Harper, Rains, Knight & Company

PERFORMANCE AUDIT REPORT

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

FOR THE FISCAL YEAR ENDING
SEPTEMBER 30, 2024

Harper, Rains, Knight & Company, P.A.
1425 K ST NW, Suite 1120
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.

Harper, Rains, Knight & Company

INDEPENDENT AUDITORS' PERFORMANCE AUDIT REPORT ON THE U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION COMPLIANCE WITH FEDERAL INFORMATION SECURITY MODERNIZATION ACT FOR FISCAL YEAR 2024

Joyce T. Willoughby, Esq
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) 2024.

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 2024. As part of our audit, we responded to the core metrics and supplemental metrics identified in the *FY 2023 -2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics (IG Metrics)*, the associated *FY 2024 Inspector General FISMA Metrics Evaluator's Guide*, and assessed the maturity levels on behalf of the EEOC OIG to be consistently implemented, which we determined to be effective. We also considered applicable OMB policy and guidelines, National Institute of Standards and Technology's (NIST) standards and guidelines, and the NIST *Cybersecurity Framework (CSF), February 26, 2024*.

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:

Section withheld from public release due to the sensitive content.

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
December 12, 2024

Background

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 codifies the Department of Homeland Security's (DHS) 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 DHS authority to develop and oversee the implementation of binding operational directives to other agencies, in coordination and consistent with OMB policies and practices. FISMA 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, the OIG must submit to DHS the "Inspector General FISMA Reporting Metrics" that depicts the effectiveness of the agency's information security program.

Fiscal Year 2024 IG Metrics

FISMA requires each agency inspector general (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. OMB, CIGIE, and other stakeholders worked collaboratively to develop the *FY 2023-2024 IG FISMA Reporting Metrics*. The *FY 2023-2024 IG FISMA Reporting Metrics* represent a continuation of the work started in FY 2022, when the IG metrics reporting process was transitioned to a multi-year cycle.

The Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements (M-22-05) encouraged agencies to shift towards a continuous assessment process for their annual independent assessment. To help facilitate this, the memo also announced that OMB and CIGIE are transitioning the IG FISMA metrics to a multi-year cycle—with a set of core metrics that must be evaluated annually and the remaining metrics that will be evaluated on a two-year cycle, beginning in FY 2023.

The core metrics represent a combination of Administration priorities and other highly valuable controls that must be evaluated annually. Specifically, these core metrics align with the Executive Order on Improving the Nation's Cybersecurity (EO 14028), and guidance from OMB to agencies to improve federal cybersecurity, including:

- *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (M-22-09)*, sets forth a plan for migrating the federal government to a new cybersecurity paradigm that does not presume that any person or device inside an organization's perimeter is trusted, and focuses agencies on strengthening their capability to limit, and continuously verify, the access those people and devices have to government data.
- *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents (M-21-31)*, sets detailed requirements for log management, configuration, and enterprise-level centralization. It also provides a maturity model that prioritizes the most critical software types and requirements.
- *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (M-22-01)*, directs agencies to with the Cybersecurity and Infrastructure Security Agency (CISA) to accelerate their adoption of robust endpoint, detection, and response (EDR) solutions, an essential component for zero trust architecture that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.
- *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices (M-22-18)*, initiates a government-wide shift towards requiring agencies to use software developed in a secure manner. This will minimize the risks associated with running unvetted technologies on agency networks, increasing the resilience of Federal technology against cyber threats.

The IG FISMA metrics are aligned with the five function areas in the NIST 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.

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, 2023 through June 30, 2024. As part of our performance audit, we responded to the core metrics identified in the *FY 2023 - 2024 Inspector General FISMA Reporting Metrics,* the associated *FY 2024 Inspector General FISMA Metrics Evaluator's Guide*, and assessed the maturity levels on behalf of the EEOC OIG. We also considered applicable OMB policy and guidelines, NIST standards and guidelines, and the NIST *Cybersecurity Framework*.

To address our performance 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 performance 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 performed procedures to determine the status of 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;
- Completed an internal network vulnerability assessment of selected EEOC systems; and
- Completed an external network penetration testing of selected EEOC systems.

The independent performance audit was conducted from February 29, 2024, through July 31, 2024. It covered the period from October 1, 2023, through June 30, 2024.

Criteria

The criteria used in conducting this performance audit included:

- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- FY 2023 – 2024 Inspector General (IG) Federal Information Security Modernization Act (FISMA) Reporting Metrics;
- FY 2024 IG FISMA Metrics Evaluator's Guide, v 4.0, April 30, 2024;
- 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* v1.1;
- NIST *Cybersecurity Framework* (CSF) v1.1;
- 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-21-30, *Protecting Critical Software through Enhanced Security Measures*;
- 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*;
- OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*;
- OMB Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements;*
- Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*;
- DHS CISA Binding Operational Directives (BODs) and Emergency Directives (EDs);
- 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 assessed EEOC's information security program to be consistently implemented, which is not effective, per the IG Metrics. 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.

Maturity Level Scoring
The maturity level scoring was developed by DHS and OMB. Level 1 (Ad-hoc) is the lowest level and Level 5 (Optimized) is the highest level. The maturity levels are defined as follows:

1. Level 1 (Ad-hoc): Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
2. Level 2 (Defined): Policies, procedures, and strategies are formalized and documented but not consistently implemented.
3. Level 3 (Consistently Implemented): Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
4. 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.
5. 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.

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 Function Area	FY 2024 Maturity Level (Core & Supplemental Metrics)	FY 2023 Maturity Level (Core & Supplemental Metrics)
Identify	Managed and Measurable (Level 4)	Consistently Implemented (Level 3)
Protect	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)
Detect	Managed and Measurable (Level 4)	Consistently Implemented (Level 3)
Respond	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)
Recover	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)

Ratings in FY 2024 focus on a calculated average approach, wherein the average of the metrics in a particular domain are used by IGs to determine the effectiveness of individual function areas (identify, protect, detect, respond, and recover) and the overall program.

Findings and Recommendations

Section withheld from public release due to the sensitive content.

Informational 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.