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

Office of Inspector General

March 6, 2019

MEMORANDUM

TO: Victoria A. Lipnic
Acting Chair

FROM: Milton A. Mayo Jr.
Inspector General

SUBJECT: Federal Information Security Modernization Act of 2014 (FISMA) Fiscal Year 2018 Independent Evaluation (OIG Report Number 2018-004-AOIG)

Attached, please find the final report Federal Information Security Modernization Act of 2014 (FISMA) Fiscal Year 2018 Independent Evaluation. We appreciate your assistance and cooperation in conducting this review. The contractor integrated your responses to the draft report into the final report.

We will conduct the exit conference on Wednesday, March 13th at 2:00 p.m. in conference room 6NE17G. Staff from Brown and Company, PLLC will discuss the results of the Independent Evaluation. If you cannot attend, please designate someone to attend on your behalf. If you have any questions, contact Gregory Frazier, OIG Contracting Officer Technical Representative at 202-663-4373, or Gregory.Frazier@EEOC.GOV.

Thank you for your assistance.

cc: Donald McIntosh
Chief of Staff

Reuben Daniels, Jr.
Chief Operating Officer (Acting)

Mona Papillon
Deputy Chief Operating Officer

Bryan Burnett
Chief Information Officer

Jamell Fields
Chief Information Security Officer

Attachment

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

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).

Cause:

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.

Effect:

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.

Recommendation 4:

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.

Management's Response:

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.**

Auditor's Evaluation of Management's Response

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.

8. Appendix A - Status of Prior Year Findings

No.	FY 2017[3] Audit Recommendations	Status	Auditor's Position on Status
1	**FY 2017 FISMA audit recommendation No. 1:** *We recommend the OIT implement an automated solution to provide a centralized, enterprise-wide view of risk across the agency.*	Open	Agree
2	**FY 2017 FISMA audit recommendation No. 2** *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.*	Open	Agree
3	**FY 2017 FISMA audit recommendation No. 3:** *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.*	Open	Agree
4	**FY 2017 FISMA audit recommendation No. 4:** *We recommend that EEOC establish a separate position for the Deputy Chief Information Security Officer and Chief Information Security Officer (CISO) as additional resources to meet Federal information system security program requirements and reduce the risk of conflict in managing operations and security risk.*	Closed	Agree

[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 2017-07-AOIG.*

9. Appendix B – FY 2018 Inspector General FISMA Metrics Results

Function 0.01: Overall Assessment on Effectiveness

The overall assessment rating for EEOC information system programs are effective.

Function 0.02: Overall Assessment of EEOC Information System Program.

Assessment Scope

We assessed the EEOC's security control effectiveness to the extent which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies.

Summary on the Information System Program Effectiveness

Summary on the Information System Program Effectiveness

We utilized the Final FY 2018 Inspector General FISMA Metrics v1.0 maturity model to access the maturity of the EEOC's information system security program. The metrics include eight functional areas and related category. Ratings throughout the eight function areas were by a simple majority, where the most frequent level (i.e., the mode) across the questions served as the function area rating. For example, if there are seven questions in a function area, and the EEOC received defined ratings for three questions and managed and Measurable ratings for four questions, then the function area rating is managed and Measurable.

The overall assessment of the EEOC information system program is "Level 4: Managed and Measurable." EEOC information system grogram could be improve by developing qualitative and quantitative performance measures and metrics in the areas of Protect and Recover. "Managed and Measurable," is considered to be an effective level of security at the domain, functions, and overall program level.

Exhibit 4 – EEOC Overall Maturity Level Assessment by Functions Area

Summary of FY 2018 Cyberscope Results	Maturity Level
1. Identify - Risk Management	Managed and Measurable
2. Protect - Configuration Management	Managed and Measurable
3. Protect - Identify and Access Management	Managed and Measurable
4. Protect- Data Protection & Privacy	Consistently Implemented
5. Protect - Security Training	Consistently Implemented
6. Detect - Information Security Continuous Monitoring	Managed and Measurable
7. Respond - Incident Response	Managed and Measurable
8. Recover - Contingency Planning	Consistently Implemented
Overall Effectiveness Rating	Managed and Measurable

The five maturity model levels are: ad hoc, defined, consistently implemented, managed and Measurable, and optimized.

