

PERFORMANCE AUDIT REPORT

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION
FEDERAL INFORMATION SECURITY MODERNIZATION ACT
OF 2014 (FISMA)

FOR THE FISCAL YEAR ENDING
SEPTEMBER 30, 2020

Harper, Rains, Knight & Company, P.A.
700 12th ST NW, Suite 700
Washington, DC 20005
601-605-0722
www.hrkcpa.com

TABLE OF CONTENTS

Independent Auditors' Performance Audit Report on the U.S. Equal Employment Opportunity Commission Federal Information Security Modernization Act for Fiscal Year 2020	1
Background	3
Objective, Scope, and Methodology	6
Results	9
Findings and Recommendations	9
Appendix A – Status of Prior Findings	12
Appendix B – EEOC Management’s Response	14



Harper, Rains, Knight & Company

**INDEPENDENT AUDITORS' PERFORMANCE AUDIT REPORT ON THE U.S. EQUAL
EMPLOYMENT OPPORTUNITY COMMISSION FEDERAL INFORMATION
SECURITY MODERNIZATION ACT FOR FISCAL YEAR 2020**

Inspector General
U.S. Equal Employment Opportunity Commission:

This report presents the results of our independent performance audit of the U.S. Equal Employment Opportunity Commission's (EEOC) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires Federal agencies, including EEOC, to have an annual independent evaluation performed of their information security programs and practices to determine the effectiveness of such programs and practices, and to report the results of the evaluation to the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS). The EEOC Office of Inspector General (OIG) contracted with Harper, Rains, Knight & Company, PA (HRK) to conduct a performance audit of EEOC's information security program and practices for Fiscal Year (FY) 2020.

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 for the period October 1, 2019 through September 30, 2020. As part of our audit, we responded to the DHS's *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 4.0*, dated April 17, 2020, and assessed the maturity levels on behalf of the EEOC OIG. We also considered applicable OMB policy and guidelines, National Institute of Standards and Technology's (NIST) standards and guidelines, and *NIST Cybersecurity Framework (version 1.1)*.

We determined EEOC established and maintained an effective information security program and practices, consistent with applicable FISMA requirements, OMB policy and guidance, DHS guidance, and NIST standards and guidelines. Our report identified the following finding where the EEOC Office of Information Technology's (OIT) information security program can better protect the confidentiality, integrity, and availability of its information and information systems:

- EEOC OIT needs to remediate internal vulnerabilities on its network. (Repeat finding)

Certified Public Accountants • Consultants • hrkcpa.com

1052 Highland Colony Parkway, Suite 100
Ridgeland, MS 39157
p: 601-605-0722 • f: 601-605-0733

700 12th Street NW, Suite 700
Washington, DC 20005
p: 202-558-5162 • f: 601-605-0733

Inspector General
U.S. Equal Employment Opportunity Commission (continued)

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

This report is for the purpose of concluding on the audit objective described above. Accordingly, this report is not suitable for any other purpose. We appreciate the cooperation and courtesies that EEOC personnel extended to us during the execution of this performance audit.

Harper, Raina, Knight & Company, P.A.

February 24, 2021
Washington, DC

Background

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

The EEOC is responsible for enforcing federal laws that make it illegal to discriminate against a job applicant or an employee because of the person's race, color, religion, sex (including pregnancy, gender identity, and sexual orientation), national origin, age (40 or older), disability or genetic information. It is also illegal to discriminate against a person because the person complained about discrimination, filed a charge of discrimination, or participated in an employment discrimination investigation or lawsuit. EEOC provides services at the headquarters offices in Washington, D.C. and through 53 field offices.

