PERFORMANCE AUDIT REPORT

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

FOR THE FISCAL YEAR ENDING
SEPTEMBER 30, 2021
TABLE OF CONTENTS


Background ..................................................................................................................................... 3

Objective, Scope, and Methodology .............................................................................................. 6

Results .............................................................................................................................................. 9

Findings and Recommendations ................................................................................................ 9

Appendix A – Status of Prior Findings ......................................................................................... 10

Appendix B – EEOC Management’s Response ............................................................................. 11
IMPORTANT NOTICE

This report contains sensitive content. Sections of this report are being withheld from public release due to the sensitive content.
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) 2021.

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, 2020 through September 30, 2021. As part of our audit, we responded to the FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.1, dated May 12, 2021, 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 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.
- EEOC has
Inspector General  
U.S. Equal Employment Opportunity Commission (continued)

- EEOC needs to consistently utilize and document Plans of Actions and Milestones (POAMs) to effectively mitigate identified security weaknesses.
- EEOC has
- EEOC does
- EEOC needs
- EEOC needs
- EEOC needs
- EEOC needs
- EEOC needs
- EEOC needs

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, Raini, Knight & Company, P.A.

Washington, DC  
March 9, 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. 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.

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

- 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 2021 IG Metrics**

The FY 2021 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 2021 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.

Table 1 below provides an overview of the IG metrics by NIST Cybersecurity Framework (CSF) function area and related categories. The FY 2021 metrics include a new Supply Chain Risk Management domain within the Identify function area.

<table>
<thead>
<tr>
<th>IG Metric Function Area and Related Domains</th>
<th>Related CSF Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify (Risk Management)</td>
<td>Asset Management (ID.AM), Business Environment (ID.BE), Governance (ID.GV), Risk Assessment (ID.RA), and Risk Management Strategy (ID.RM)</td>
</tr>
<tr>
<td>Identify (Supply Chain Risk Management)</td>
<td>Supply Chain Risk Management (ID.SC)</td>
</tr>
<tr>
<td>Protect (Configuration Management)</td>
<td>Information Protection Processes and Procedures (PR.IP)</td>
</tr>
<tr>
<td>Protect (Identify and Access Management)</td>
<td>Identity Management and Access Control (PR.AC)</td>
</tr>
</tbody>
</table>
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.

### Table 2: IG Evaluation Maturity Levels

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Maturity Level Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level 1: Ad-hoc</strong></td>
<td>Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.</td>
</tr>
<tr>
<td><strong>Level 2: Defined</strong></td>
<td>Policies, procedures, and strategies are formalized and documented but not consistently implemented.</td>
</tr>
<tr>
<td><strong>Level 3: Consistently Implemented</strong></td>
<td>Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.</td>
</tr>
<tr>
<td><strong>Level 4: Managed and Measurable</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Level 5: Optimized</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
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, 2020 through September 30, 2021. As part of our audit, we responded to the DHS’s FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.1, dated May 12, 2021, 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 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 at EEOC’s headquarters in Washington, D.C., from May 1, 2021 through October 30, 2021. It covered the period from October 1, 2020, through September 30, 2021.

Criteria
The criteria used in conducting this audit included:

- NIST SP 800-12, Rev. 1, *An Introduction to Computer Security: The NIST Handbook*;
- 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 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*;
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*;
- OMB Memorandum M-21-02, Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements;
- Federal Cybersecurity Workforce Assessment Act of 2015;
Federal Information Processing Standard (FIPS) Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors and*

• Other criteria as appropriate.
Inspector General
U.S. Equal Employment Opportunity Commission (continued)

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**

<table>
<thead>
<tr>
<th>FISMA NIST Cybersecurity Framework Functions Area (Domains)</th>
<th>Current Year Maturity Level</th>
<th>Prior Year Maturity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify (Risk Management)</td>
<td>Managed and Measurable</td>
<td>Consistently Implemented</td>
</tr>
<tr>
<td>Identify (Supply Chain Risk Management)</td>
<td>Ad Hoc</td>
<td>N/A</td>
</tr>
<tr>
<td>Protect (Configuration Management)</td>
<td>Managed and Measurable</td>
<td>Managed and Measurable</td>
</tr>
<tr>
<td>Protect (Identity and Access Management)</td>
<td>Managed and Measurable</td>
<td>Managed and Measurable</td>
</tr>
<tr>
<td>Protect (Data Protection and Privacy)</td>
<td>Consistently Implemented</td>
<td>Consistently Implemented</td>
</tr>
<tr>
<td>Protect (Security Training)</td>
<td>Consistently Implemented</td>
<td>Managed and Measurable</td>
</tr>
<tr>
<td>Detect (Information Security Continuous Monitoring (ISCM))</td>
<td>Managed and Measurable</td>
<td>Managed and Measurable</td>
</tr>
<tr>
<td>Respond (Incident Response)</td>
<td>Managed and Measurable</td>
<td>Managed and Measurable</td>
</tr>
<tr>
<td>Recover (Contingency Planning)</td>
<td>Consistently Implemented</td>
<td>Consistently Implemented</td>
</tr>
</tbody>
</table>

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.
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.