Exhibit 5– 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 6 – EEOC Inspector General FISMA Reporting Metrics Results

For Official Use Only

Inspector General

Section Report

2018

Annual FISMA Report

Equal Employment Opportunity Commission

For Official Use Only

Function 1: Identify - Risk Management

1 To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third party systems), and system interconnections (NIST SP 800-53: CA-3, PM-5, and CM-8; OMB M-04-25; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2018 CIO FISMA Metrics: 1.1, 1.4, and 1.5)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not have an automated process to capture inventory data for all hardware and software components.

2 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-53: CA-7 and CM-8; NIST SP 800-137; Federal Enterprise Architecture (FEA) Framework, v2; FY 2018 CIO FISMA Metrics: 1.2)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not employ automation to track the life cycle of all hardware components.

3 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting (NIST SP 800-53: CA-7, CM-8, and CM-10; NIST SP 800-137; FEA Framework, v2)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not employ automation to track the life cycle of all software components.

4 To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions (NIST SP 800-53: RA-2, PM-7, and PM-11; NIST SP 800-60; CSF: ID.BE-3; FIPS 199; FY 2018 CIO FISMA Metrics: 1.1)?

Consistently Implemented (Level 3)

Comments: Met

5 To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that includes the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk (NIST SP 800-39; NIST SP 800-53: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; OMB M-16-17; Green Book (Principle #6); CFO Council ERM Playbook; OMB M-17-25; FY 2018 CIO FISMA Metrics: 1.6)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC's risk management program is not embedded into daily decision making across the organization and does not provide for continuous risk identification.

Function 1: Identify - Risk Management

6 To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain (NIST SP 800-39; FEA Framework; NIST SP 800-53: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-161; DHS Binding Operational Directive 17-01)?

Defined (Level 2)

Comments: The next level is not met because EEOC does not consistently implement its security architecture across the enterprise, business process, and system levels.

7 To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer/Senior Accountable Official for Risk Management, Chief Information Officer, Chief Information Security Officer, and other internal and external stakeholders and mission specific resources been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2; OMB A-123; CFO Council ERM Playbook)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC's risk management program does not address the full spectrum of an agency's risk portfolio across all organizational aspects.

8 To what extent has the organization ensured that plans of action and milestones (POA&Ms) are utilized for effectively mitigating security weaknesses (NIST SP 800-53: CA-5; OMB M-04-25)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not employ automation to correlate security weaknesses amongst information systems and identify enterprise-wide trends and solutions on a near real- time basis.

9 To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system level risk assessments, including for identifying and prioritizing
(i) internal and external threats, including through use of the common vulnerability scoring system, or other equivalent framework
(ii) internal and external asset vulnerabilities, including through vulnerability scanning,
(iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities, and
(iv) security controls to mitigate system-level risks (NIST SP 800-37; NIST SP 800-39; NIST SP 800-53: PL-2 and RA-1; NIST SP 800-30; CSF:ID.RA-1 – 6)?

Managed and Measurable (Level 4)

Comments: Met

Function 1: Identify - Risk Management

10 To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders (CFO Council ERM Playbook; OMB A-123; OMB Circular A-11; Green Book (Principles #9, #14 and #15))?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not employ robust diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of interrelated risks across the organization.

11 To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services (FAR Case 2007-004; Common Security Configurations; FAR Sections: 24.104, 39.101, 39.105, 39.106, and 52.239-1; President's Management Council; NIST SP 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; FY 2018 CIO FISMA Metrics: 1.5; Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)?

Managed and Measurable (Level 4)

Comments: Met

12 To what extent does the organization utilize technology (such as a governance, risk management, and compliance tool) to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123; CFO Council ERM Playbook)?

Defined (Level 2)

Comments: The next level is not met because EEOC has not implemented an automated solution across the enterprise that provides a centralized, enterprise wide view of risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards.

13.1 Please provide the assessed maturity level for the agency's Identify - Risk Management function.

Managed and Measurable (Level 4)

Comments: N/A

13.2 Provide any additional information on the effectiveness (positive or negative) of the organization's risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?

N/A

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 2A: Protect - Configuration Management

14 To what degree have the roles and responsibilities of configuration management stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53: CM-1; NIST SP 800-128: Section 2.4)?

Consistently Implemented (Level 3)

Comments: MET

15 To what extent does the organization utilize an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems (NIST SP 800-128: Section 2.3.2; NIST SP 800-53: CM-9)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not have an automated process to change cybersecurity landscape on a near real-time basis.