The Office of Information Technology (OIT) is responsible for planning, developing, implementing, and maintaining EEOC's Information Technology (IT) program, policies, standards and procedures. OIT promotes the application and use of information technologies and administers policies and procedures within EEOC to ensure compliance with related federal laws and regulations, to include information security. OIT is responsible for designing the enterprise information architecture; determining the requirements of EEOC's information systems; and developing the integrated systems for nationwide use. The OIT consists of the following components: Office of the Chief Information Officer (OCIO); Customer Services Management Division; Infrastructure Management and Operations Division; and Enterprise Applications Innovation Division.

Federal Information Security Modernization Act of 2014

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

- Reasserts the authority of the Director of the OMB with oversight, while authorizing the Secretary of DHS to administer the implementation of security policies and practices for federal information systems.
- Gives the delegation of OMB's authorities to the Director of National Intelligence (DNI) for systems operated by an element of the intelligence community.
- Requires agencies to notify Congress of major security incidents within seven (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.

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.

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

Fiscal Year 2020 IG Metrics

The FY 2020 IG FISMA Reporting Metrics were developed as a collaborative effort amongst OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in consultation with the Federal Chief Information Officer (CIO) Council. The FY 2020 metrics represent a continuation of work begun in FY 2016, when the IG metrics were aligned with the five function areas in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks

The FY 2020 metrics also mark a continuation of the work that OMB, DHS, and CIGIE undertook in FY 2017 to transition the IG evaluations to a maturity model approach. In previous years, CIGIE, in partnership with OMB and DHS, fully transitioned two of the NIST Cybersecurity Framework function areas, Detect and Respond, to maturity models, with other function areas utilizing maturity model indicators. The FY 2017 IG FISMA Reporting Metrics completed this work by not only transitioning the Identify, Protect, and Recover functions to full maturity models, but by reorganizing the models themselves to be more intuitive. This alignment with the Cybersecurity Framework helps promote consistent and comparable metrics and criteria in the CIO and IG metrics processes while providing agencies with a meaningful independent assessment of the effectiveness of their information security programs. Table 1 below provides an overview of the alignment of the IG and CIO FISMA metrics by NIST Cybersecurity Framework function area.

Table 1: IG and CIO Metrics Align Across NIST Cybersecurity Framework Function Areas

Function (Domain)	IG Metrics	CIO Metrics
Identify (Risk Management)	✓	✓
Protect (Configuration Management)	✓	✓
Protect (Identify and Access Management)	✓	✓
Protect (Data Protection and Privacy)	✓	✓
Protect (Security Training)	✓	✓
Detect (Information Security Continuous Monitoring)	✓	✓
Respond (Incident Response)	✓	✓
Recover (Contingency Planning)	✓	✓

IGs are required to assess the effectiveness of 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. Table 2 below details the five maturity model levels: ad-hoc, defined, consistently implemented, managed and measurable, and optimized.¹

Table 2: IG Evaluation Maturity Levels

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

¹ FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 4.0, April 17, 2020, page 5 of 45
 (https://www.cisa.gov/sites/default/files/publications/FY_2020_IG_FISMA_Metrics.pdf)

Objective, Scope, and Methodology

The objective of this independent performance audit was to assess the effectiveness of the EEOC's information security program and practices for the period October 1, 2019 through September 30, 2020. As part of our audit, we responded to the DHS's *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 4.0*, dated April 17, 2020, and assessed the maturity levels on behalf of the EEOC OIG. We also considered applicable OMB policy and guidelines, National Institute of Standards and Technology's (NIST) standards and guidelines, and *NIST Cybersecurity Framework (version 1.1)*.

To address our audit objective, we assessed the overall effectiveness of the EEOC information security program and practices in accordance with DHS's FISMA Inspector General reporting requirements:

- Risk Management (Identify);
- Configuration Management (Protect);
- Identity, Credential, and Access Management (Protect);
- Data Protection and Privacy (Protect);
- Security Training (Protect);
- Information Security Continuous Monitoring (Detect);
- Incident Response (Respond); and
- Contingency Planning (Recover).

