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, 2023

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

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 2023

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) 2023.

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 2023. 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 2023 Inspector General FISMA Metrics Evaluator's Guide*, and assessed the maturity levels on behalf of the EEOC OIG to be consistently implemented, which is not effective, per the IG Metrics. We also considered applicable OMB policy and guidelines, National Institute of Standards and Technology's (NIST) standards and guidelines, and the NIST *Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)*.

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:

- Supply Chain Risk Management (SCRM) and Cybersecurity Supply Chain Risk Management (C-SCRM) policies and been adopted by the OIT but have not been adopted EEOC-wide. (*Repeat finding*)
- Weak Mechanisms for Privileged and Non-privileged users. (*Repeat finding*)
- Unadopted Trusted Internet Connection (TIC) program. (*Repeat finding*)
- EEOC has not met event logging tiers in accordance with OMB M-21-31
- EEOC has outdated, unsigned, and draft policies and procedures.
- Default passwords were identified in implemented systems.
- Running outdated and exploitable versions of tools and firmware on implemented systems.
- HTML and JavaScript source code discloses internal IP addresses and URLs.
- EEOC does not limit access from specific IP addresses to the Amazon AWS EKS API and did not configure the AWS Control Tower's date residency controls to alert on publicly accessible Amazon EKS endpoints.
- EEOC does not have an effective policy and procedures in place to ensure all form fields posted to the host are encrypted, including the username and password sent to the host during login.
- EEOC's flaw remediation is not followed resulting in significant Level 5 and Level 4 vulnerabilities that have not been remediated in compliance with its patch policy. (*Repeat finding*)

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 23, 2023

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 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 2023 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, 2022, through June 30, 2023. As part of our audit, we responded to the core metrics identified in the *FY 2023 -2024 Inspector General FISMA Reporting Metrics, the associated FY 2023 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, National Institute of Standards and Technology's (NIST) standards and guidelines, and the NIST *Cybersecurity Framework*.

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 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; and
- Completed an internal network vulnerability assessment of selected EEOC systems.
- Completed an external network penetration testing of selected EEOC systems.

The independent performance audit was conducted from February 21, 2023 through July 31, 2023. It covered the period from October 1, 2022, through June 30, 2023.

Criteria

The criteria used in conducting this audit included:

- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- FY 2023 – 2024 IG FISMA Metrics
- FY 2023 IG FISMA Metrics Evaluation Guide
- 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*;
- 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-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements;*
- Executive Order (EO) 14028, *Improving the Nation's Security*;
- DHS Binding Operational Directive 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks*;
- 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.

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	FY 2023 Maturity Level (Core & Supplemental Metrics)	FY 2022 Maturity Level (Core Metrics)
Identify	Consistently Implemented	Consistently Implemented
Protect	Consistently Implemented	Consistently Implemented
Detect	Consistently Implemented	Consistently Implemented
Respond	Consistently Implemented	Consistently Implemented
Recover	Consistently Implemented	Managed and Measurable

Ratings in FY 2023 will focus on a calculated average approach, wherein the average of the metrics in a particular domain will be used by IGs to determine the effectiveness of individual function areas (identify, protect, detect, respond, and recover) and the overall program.

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 findings and its associated recommendation are discussed below.

Finding 1: SCRM and C-SCRM policies have been adopted by OIT but have not been adopted EEOC-wide.

Condition:

EEOC has developed and defined Supply Chain Risk Management (SCRM) and Cybersecurity Supply Chain Risk Management (C-SCRM) strategies, however they have not been adopted EEOC-wide. Additionally, EEOC has not performed a formal supply chain risk assessment.

Criteria:

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, establishes controls for systems and organizations, including the minimum controls required by the provisions of FISMA to protect federal information and information systems.

IG-Metric-12: (*FY 2023 IG FISMA Metrics Evaluation Guide*)
To what extent does the organization use an organization wide SCRM strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services?