16 To what degree have information system configuration management policies and procedures been defined and implemented across the organization? (Note: the maturity level should take into consideration the maturity of questions 17, 18, 19, and 21) (NIST SP 800-53: CM-1; NIST SP 800-128: 2.2.1)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not actively adapt its configuration management plan and related processes and activities to a changing cybersecurity landscape to respond to evolving and sophisticated threats on a real-time basis.

17 To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53: CM-2 and CM-8; FY 2018 CIO FISMA Metrics: 1.1 and 2.2; CSF: ID.DE.CM-7)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC has not fully employ automated mechanisms to detect unauthorized hardware on its network.

18 To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53: CM-6, CM-7, and SI-2; FY 2018 CIO FISMA Metrics: 1.1 and 2.2; SANS/CIS Top 20 Security Controls 3.7)?

Optimized (Level 5)

Comments: MET

Function 2A: Protect - Configuration Management

19 To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53: CM-3 and SI-2; NIST SP 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20, Control 4.5; FY 2018 CIO FISMA Metrics: 2.13; and DHS Binding Operational Directive 15-01)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not utilize automated patch management and software update tools for all applications and network devices.

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-08-05)?

Ad Hoc (Level 1)

Comments: The next level is not met because EEOC does not participate in the DHS Trusted Internet Connections (TIC) Initiative.

21 To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate (NIST SP 800-53: CM-2 and CM-3)?

Managed and Measurable (Level 4)

Comments: MET

22 Provide any additional information on the effectiveness (positive or negative) of the organization's configuration management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?

N/A

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 2B: Protect - Identity and Access Management

23 To what degree have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53: AC-1, IA-1, and PS-1; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

Consistently Implemented (Level 3)

Comments: MET

Function 2B: Protect - Identity and Access Management

24 To what degree does the organization utilize an ICAM strategy to guide its ICAM processes and activities (FICAM)?

Defined (Level 2)

Comments: The next level is not met because EEOC has not consistently implemented its ICAM strategy to include stronger authentication (e.g. two-factors authentication).

25 To what degree have ICAM policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 26 through 31) (NIST SP 800-53: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; FY 2018 CIO FISMA Metrics: 2.3).

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC automated mechanism does not identify suspicious behavior and potential violations of its ICAM policies and procedures on a near-real time basis.

26 To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems (NIST SP 800-53: PS-2 and PS-3; National Insider Threat Policy; FY 2018 CIO FISMA Metrics: 2.16)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not evaluate personnel security information from various sources, and integrate this information with anomalous user behavior data and inside threat on a real-time basis.

27 To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems are completed and maintained (NIST SP 800-53: AC-8, PL-4, and PS-6)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not ensure that access agreements for privileged and non-privileged users are updated on a real-time basis.

28 To what extent has the organization implemented strong authentication mechanisms (two-factor PIV credential or other NIST 800-63 r3 Identity Assurance Level (IAL)3/ Authenticator Assurance Level (AAL) 3/ Federated Assurance Level (FAL) 3 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2018 CIO FISMA Metrics: 2.4; and Cybersecurity Sprint)?

Defined (Level 2)

Comments: The next level is not met because EEOC has not implemented strong authentication mechanisms (PIV) for non- privileged users of the organization's facilities and networks, including for remote access, in accordance with Federal targets.

Function 2B: Protect - Identity and Access Management

29 To what extent has the organization implemented strong authentication mechanisms (two-factor PIV credential or other NIST 800-63 r3 IAL 3/ AAL 3/ FAL 3 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2018 CIO FISMA Metrics: 2.5; and Cybersecurity Sprint)?

Defined (Level 2)

Comments: The next level is not met because EEOC has not implemented strong authentication mechanisms (PIV) for privileged users of the organization's facilities and networks, including for remote access, in accordance with Federal targets.

30 To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (FY 2018 CIO FISMA Metrics: 2.4 and 2.5; NIST SP 800-53: AC-1, AC-2 (2), and AC-17; CSIP)?

Managed and Measurable (Level 4)

Comments: MET

31 To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions (NIST SP 800-53: AC-17 and SI-4; and FY 2018 CIO FISMA Metrics: 2.10)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC has not configured it information systems to restrict individual's ability to transfer data accessed remotely to non-authorized devices.

32 Provide any additional information on the effectiveness (positive or negative) of the organization's identity and access management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?

