
	Identify and Access Management

[1] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, National Institute of Standards and Technology, February 12, 2014, defines the NIST functions and categories.

NIST Cybersecurity Framework Functions	NIST Cybersecurity Framework Domains
	Data Protection and Privacy
	Security Training
Detect Function Area	Information Security Continuous Monitoring (ISCM)
Respond Function Area	Incident Response
Recover Function Area	Contingency Planning

The FY 2018 IG FISMA Reporting Metrics require IGs to assess the effectiveness of its information security programs on a maturity model spectrum, in which the foundational levels ensure that agencies develop sound policies and procedures and the advanced levels capture the extent that agencies institutionalize those policies and procedures. **Exhibit 2** details the five maturity model levels: ad hoc, defined, consistently implemented, managed and Measurable, and optimized.

Exhibit 2– 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.

The period covered by this performance audit is October 1, 2017 to September 30, 2018. The work was performed in accordance with generally accepted government auditing standards (GAGAS).

The scope includes reviewing the effectiveness of EEOC's information security program and evaluating the following information systems:

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

5. Testing Methodology

Brown & Company's testing methodology included: interviews with EEOC management and staff review of legal and regulatory requirements, performance of audit procedures, and review of documentation relating to EEOC's information security program. We utilized the Final FY 2018 IG FISMA Metrics V 1.0 maturity model[2] to assess the maturity of the organization's information system security program. See **Appendix B**: *FY 2018 Inspector General FISMA Metrics Results* for details.

6. Summary of Results

FISMA requires each federal agency to develop and implement an agency-wide information security program to address security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another organization, contractor, or other source. In addition, FISMA requires each agency's Inspector General (IG) to conduct an independent evaluation to determine the effectiveness of the information security program and practices of its respective agency.

On behalf of the OIG, Brown & Company has assessed the effectiveness of EEOC information system security controls and identified weaknesses. We found that the EEOC's information security program is generally in compliance with FISMA legislation and OMB guidance, and it provides reasonable assurance of adequate security.

We found that EEOC's information security program has an overall maturity level of "Managed and Measurable" based on the FY 2018 DHS IG FISMA Cyberscope Metric functions against the criteria listed below. **Exhibit 3** provides our overall assessment of EEOC's maturity level by function area. **Exhibit 2** above provides DHS maturity level criteria.

Exhibit 3 – EEOC Overall Maturity Level Assessment by Functions Area

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

[2] FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics V 1.0, April 11, 2018.

In conducting our audit work, Brown & Company identified the following three findings related to EEOC's information security program that can be improved:

1. The OIT has not employed an automated mechanism that ensures full-encryption of sensitive data and Personally Identifiable Information (PII) on mobile devices.
2. The OCHCO and OIT need to conduct a baseline assessment of the EEOC's cybersecurity workforce.
3. The OIT needs to analyze and resolve internal vulnerabilities.

7. Findings and Recommendations

The results of our audit identified areas in EEOC's information security program that need improvement. The three findings and four recommendations are discussed below.

Finding 1: The OIT has not employed an automated mechanism that ensures full-encryption of sensitive data and Personally Identifiable Information (PII) on mobile devices.

Condition:

The Office of Information Technology (OIT) has not employed an automated mechanism that ensure full-encryption of Personally Identifiable Information (PII) on mobile devices. Specifically, EEOC cannot prevent users from storing unencrypted sensitive and PII data on untrusted mobile devices such as USB drives.

Criteria:

NIST Special Publication 800-53, Revision 4, *"Security and Privacy Controls for Federal Information Systems and Organizations, Ac-19(5) Access Control For Mobile Devices | Full Device / Container-Based Encryption,"* states:

> The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].

EEOC Policy for Personally Identifiable Data Extracts Removed from EEOC Premises, states the following:

> In order to remove data extracts containing sensitive PII from EEOC premises, users must:
>
> > ***
> >
> > Encrypt and password-protect all sensitive PII data extracts maintained on a portable storage device (such as CD, memory key, flash drive, etc.). Exceptions due to technical limitations must have the approval of the Office Director and alternative protective measures must be in place prior to removal from EEOC premises.