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

We followed-up on recommendations from prior FISMA audits (see *Appendix A*). The audit also included a vulnerability assessment and penetration testing of EEOC-managed systems, consisting of its general support system (GSS) and major application, and an evaluation of EEOC's process for identifying and mitigating technical vulnerabilities.

We reviewed EEOC's general FISMA compliance efforts in the specific areas defined in DHS's guidance and the corresponding reporting instructions. We considered the internal control structure for EEOC's systems in planning our audit procedures. Accordingly, we obtained an understanding of the internal controls over EEOC's systems through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. Our understanding of these systems' internal controls was used to evaluate the degree to which the appropriate internal controls were designed and implemented. When appropriate, we conducted tests using judgmental sampling to determine the extent to which established controls and procedures are functioning as required.

To accomplish our audit objective, we:

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

The independent performance audit was conducted at EEOC's headquarters in Washington, D.C., from May 1, 2020 through October 30, 2020. It covered the period from October 1, 2019, through September 30, 2020.

Criteria

The criteria used in conducting this audit included:

- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- FY 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 4.0, dated April 17, 2020;
- NIST SP 800-12, Rev. 1, *An Introduction to Computer Security: The NIST Handbook*;
- NIST SP 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*;
- NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments*;
- NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*;
- NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A system Life Cycle Approach for Security and Privacy*;
- NIST SP 800-39, *Managing Information Security Risk Organization, Mission, and Information System View*;
- NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*;
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*;
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*;
- OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*;
- OMB Memorandum M-20-04, Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements;
- Federal Cybersecurity Workforce Assessment Act of 2015;
- Federal Identity, Credential, and Access Management Roadmap Implementation Guidance;

Inspector General

U.S. Equal Employment Opportunity Commission (continued)

- Federal Information Processing Standard (FIPS) Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors and*
- Other criteria as appropriate.

Results

We determined EEOC’s information security program is effective and provides reasonable assurance of adequate security. The results of our independent performance audit concluded that EEOC's information security program is generally compliant with the FISMA legislation and is consistent with the functional areas outlined in the NIST Cybersecurity Framework.

The summary assessment results for EEOC maturity level assessment by function areas are in *Exhibit 1*.

Exhibit 1 – EEOC Overall Maturity Level Assessment by Functions Area

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

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

Findings and Recommendations

HRK has assessed the effectiveness of EEOC information system security controls and identified weaknesses. The results of our audit identified areas in EEOC’s information security program that need improvement. The finding and its associated recommendation are discussed below.

Finding 1: EEOC OIT needs to remediate internal vulnerabilities on its network. (Repeat finding)

Condition

An internal vulnerability assessment was performed on EEOC’s internal computer networks from October 23, 2020 through October 29, 2020 by the auditor. The internal vulnerability assessment consisted of an automated assessment of 25,331 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. On a scale of 1.0 to 5.0, with 5.0 being the most critical, the overall assessment of EEOC’s network security posture for all tested assets was 2.4. On a scale of 0 to 100, with 100 being the highest business risk, the overall business risk assessment of EEOC's network security posture for all tested assets was 10. The overall rating is based on the average rating values of each asset scanned. The vulnerability assessment further leveraged the available DHS CISA top exploitable vulnerabilities

by Chinese state-sponsored actors. Of the identified critical scans from the overall vulnerability assessment, those critical vulnerabilities were identified within EEOCs network.

We also performed an external penetration test of the EEOC network. The overall results determined that EEOC's externally facing infrastructure that was tested is secured and had almost no vulnerabilities. However, vulnerabilities were discovered that EEOC should assess.

The results of the vulnerability scans and penetration testing included, but were not limited to, the following identified critical and high risk vulnerabilities: (1) unpatched systems; (2) default passwords, (3) guessable credentials; (4) unsupported operating systems; (5) compromised passwords.