N/A

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 2C: Protect - Data Protection and Privacy

Function 2C: Protect - Data Protection and Privacy

33 To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems (NIST SP 800-122; OMB M-18-02; OMB A-130, Appendix I; NIST SP 800-53: AR-4 and Appendix J)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not monitor and analyses quantitative and qualitative performance measures on the effectiveness of its privacy activities and uses that information to make appropriate adjustments as needed.

34 To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? (NIST SP 800-53; Appendix J, SC-8, SC-28, MP-3, and MP-6; FY 2018 CIO FISMA Metrics: 2.9 and 2.10)?

Encryption of data at rest
Encryption of data in transit
Limitation of transfer to removable media
Sanitization of digital media prior to disposal or reuse

Defined (Level 2)

Comments: The next level is not met because EEOC has not employed mechanism for the prevention and detection of untrusted removable media.

35 To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (NIST SP 800-53: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2018 CIO FISMA Metrics: 3.8 – 3.12)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not measure the effectiveness of its data exfiltration and enhanced network defenses by conducting exfiltration exercises.

36 To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events? (NIST SP 800-122; NIST SP 800-53: Appendix J, SE-2; FY 2018 SAOP FISMA metrics; OMB M-17-12; and OMB M-17-25)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not monitor and analyze its qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan, as appropriate.

Function 2C: Protect - Data Protection and Privacy

37 To what degree does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53: AR-5)? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC has not institutionalized a process of continuous improvement incorporating advanced privacy training practices and technologies.

38 Provide any additional information on the effectiveness (positive or negative) of the organization's data protection and privacy program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective?

N/A

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 2D: Protect - Security Training

39 To what degree have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated across the agency, and appropriately resourced? (Note: this includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities (NIST SP 800-53: AT-1; and NIST SP 800-50).

Consistently Implemented (Level 3)

Comments: MET

40 To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (NIST SP 800-53: AT-2 and AT-3; NIST SP 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS/SANS Top 20: 17.1)?

Ad Hoc (Level 1)

Comments: The next level is not met because EEOC has not defined a process for conducting assessment of the knowledge, skills, and abilities of its workforce.

Function 2D: Protect - Security Training

41 To what extent does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (Note: the strategy/plan should include the following components: the structure of the awareness and training program, priorities, funding, the goals of the program, target audiences, types of courses/material for each audience, use of technologies (such as email advisories, intranet updates/wiki pages/social media, web based training, phishing simulation tools), frequency of training, and deployment methods (NIST SP 800-53: AT-1; NIST SP 800-50: Section 3).

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans.

42 To what degree have security awareness and specialized security training policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 43 and 44 below) (NIST SP 800-53: AT-1 through AT-4; and NIST SP 800-50).

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training policies and procedures.

43 To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST SP 800-53: AT-2; FY 2018 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; SANS Top 20: 17.4).

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC has not institutionalized a process of continuous improvement incorporating advanced security awareness practices and technologies.

44 To what degree does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST SP 800-53: AT-3 and AT-4; FY 2018 CIO FISMA Metrics: 2.15)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not obtain feedback on its security training content and makes updates to its program, as appropriate.

Function 2D: Protect - Security Training

45.1 Please provide the assessed maturity level for the agency's Protect Function.

Consistently Implemented (Level 3)

Comments: N/A

45.2 Provide any additional information on the effectiveness (positive or negative) of the organization's security training program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the security training program effective?

N/A

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 3: Detect - ISCM

46 To what extent does the organization utilize an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organization-wide approach to ISCM (NIST SP 800-137: Sections 3.1 and 3.6)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC's ISCM strategy is not fully integrated with its risk management, configuration management, incident response, and business continuity functions.

47 To what extent does the organization utilize ISCM policies and procedures to facilitate organization-wide, standardized processes in support of the ISCM strategy? ISCM policies and procedures address, at a minimum, the following areas: ongoing assessments and monitoring of security controls; collection of security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and reviewing and updating the ISCM strategy (NIST SP 800-53: CA-7) (Note: The overall maturity level should take into consideration the maturity of question 49)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC's ISCM policies and procedures are not fully integrated with its risk management, configuration management, incident response, and business continuity functions.

48 To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53: CA-1; NIST SP 800-137; and FY 2018 CIO FISMA Metrics)?

Managed and Measurable (Level 4)

Comments: MET

Function 3: Detect - ISCM

49 How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls (NIST SP 800-137: Section 2.2; NIST SP 800-53: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; OMB M-14-03)?