IG-Metric-13: (*FY 2023 IG FISMA Metrics Evaluation Guide*)
To what extent does the organization use SCRM policies and procedures to manage SCRM activities at all organizational tiers?

SA-4, Acquisition Process: (*NIST SP 800-53, Rev. 5*)
Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [organization defined contract language]] in the acquisition contract for the system, system component, or system service: Security and privacy functional requirements; Strength of mechanism requirements; Security and privacy assurance requirements; Controls needed to satisfy the security and privacy requirements; Security and privacy documentation requirements; Requirements for protecting security and privacy documentation; Description of the system development environment and environment in which the system is intended to operate; Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and Acceptance criteria.

SR-3, Supply Chain Controls and Processes: (*NIST SP 800-53, Rev. 5*)

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [organization-defined system or system component] in coordination with [organization-defined supply chain personnel];
b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain related events: [organization-defined supply chain controls]; and
c. Document the selected and implemented supply chain processes and controls in [Selection: security and privacy plans; supply chain risk management plan; [organization defined document]].

SR-5, Acquisition Strategies, Tools, and Methods: (*NIST SP 800-53, Rev. 5*)
Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [organization-defined acquisition strategies, contract tools, and procurement methods].

SR-6, Supplier Assessments and Reviews: (*NIST SP 800-53, Rev. 5*)
Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [organization-defined frequency].

ID.SC-2, Supply Chain Risk Management: (*NIST CSF V 1.1*)
Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.

ID.SC-3, Supply Chain Risk Management: (*NIST CSF V 1.1*)
Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.

ID.SC-4, Supply Chain Risk Management: (*NIST CSF V 1.1*)
Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.

Cause:

EEOC has developed both a C-SCRM policy and guide as of 1st quarter of FY2023, however the overall SCRM program is currently only implemented in OIT, not agency-wide.

Effect:

The identification and prioritization of suppliers of critical or mission-essential technologies, products, and services through a SCRM/C-SCRM programs is paramount to the mission/business success of organizations. An analysis of supply chain risks can help an organization identify systems or components for which additional supply chain risk mitigations are required.

Failure to adopt an organization-wide SCRM and C-SCRM strategy could impact the agency's information security program and, therefore, threatens the confidentiality, integrity, & availability of EEOC's information systems.

Recommendation:

We recommend that EEOC communicates and implements an organization-wide SCRM and C-SCRM strategy to guide supply chain analyses, provide communication channels with internal/external partners and stakeholders, and assist in building consensus regarding the appropriate resources for SCRM and C-SCRM. We recommend that EEOC offices of the Chief Financial Officer and the Chief Information Officer identify SCRM/C-SCRM as a risk to be included in their respective ERM risk registers until the issue is resolved so that commission management understand that SCRM/C-SCRM is a commission-wide requirement.

Managements' Response:

OIT concurs with the basis of these findings and the associated recommendations. OIT will investigate options to further validate, acceptably mitigate or remediate these findings using technology enhancements to include managerial controls to address the subject discrepancies.

OCFO concurs and is in the process of updating our Risk Register.

For managements' complete response see ***Appendix B***.

Auditors' Response:

FY 2024 performance audit procedures will be performed to determine if the corrective actions being taken have been implemented and address this finding.

Finding 2: Identity and Access Management (ICAM) – Weak Authentication Mechanisms for Privileged & Non-Privileged Users

Condition:

EEOC has not implemented strong authentication mechanisms for all non-privileged and privileged users of the agency's networks, systems, including remote access, and end points on the networks, in accordance with Federal targets identified in OMB Memorandum 19-17 and NIST Special Publication 800-63.

Criteria:

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, establishes controls for systems and organizations, including the minimum controls required by the provisions of FISMA to protect federal information and information systems.

IG-Metric-30: (*FY 2023 IG FISMA Metrics Evaluation Guide*)
To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO or web authentication) for non- privileged users to access the organization`s facilities [organization-defined entry/exit points], networks, and systems, including for remote access?