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. Remediate legitimate vulnerabilities response times in accordance with an organizational assessment of risk; and
- e. Shares information obtained from the vulnerability scanning process and security control assessments with personnel or roles to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Cause:

EEOC provided a risk acceptance on previously identified internal vulnerabilities and OIG report findings of outstanding critical, high, and medium vulnerabilities which identified the remediation date being in FY2021.

Effect:

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

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

Recommendation 1:

We recommend EEOC's Office of Information Technology (OIT) review and remediate critical-risk and high-risk vulnerabilities in accordance with EEOC OIT's assessment of risk. Where risk acceptance is required for vulnerabilities based on EEOC's network operation, we recommend that EEOC formally document the risk acceptance along with any associated mitigation activities.

Management's Response:

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

OIT concurs with the basis of this finding and the recommendation. OIT will seek to continue progress, substantially reducing the occurrence of high and critical vulnerabilities and increasing the effectiveness of remediating vulnerabilities. OIT will investigate options to further validate and mitigate these findings using technology enhancements and bolstered procedures. OIT is continuing to implement a Governance, Risk and Compliance (GRC) solution to enhance risk management and improve risk visibility, monitoring, as well as documenting risk decisions to include risk acceptance. OIT will seek to increase efficiencies in: (1) evaluating current vulnerability remediation lifecycles as well as circumstances which affect these lifecycles; (2) exploring vulnerability management timelines and remediation processes; and (3) drafting, approving and implementing improved vulnerability management standard operating procedures (SOP) within the GRC solution.

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

Auditor's Evaluation of Management's Response

EEOC management generally concurred with our recommendations; however, we have not performed any audit procedures over their response and therefore cannot verify the corrective actions have been implemented and are operating effectively.

Appendix A – Status of Prior Findings

No.	Prior Year Audit Recommendations for FY2019 ² , FY2018 ³ , and FY2017 ⁴	Status
1	FY 2019-01 FISMA audit recommendation No. 1: <i>We recommend EEOC OIT conduct a privacy impact assessment of the SharePoint system to identify privacy issues and risks associated with the security settings; and to provide recommendations to mitigate potential privacy risk.</i>	Open
2	FY 2019-02 FISMA audit recommendation No. 2: <i>We recommend EEOC OIT provide specialized training for SharePoint administrators and users to reduce the risk of exposing sensitive information and PII.</i>	Open
3	FY 2019-03 FISMA audit recommendation No. 3: <i>We recommend EEOC OIT review and remediate critical-risk, high-risk and medium-risk vulnerabilities in accordance with EEOC OIT’s assessment of risk. If the risk is not remediated then we recommend EEOC OIT document the acceptance of the risk.</i>	Open
4	FY 2019-03 FISMA audit recommendation No. 4: <i>We recommend EEOC OIT enforce its mobile device management compliance policies for all enrolled mobile devices and report noncompliance to the user and OIT senior management for corrective action.</i>	Closed
5	FY 2018-01 FISMA audit recommendation No. 1: <i>We recommend the OIT employed an automated mechanism that ensures sensitive PII is encrypted on removable mobile media.</i>	Open
6	FY 2018-02 FISMA audit recommendation No. 2: <i>We recommend the OCHCO and OIT define and implement a process for conducting assessment of the knowledge, skills, and abilities of EEOC’s cybersecurity workforce.</i>	Closed

² The U.S. Equal Employment Opportunity Commission Federal Information Security Modernization Act of 2014 (FISMA) Fiscal Year 2019 Performance Audit. (report no. 2019-04-AOIG)

³ The Independent Evaluation of the U.S. Equal Employment Opportunity Commission’s Compliance with Provisions of the Federal Information Security Modernization Act of 2014 (FISMA) for Fiscal Year 2018 (report no. 2018-04-AOIG).

⁴ The Independent Evaluation of the U.S. Equal Employment Opportunity Commission’s Compliance with Provisions of the Federal Information Security Modernization Act of 2014 (FISMA) for Fiscal Year 2017 (report no. 2017-07-AOIG).