Managed and Measurable (Level 4)

Comments: The next level is not met because the EEOC ISCM program IT security objectives and goals are not supported by cost-effective decision making that is based on cost, risk, and mission impact.

50 How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC is unable to integrate metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization.

51.1 Please provide the assessed maturity level for the agency's Detect - ISCM function.

Managed and Measurable (Level 4)

Comments: N/A

51.2 Provide any additional information on the effectiveness (positive or negative) of the organization's ISCM program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?

N/A

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 4: Respond - Incident Response

52 To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events (NIST SP 800-53: IR-1; NIST SP 800-61 Rev. 2; NIST SP 800-184; OMB M-17-25; OMB M-17-09; FY 2018 CIO FISMA Metrics: 4.1, 4.3, 4.6, and 5.3; Presidential Policy Direction (PPD) 41)? (Note: The overall maturity level should take into consideration the maturity of questions 53 - 58)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not monitor and analyze qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies, as appropriate.

Function 4: Respond - Incident Response

53 To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMB M-16-04; FY 2018 CIO FISMA Metrics: Section 4; and US-CERT Federal Incident Notification Guidelines)?

Managed and Measurable (Level 4)

Comments: MET

54 How mature are the organization's processes for incident detection and analysis? (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-18-02; and US-CERT Incident Response Guidelines)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not utilize profiling techniques to measure the characteristics of expected activities on its networks and systems to detect security incidents such as file integrity checking software for critical files.

55 How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not utilize dynamic reconfiguration to stop attacks, misdirect attackers, and to isolate components of systems.

56 To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-18-02; NIST SP 800-53: IR-6; US-CERT Incident Notification Guidelines; PPD-41; DHS Cyber Incident Reporting Unified Message)?

Managed and Measurable (Level 4)

Comments: MET

57 To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support (FY 2018 CIO FISMA Metrics: 4.4; NIST SP 800-86; NIST SP 800-53: IR-4; OMB M-18-02; PPD-41).

Managed and Measurable (Level 4)

Comments: MET

Function 4: Respond - Incident Response

58 To what degree does the organization utilize the following technology to support its incident response program?
Web application protections, such as web application firewalls
Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools
Aggregation and analysis, such as security information and event management (SIEM) products
Malware detection, such as antivirus and antispam software technologies
Information management, such as data loss prevention
File integrity and endpoint and server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2; NIST SP 800-44)

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not uses technologies for monitoring and analyzing qualitative and quantitative performance across the organization and collecting, analyzing, and reporting data on the effectiveness of its technologies for performing incident response activities.

59.1 Please provide the assessed maturity level for the agency's Respond - Incident Response function.

Managed and Measurable (Level 4)

Comments: N/A

59.2 Provide any additional information on the effectiveness (positive or negative) of the organization's incident response program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?

N/A

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 5: Recover - Contingency Planning

60 To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined and communicated across the organization, including appropriate delegations of authority (NIST SP 800-53: CP-1 and CP-2; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?

Consistently Implemented (Level 3)

Comments: MET

Function 5: Recover - Contingency Planning

61 To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and strategies, as appropriate (Note: Assignment of an overall maturity level should take into consideration the maturity of questions 62-66) (NIST SP 800-34; NIST SP 800-161; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5).

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC's information system contingency planning program is not fully integrated with the enterprise risk management program.

62 To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST SP 800-53: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17-09; FY 2018 CIO FISMA Metrics: 5.6)?

Consistently Implemented (Level 3)

Comments: MET

63 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST SP 800-53: CP-2; NIST SP 800-34; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC is unable to integrate metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans.

64 To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53: CP-3 and CP-4; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not employ automated mechanisms to more thoroughly and effectively test system contingency plans.

65 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST SP 800-53: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD-1; NIST CSF: PR.IP-4; FY 2018 CIO FISMA Metrics: 5.4; and NARA guidance on information systems security records)?

Consistently Implemented (Level 3)

Comments: MET

Function 5: Recover - Contingency Planning

66 To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk based decisions (CSF: RC.CO-3; NIST SP 800-53: CP-2 and IR-4)?

Consistently Implemented (Level 3)

Comments: MET

67.1 Please provide the assessed maturity level for the agency's Recover - Contingency Planning function.

Consistently Implemented (Level 3)

Comments: N/A

67.2 Provide any additional information on the effectiveness (positive or negative) of the organization's contingency planning program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the contingency program effective?