IG-Metric-31: (*FY 2023 IG FISMA Metrics Evaluation Guide*)
To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO or web authentication) for privileged users to access the organization`s facilities [organization-defined entry/exit points], networks, and systems, including for remote access?

Cause:

The agency has plans in place for organization-wide use of strong authentication mechanisms for privileged and non-privileged users. However, it has not fully implemented across the organization.

Effect:

Strong authentication mechanisms, such as multifactor authentication or PIV credentials, reduce the risk of security breaches from occurring. Strong authentication mechanisms protect the data and information on agency information systems, system components, and devices, from being accessed and exploited by unauthorized individuals.

Failure to consistently implement strong authentication mechanisms for privileged and non-privileged users could impact the agency's information security program and, therefore, threatens the confidentiality, integrity, & availability of EEOC's information systems.

Recommendation:

We recommend that EEOC continue its full implementation in accordance with their plan. For the ZTA Identity pillar, to better meet ZT requirements for all agency-provided devices, the EEOC made a strategic decision to move away from the prior PIV-based device-login solution to a new password-less Multi-Factor Authentication (MFA) strategy - providing a strong, non-impersonable authentication process for all agency resource access. In FY 2022, the EEOC piloted and acquired FIDO2/WebAuthn-compliant devices and services for workstation logon, remote desktop (RDP) sessions, network device login, and cloud applications access. Deployment of this new ZT MFA service will be completed in FY 2023. In addition, in FY 2022, the EEOC established a MOU with GSA's Technology Transformation Services for Login.Gov integration. The secure sign-in service integration will provide the public with MFA and phishing-resistant authentication methods for EEOC's public-facing systems. In early FY 2023, the EEOC completed Login.Gov integration for its public-facing system receiving FOIA requests. Integration work will continue with the EEOC's other public portals during FYs 2023 and 2024.

Managements' Response:

OIT concurs with the basis of these findings and the associated recommendations. OIT will investigate options to further validate, acceptably mitigate or remediate these findings using technology enhancements to include managerial controls to address the subject discrepancies.

For managements' complete response see ***Appendix B***.

Auditors' Response:

FY 2024 performance audit procedures will be performed to determine if the corrective actions being taken have been implemented and address this finding.

Finding 3: Configuration Management – Unadopted Trusted Internet Connection (TIC) Program

Condition:

EEOC has not prepared and planned to meet the goals of the TIC initiative, consistent with OMB M-19-26. The agency has not defined and customized, as appropriate, its policies, procedures, and processes to implement TIC 3.0, including updating its network and system boundary policies, in accordance with OMB M-19-26.

Criteria:

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, establishes controls for systems and organizations, including the minimum controls required by the provisions of FISMA to protect federal information and information systems.

IG-Metric-22: (*FY 2021 IG FISMA Reporting Metrics, V 1.1*)
To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network? (*References:* OMB M-19-26, DHS-CISA TIC 3.0 Core Guidance Documents)

> **DHS CISA Guidance**:
> Determine if the organization:
> a. Has prepared and planned to meet the goals of the TIC initiative, consistent with OMB M-19-26. Specifically, the agency has a defined and customized set of policies, procedures, and processes to implement TIC 3.0 that update its network and system boundary policies. This includes, as appropriate, incorporation of TIC security capabilities catalog, TIC use cases, and TIC overlays.
> b. Has as defined processes to develop and maintain an accurate inventory of its network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection.

Cause:

EEOC has not prepared and planned to meet the goals of the TIC initiative, consistent with OMB M-19-26. The agency has not defined and customized, as appropriate, its policies, procedures, and processes to implement TIC 3.0, including updating its network and system boundary policies, in accordance with OMB M-19-26. This includes, as appropriate, the TIC security capabilities catalog, TIC use cases, and TIC overlays.

Effect:

TIC guidance provides agencies with the flexibility to secure distinctive computing scenarios in accordance with their unique risk tolerance levels. Agencies are expected to reference the initiative's Program Guidebook, Reference Architecture, and Security Capabilities Catalog to determine how to protect their environments to conform with their risk management strategy and the security considerations outlined in TIC use cases.

