PERFORMANCE AUDIT REPORT

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

FOR THE FISCAL YEAR ENDING
SEPTEMBER 30, 2022

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

Harper, Rains, Knight & Company

TABLE OF CONTENTS

Harper, Rains, Knight & Company

IMPORTANT NOTICE

This report contains sensitive content. Sections of this report are being withheld from public release due to the sensitive content.

HRK

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 2022

Joyce T. Willoughby, Esq
Acting 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) 2022.

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 FY 2022. As part of our audit, we responded to the core metrics identified in the *FY22 Core IG Metrics Implementation Analysis and Guidelines*, the associated *FY 2022 Core IG FISMA Metrics Evaluation Guide*, and assessed the maturity levels on behalf of the EEOC OIG to be consistently implemented. We also considered applicable OMB policy and guidelines, National Institute of Standards and Technology's (NIST) standards and guidelines, the Carnegie Mellon Cybersecurity Maturity Model Certification (CMMI), and *NIST Cybersecurity Framework (version 1.1)*.

We determined EEOC established and maintained a consistently implemented 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 findings where the EEOC Office of Information Technology's (OIT) information security program can better protect the confidentiality, integrity, and availability of its information and information systems:

- EEOC needs to implement and communicate an organization-wide Supply Chain Risk Management strategy and policy. (*Repeat finding*)
- EEOC has [redacted]
- EEOC needs [redacted]
- EEOC needs [redacted]
- EEOC needs [redacted]
- EEOC needs [redacted]

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, Rains, Knight & Company, P.A.

Washington, DC
October 31, 2022

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. The Chief Information Officer is the official responsible for carrying out the mission of the OIT, which is responsible for designing the enterprise information architecture; determining the requirements of EEOC's information systems; and developing the integrated systems for nationwide use. Within the OIT is the Chief Information Security Officer (CISO) who is the official responsible for carrying out the OIT responsibilities under FISMA, including IT governance and security, and is the primary liaison to EEOC's authorizing officials, systems owners, and information security officials.

Federal Information Security Modernization Act of 2014

FISMA 2014 codifies the Department of Homeland Security's role in administering the implementation of information security policies for federal Executive Branch civilian agencies, overseeing agencies' compliance with those policies, and assisting OMB in developing those policies. The legislation provides the Department authority to develop and oversee the implementation of binding operational directives to other agencies, in coordination and consistent with OMB policies and practices. It also:

- Authorizes DHS to provide operational and technical assistance to other federal Executive Branch civilian agencies at the agency's request;
- Places the federal information security incident center (a function fulfilled by US-CERT) within DHS by law;
- Authorizes DHS technology deployments to other agencies' networks (upon those agencies' request);

- Directs OMB to revise policies regarding notification of individuals affected by federal agency data breaches;
- Requires agencies to report major information security incidents as well as data breaches to Congress as they occur and annually; and
- Simplifies existing FISMA reporting to eliminate inefficient or wasteful reporting while adding new reporting requirements for major information 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 2022 IG Metrics

The Federal Information Security Modernization Act of 2014 (FISMA) requires each agency IG, or an independent external auditor, to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency. Accordingly, the fiscal year (FY) 2022 IG FISMA Reporting Metrics focus on key areas to ensure successful independent evaluations of agencies' information security programs.

The FY 2022 Core IG Metrics represent a continuation of work begun in FY 2016, when the IG metrics were aligned to 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 assessing cybersecurity capabilities and associated risks implemented across the enterprise and enables the IGs to have a framework for the communication of capabilities and the maturity of controls that support them.

The FY22 Core IG Metrics were chosen based on alignment with Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," as well as recent OMB guidance to agencies in furtherance of the modernization of federal cybersecurity, including:

- Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (M-22-09) – OMB and CISA solicited public feedback on strategic and technical guidance documents meant to move the U.S. government towards a zero trust architecture. The goal of OMB's Federal Zero Trust Strategy is to accelerate agencies towards a baseline of early zero trust maturity.
- Multifactor Authentication (MFA) and Encryption (EO 14028) – Per the EO, agencies were required to fully adopt MFA and encryption for data at rest and in transit by November 8, 2021. For agencies that were unable to meet these requirements within 180 days of the date

of the order, the agency head was directed to provide a written rationale to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the APNSA.

- Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents (M-21-31) – This memorandum provides specific requirements for log management. It includes a maturation model, prioritizing the most critical log types and requirements, to build a roadmap to success.
- Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (M-22-01) – On October 8, 2021, this memorandum was issued for agencies to focus on improving early detection capabilities, creating "enterprise-level visibility" across components and sub-agencies, and requires agencies to deploy an EDR solution.
- Software Supply Chain Security & Critical Software – Section 4 of EO 14028 tasks OMB, NIST, and other federal entities with developing new guidelines and frameworks to improve the security and integrity of the technology supply chain. In collaboration with industry and other partners, this effort is providing frameworks and guidelines on how to assess and build secure technology, including open source software.

Additionally, OMB Memorandum M-22-05 adjusts the timeline for the Inspectors General evaluation of agency effectiveness to align the results of the evaluation with the budget submission cycle. Historically, the evaluation of agency effectiveness by Inspectors General finished in October. This timing limited agency leadership's ability to request resources in the next Budget Year submissions to provide for remediations. The expectation is this change will reduce the time between issue identification, resource request and allocation. Outlined below is implementation guidance to support IGs as they manage this adjustment.

Objective, Scope, and Methodology

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, 2021, through June 30, 2022. As part of our audit, we responded to the core metrics identified in the *FY22 Core IG Metrics Implementation Analysis and Guidelines*, the associated *FY 2022 Core IG FISMA Metrics Evaluation Guide*, 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, the Carnegie Mellon Cybersecurity Maturity Model Certification (CMMI), 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 Inspector General reporting requirements:

- Risk Management (Identify);
- Supply Chain 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 from February 16, 2022 through June 30, 2022. It covered the period from October 1, 2021, through June 30, 2022.

Criteria

The criteria used in conducting this audit included:

- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- FY22 Core IG Metrics Implementation Analysis and Guidelines;
- FY 2022 Core IG FISMA Metrics Evaluation Guide;
- 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. 5 *Security and Privacy Controls for Federal Information Systems and Organizations;*
- NIST *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1;
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*;
- 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-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*;
- OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*;
- OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*;
- OMB Memorandum M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*;
- OMB Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*;
- OMB Memorandum M-22-09, *Moving the U.S. Government to Zero Trust Cybersecurity Principles*;
- Executive Order (EO) 14028, *Improving the Nation's Security*;
- Federal Cybersecurity Workforce Assessment Act of 2015;
- Federal Identity, Credential, and Access Management Roadmap Implementation Guidance;
- Federal Information Processing Standard (FIPS) Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors and*
- Other criteria as appropriate.

Results

We determined EEOC's information security program is consistently implemented 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 for Core Metrics

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

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

Section withheld from public release due to the sensitive content.

Additional Observations

Section withheld from public release due to the sensitive content.

Appendix A – Status of Prior Findings

Section withheld from public release due to the sensitive content.

Appendix B – EEOC Management’s Response

Section withheld from public release due to the sensitive content.