Cause:

EEOC has not fully implemented access control for mobile devices due to lack of resources.

Effect:

The effect of not employing an automated mechanism to ensure PII is fully encrypted on mobile devices increases the risk of unauthorized access and confidentially.

Recommendation 1:

We recommend the OIT employed an automated mechanism that ensures sensitive PII is encrypted on removable mobile media.

Management's Response:

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

> *OIT agrees with this finding. OIT intends to further implement the data loss prevention (DLP) controls within its Office 365 subscriptions, bolstered by the deployment of Windows 10, to better protect sensitive data from exfiltration. In addition, OIT also is in the process of implementing secure repositories for sensitive data within SharePoint, including for the purposes of receiving and sharing this data with external parties.*

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 recommendation. Management should ensure its' implementation of corrective actions will reduce the risk of unencrypted sensitive data and PII stored on mobile devices.

Finding 2: The OCHCO and OIT need to conduct a baseline assessment of the EEOC's cybersecurity workforce.

Condition

The Office of Chief Human Capital Officer (OCHCO) and Office of Information Technology (OIT) have not fully implemented a process for conducting assessment of the knowledge, skills, and abilities of EEOC's cybersecurity workforce.

The OCHCO initiated a workforce assessment that consisted of a multiyear approach for assessing EEOC's workforce. The OCHCO conducted an on-line survey disseminated EEOC-wide that focused on e-learning and the types of professional development and training needed. However, the OCHCO and OIT have not fully developed and implemented an information security workforce development and improvement program. The OCHCO and OIT did not conduct a baseline assessment of 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.

Criteria

NIST Special Publication 800-53, Revision 4, ***Security and Privacy Controls for Federal Information Systems and Organizations*****, PM-13 "Information Security Workforce,"** states:

> The organization establishes an information security workforce development and improvement program.
>
> > Supplemental Guidance: Information security workforce development and improvement programs include, for example: (i) defining the knowledge and skill levels needed to perform information security duties and tasks; (ii) developing role-based training programs for individuals assigned information security roles and responsibilities; and (iii) providing standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions. Such workforce programs can also include associated information security career paths to encourage: (i) information security professionals to advance in the field and fill positions with greater responsibility; and (ii) organizations to fill information security-related positions with qualified personnel. Information security workforce development and improvement programs are complementary to organizational security awareness and training programs. Information security workforce development and improvement programs focus on developing and institutionalizing core information security capabilities of selected personnel needed to protect organizational operations, assets, and individuals.

NIST SP 800-181, ***National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework***

Use of the NICE Framework's common lexicon enables employers to inventory and develop their cybersecurity workforce. The NICE Framework can be used by employers and organizational leadership to:

- Inventory and track their cybersecurity workforce to gain a greater understanding of the strengths and gaps in Knowledge, Skills, and Abilities (KSAs) and Tasks performed;
- Identify training and qualification requirements to develop critical KSAs to perform cybersecurity Tasks;
- Improve position descriptions and job vacancy announcements selecting relevant KSAs and Tasks, once work roles and tasks are identified;
- Identify the most relevant work roles and develop career paths to guide staff in gaining the requisite skills for those roles; and
- Establish a shared terminology between hiring managers and human resources (HR) staff for the recruiting, retention, and training of a highly-specialized workforce.

Federal Cybersecurity Workforce Assessment Act of 2015

> This bill requires federal agencies to: (1) identify all personnel positions that require the performance of information technology, cybersecurity, or other cyber-related functions; and (2) assign a corresponding employment code to such positions using a coding structure that the National Institute of Standards and Technology must include in the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework.
>
> ***
>
> Federal agencies must submit to Congress a report identifying: (1) the percentage of personnel with such job functions who currently hold industry-recognized certifications, (2) the preparedness of other civilian and non-civilian cyber personnel without existing credentials to pass certification exams, and (3) a strategy for mitigating any identified gaps with training and certification for existing personnel.
>
> The agencies must establish procedures to identify all encumbered and vacant positions with such functions and assign the appropriate employment code to each position.
>
> Annually through 2022, the agencies must submit a report to the OPM that identifies cyber-related roles designated as critical needs in the agency's workforce. The OPM must provide agencies with guidance for identifying roles with acute and emerging skill shortages.
>
> ***

Cause

EEOC lacks an effective process to implement an information security workforce development and improvement program to supports its security awareness and training program.