Failure to plan and prepare for meeting the goals of the TIC initiative, consistent with OMB M-19-26, could impact the agency's information security program and, therefore, threatens the confidentiality, integrity, & availability of EEOC's information systems.

Recommendation:

We recommend that EEOC plans and prepares to meet the goals of the TIC initiative, consistent with OMB M-19-26. The agency should define and customize, as appropriate, a set of policies, procedures, and processes to implement TIC 3.0, including updating its network and system boundary policies, in accordance with OMB M-19-26. This includes, as appropriate, incorporation of TIC security capabilities catalog, TIC use cases, and TIC overlays.

Managements' Response:

OIT concurs with the basis of these findings and the associated recommendations. OIT will investigate options to further validate, acceptably mitigate or remediate these findings using technology enhancements to include managerial controls to address the subject discrepancies.

For managements' complete response see ***Appendix B***.

Auditors' Response:

FY 2024 performance audit procedures will be performed to determine if the corrective actions being taken have been implemented and address this finding.

Finding 4: Incident Response – EEOC Has Not Met Event Logging Tiers in Accordance with OMB M-21-31

Condition:

EEOC has not met event logging tiers of EL1 and EL2 in accordance with OMB M-21-31.

Criteria:

OMB M-21-31 states the following under Section II: Agency Implementation Requirements:

Agencies must immediately begin efforts to increase performance in accordance with the requirements of this memorandum. Specifically, agencies must:

- Within 60 calendar days of the date of this memorandum, assess their maturity against the maturity model in this memorandum and identify resourcing and implementation gaps associated with completing each of the requirements listed below. Agencies will provide their plans and estimates to their OMB Resource Management Office (RMO) and Office of the Federal Chief Information Officer (OFCIO) desk officer.
- Within one year of the date of this memorandum, reach EL1 maturity.
- Within 18 months of the date of this memorandum, achieve EL2 maturity.
- Within two years of the date of this memorandum, achieve EL3 maturity.
- Provide, upon request and to the extent consistent with applicable law, relevant logs to the Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI). This sharing of information is critical to defend Federal information systems.
- Share log information, as needed and appropriate, with other Federal agencies to address cybersecurity risks or incidents.

The Memorandum was dated August 27, 2021, which would require EL1 and EL2 maturities by August 27, 2022 and February 27, 2023, respectively.

Cause:

EEOC has achieved approximately over 70% completion on its path to achieving EL1 using Microsoft Sentinel and associated connectors. EL1 not being complete prevents EL2 and EL3 from being attained in accordance with OMB guidance.

Effect:

Without meeting the required maturity models for event logging, EEOC may not have visibility before, during, and after a cybersecurity incident. Without the required event logs EEOC may not be able to detect, investigate, and remediate cyber threats.

Recommendation:

EEOC should develop an executable plan to meet the requirements of OMB M-21-31 and ensure the plan is properly supported.

Managements' Response:

OIT concurs with the basis of these findings and the associated recommendations. OIT will investigate options to further validate, acceptably mitigate or remediate these findings using technology enhancements to include managerial controls to address the subject discrepancies.

For managements' complete response see ***Appendix B***.

Auditors' Response:

FY 2024 performance audit procedures will be performed to determine if the corrective actions taken have been implemented and address this finding.

Finding 5: Documentation of Policies and Procedures

Condition:

EEOC provided outdated, unsigned, and draft policies and procedures.