N/A

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 0: Overall

0.1 Please provide an overall IG self-assessment rating (Effective/Not Effective)

Effective

Comments: N/A

Function 0: Overall

0.2 Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.

We utilized the Final FY 2018 Inspector General FISMA Metrics v1.0 maturity model to access the maturity of the EEOC's information system security program. The metrics include eight functional areas and related category. Ratings throughout the eight function areas were by a simple majority, where the most frequent level (i.e., the mode) across the questions served as the function area rating. For example, if there are seven questions in a function area, and the EEOC received defined ratings for three questions and managed and measurable ratings for four questions, then the function area rating is managed and measurable.

The overall assessment of the EEOC information system program is "Level 4: Managed and Measurable." EEOC information system program could be improve by developing qualitative and quantitative performance measures and metrics in the areas of Protect and Recover.

APPENDIX A: Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	0
Defined	2
Consistently Implemented	2
Managed and Measurable	8
Optimized	0
Function Rating: Managed and Measurable (Level 4)Effective	0

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	1
Defined	0
Consistently Implemented	2
Managed and Measurable	4
Optimized	1
Function Rating: Managed and Measurable (Level 4)Effective	0

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	0
Defined	3
Consistently Implemented	2
Managed and Measurable	4
Optimized	0
Function Rating: Managed and Measurable (Level 4)Effective	0

Function 2C: Protect - Data Protection and Privacy

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	3
Managed and Measurable	1
Optimized	0
Function Rating: Consistently Implemented (Level 3)Not Effective	0

Function 2D: Protect - Security Training

Function	Count
Ad-Hoc	1
Defined	0
Consistently Implemented	4
Managed and Measurable	1
Optimized	0
Function Rating: Consistently Implemented (Level 3)Not Effective	0

Function 3: Detect - ISCM

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	1
Managed and Measurable	4
Optimized	0
Function Rating: Managed and Measurable (Level 4)Effective	0

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	3
Managed and Measurable	4
Optimized	0
Function Rating: Managed and Measurable (Level 4)Effective	0

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	6
Managed and Measurable	1
Optimized	0
Function Rating: Consistently Implemented (Level 3)Not Effective	0

Maturity Levels by Function

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	N/A
Function 2: Protect - Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training	Managed and Measurable (Level 4)	Consistently Implemented (Level 3)	N/A
Function 3: Detect - ISCM	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	N/A
Function 4: Respond - Incident Response	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	N/A
Function 5: Recover - Contingency Planning	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	N/A
Overall	Effective	Effective	

10. Appendix C – EEOC Management's Comments

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

February 7, 2019

MEMORANDUM

TO: Milton Mayo, Inspector General

FROM: Jamell Fields, Chief Information Security Officer

Digitally signed by JAMELL FIELDS
DN: c=US, o=U.S. Government, ou=Equal Employment Opportunity Commission, cn=JAMELL FIELDS, 0.9.2342.19200300.100.1.1=45001003673996
Date: 2019.02.07 16:34:37 -05'00'

SUBJECT: Office of Information Technology's (OIT) Response to the FY 2018 Independent Evaluation of the EEOC's Compliance with Provisions of the Federal Information Security Modernization Act (FISMA)

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

FINDING/RECOMMENDATIONS:

1. **Finding: 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.**

   Recommendation 1: We recommend the OIT employ an automated mechanism that ensures sensitive PII (SPII) is encrypted on removable mobile media.

   Response: The audit finding specifically references that EEOC cannot prevent users from storing unencrypted sensitive and PII data on untrusted portable devices, such as USB drives. 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.

   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. 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 secure SharePoint repositories and mission focused electronic services will greatly diminish the need to use removable media to transport 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

2. **Finding: The Office Chief Human Capital Officer (OCHCO) and OIT need to conduct a baseline assessment of the EEOC's cybersecurity workforce.**

   Recommendation 2: We recommend the OCHCO and OIT define and implement a process for conducting an 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.

   Response: OIT will 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. This framework will support by providing a common lexicon and proper taxonomy to define the cybersecurity work as well as the requirements that aligns to the role.

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

   Recommendation 4: 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.

   Response: OIT concurs with this finding and recommendation. OIT will (1) evaluate current vulnerability remediation lifecycles as well as scenarios which affect this lifecycle; (2) explore vulnerability management timelines and remediation procedure methodologies; and (3) draft, approve and implement improved vulnerability management standard operating procedures (SOP).

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