Effect

EEOC has not complied with the Federal Cybersecurity Workforce Assessment Act of 2015. The lack of a full cybersecurity workforce assessment increases the risk that cybersecurity workforce requirements are not aligned with the EEOC's Strategic Plan. In addition, OCHCO and OIT will not have the mechanism to identify gaps between the current and future workforce competencies.

Recommendation 2

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.

Recommendation 3:

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.

Management's Response

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

> *OIT agrees with this finding. OIT plans to partner with OCHCO to ensure EEOC compliance with The Federal Cybersecurity Workforce (CSWF) Act of 2015. EEOC will evaluate current position descriptions (PD) for existing OIT personnel and assess against current role requirements while considering the National Initiative for Cybersecurity Education (NICE) framework.*

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. Effective implementation of the recommendation to conduct a baseline assessment to evaluate current position descriptions (PD) for existing OIT personnel and assess against current role requirements while considering the National Initiative for Cybersecurity Education (NICE) framework support EEOC's complies with CSWF Act of 2015.

Finding 3: The OIT needs to analyze and resolve internal vulnerabilities.

Condition

An Internal Vulnerability Assessment was performed on EEOC's internal computer networks on September 22, 2018 by Digital Defense Inc. on Brown & Company's behalf. The Internal Vulnerability Assessment consisted of an automated assessment of 3,122 Internet or Intranet connected assets, including firewalls, routers, web and mail servers and other hosts residing within the provided IP address range. The assessment found occurrences of critical, high and medium risk 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 3.21 (B+). The overall rating is based on the average rating values of each asset scanned. EEOC should analyze and resolve the critical, high and medium risk vulnerabilities as a priority.

Criteria:

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

The organization:

a. Scans for vulnerabilities in the information system and hosted applications frequently and/or randomly in accordance with procedures and when new vulnerabilities potentially affecting the system/applications are identified and reported;

b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
   1. Enumerating platforms, software flaws, and improper configurations;
   2. Formatting checklists and test procedures; and
   3. Measuring vulnerability impact;

c. Analyzes vulnerability scan reports and results from security control assessments;

d. Remediates legitimate vulnerabilities response times in accordance with an organizational assessment of risk; and

e. Shares information obtained from the vulnerability scanning process and security control assessments with personnel or roles to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

<u>Cause:</u>

The results of the critical vulnerabilities were the result of: (1) default passwords; (2) unpatched systems; (3) no passwords; (4) guessable credentials; (5) weak SSL; and (6) default credential.

The results of the high vulnerabilities were the result of: (1) no password; (2) end-of-life applications; (3) weak configurations; (4) authentication bypass; (5) XXE injection; and (6) SQL injection. The results of the medium vulnerabilities were the result of: (1) default passwords; (2) password hash disclosures; (3) no passwords; (4) unpatched systems; and (5) weak configurations.

<u>Effect:</u>

The effects of critical, high and medium risk vulnerabilities if exploited, an attacker will gain complete control of the asset. Critical level vulnerabilities are known to have publicly accessible exploits which require little to no expert knowledge to use. The effect of high-risk vulnerabilities, an attacker could gain user or administrative access to the asset and be able to run commands, access or delete files, and launch attacks against other assets. The effect of medium-risk vulnerabilities, an attacker would gain valuable information about the asset, which would aid in gaining access.

<u>Recommendation 4:</u>

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.

<u>Management's Response:</u>

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

> *OIT concurs with this finding and recommendation.*

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

<u>Auditor's Evaluation of Management's Response</u>

Management agrees with the finding and recommendation. Effective implementation of the recommendation to evaluate current vulnerability remediation lifecycles as well as scenarios which affect this lifecycle will ensure current vulnerabilities are remediated.