Inspector General
U.S. Equal Employment Opportunity Commission (continued)

No.	Prior Year Audit Recommendations for FY2019 ² , FY2018 ³ , and FY2017 ⁴	Status
7	FY 2018-02 FISMA audit recommendation No. 3: <i>We recommend the OCHCO and OIT conduct a baseline assessment of the EEOC’s cybersecurity workforce that includes (1) the percentage of personnel with IT, cybersecurity, or other cyber-related job functions who hold certifications; (2) the level of preparedness of other cyber personnel without existing credentials to take certification exams; and (3) a strategy for mitigating any gaps identified with appropriate training and certification for existing personnel.</i>	Closed
8	FY 2018-03 FISMA audit recommendation No. 4: <i>We recommend the OIT review and remediate critical-risk, high-risk and moderate-risk vulnerabilities. These vulnerabilities should be resolved to avoid compromise to EEOC’s systems; or the Agency should document acceptance of the risk or reclassification of the risk.</i>	Open
9	FY 2017 FISMA audit recommendation No. 1: <i>We recommend the OIT implement an automated solution to provide a centralized, enterprise-wide view of risk across the agency.</i>	Open
10	FY 2017 FISMA audit recommendation No. 2 <i>We recommend the EEOC Office of Information Technology develop and implement a Trusted Internet Connection (TIC) program in accordance with Office of Management and Budget (OMB) requirements to assist in protecting the Agency’s network from cyber threats.</i>	Open
11	FY 2017 FISMA audit recommendation No. 3: <i>We recommend the OIT conduct an e-authentication risk assessment based on NIST SP 800-63-3 Digital Identity Guidelines suite, for EEOC’s digital services, and fully implement multifactor authentication for logical and remote access enterprise-wide.</i>	Open

² The U.S. Equal Employment Opportunity Commission Federal Information Security Modernization Act of 2014 (FISMA) Fiscal Year 2019 Performance Audit. (report no. 2019-04-AOIG)

³ The Independent Evaluation of the U.S. Equal Employment Opportunity Commission’s Compliance with Provisions of the Federal Information Security Modernization Act of 2014 (FISMA) for Fiscal Year 2018 (report no. 2018-04-AOIG).

⁴ The Independent Evaluation of the U.S. Equal Employment Opportunity Commission’s Compliance with Provisions of the Federal Information Security Modernization Act of 2014 (FISMA) for Fiscal Year 2017 (report no. 2017-07-AOIG).

Appendix B – EEOC Management’s Response




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

February 3, 2021

MEMORANDUM

TO: Milton Mayo, Inspector General

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

SUBJECT: Office of Information Technology’s (OIT) Response to the FY 2020 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@eoc.gov or 202.921.2597 if you have any questions related to our responses.

FINDING/RECOMMENDATIONS:

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

Recommendation 1: We recommend EEOC’s OIT review and remediate critical-risk and high-risk vulnerabilities in accordance with EEOC OIT’s assessment of risk. Where risk acceptance is required for vulnerabilities based on EEOC’s network operation, we recommend that EEOC formally document the risk acceptance along with any associated mitigation activities. (Repeat finding)

Response 1: OIT concurs with the basis of this finding and the recommendation. OIT will seek to continue progress, substantially reducing the occurrence of high and critical vulnerabilities and increasing the effectiveness of remediating vulnerabilities. OIT will investigate options to further validate and mitigate these findings using technology enhancements and bolstered procedures. OIT is continuing to implement a Governance, Risk and Compliance (GRC) solution to enhance risk management and improve risk visibility, monitoring, as well as documenting risk decisions to include risk acceptance. OIT will seek to increase efficiencies in: (1) evaluating current vulnerability remediation lifecycles as well as circumstances which affect these lifecycles; (2) exploring vulnerability management timelines and remediation processes; and (3) drafting, approving and implementing improved vulnerability management standard operating procedures (SOP) within the GRC solution.

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