System Security Plans (SSP):

- Proposed ARC SSP – Dated 12/1/2022, document indicates "Development/Preliminary Version
- EEOC DataNet General Support System (EEOC DN/GSS) – Dated 5/19/2022, unsigned by System Owner and CISO, provided as Final Draft

Policy and Procedures:

- Information Security Continuous Monitoring (ISCM) policy and information security program provided were dated 2017 and 2022, the latter was not documented as approved.
- EEOC provide Bring Your Own Device (BYOD) policy dated July 17, 2015.
- EEOC provided an entire suite of Risk Management Framework documents, none were signed.
- EEOC provided a a configure management policy dated from 2016. An additional artifact was provided dated 2022 that included updates as of 2021, however it was not in a final version nor approved.
- Patch and Maintenance procedures provided are dated 2009.
- Vulnerability Management Policy is dated 2022 but identified as a draft.
- Information Security Contingency Plan (ISCP) provided was dated 9/7/2016 and ISCP dated 2019 provided was in draft.
- Business Impact Analysis provided "For mission essential function when experiencing an IT service outage" was date as of 5/20/2017.

Criteria:

NIST SP 800-53, Rev. 5 *Security and Privacy Controls for Information Systems and Organizations*, establishes controls for systems and organizations, including the minimum controls required by the provisions of FISMA to protect federal information and information systems.

Managing security and privacy risks is a complex, multifaceted undertaking that requires:

- Well-defined security and privacy requirements for systems and organizations;
- The use of trustworthy information system components based on state-of-the-practice hardware, firmware, and software development and acquisition processes;
- Rigorous security and privacy planning and system development life cycle management;
- The application of system security and privacy engineering principles and practices to securely develop and integrate system components into information systems;
- The employment of security and privacy practices that are properly documented and integrated into and supportive of the institutional and operational processes of organizations; and

- Continuous monitoring of information systems and organizations to determine the ongoing effectiveness of controls, changes in information systems and environments of operation, and the state of security and privacy organization-wide.

Cause:

EEOC does not have a centrally accessible repository of all key cybersecurity and information security policies and procedures accessible to all required members of the Information Security team and does not have a review and update process in place.

Effect:

Without effective documentation of policy and procedures it impacts management ability to:

- Communicate requirements throughout the organization;
- Monitor the responsible party;
- Erodes the means to retain organization knowledge; and
- Mitigate risks.

Recommendation:

EEOC's information security team should, in conjunction with other EEOC offices:

1. Identify and document all applicable policies and procedures to cybersecurity and information security;
2. Develop and use an accessible repository, such as SharePoint, for all identified documents, regardless of what office they reside in;
3. Design a risk-based approach to review and update all identified documents in the repository, including who is responsible for reviewing and updating each document.
4. Document the review/update in each document as well as the responsible party within the information security team who ensures that each document has been updated per the documented procedure for review.
5. Designate a responsible official within the OIT to review and update the process as necessary on annual basis.

Managements' Response:

OIT concurs with the basis of these findings and the associated recommendations. OIT will investigate options to further validate, acceptably mitigate or remediate these findings using technology enhancements to include managerial controls to address the subject discrepancies.

For managements' complete response see ***Appendix B***.

Auditors' Response:

FY 2024 performance audit procedures will be performed to determine if the corrective actions being taken have been implemented and address this finding.

Finding 6: OpenText Big Data Analytics – Default Passwords

<u>Condition:</u>

External penetration testing identified that OpenText Big Data Analytics was running on federaldw.eeoc.org over the unencrypted HTTP protocol on port 8110. A review of the manual at the URL: http://otadocs.opentext.com/documentation/ManualsBA44/BA4.4_Installation_standalone.pdf identified a default username of "Administrator" and password of "PASSWORD". This credential works for each function identified on the server. Screenshots of various screens within the applications are provided below to prove the potential impact. Based on a review of the Big Data Analytics application, there is a potential for PII to be exposed from this vulnerability. This is potentially compounded by a lack of data encryption in transit due to the use of HTTP without SSL/TLS. No modifications of data nor any further exploitation/post-exploitation activities were performed.

<u>Criteria:</u>

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, establishes controls for systems and organizations, including the minimum controls required by the provisions of FISMA to protect federal information and information systems.

> **IA-5(5), Authenticator Management, Change Authenticators Prior to Delivery**: (*NIST SP 800-53, Rev. 5*)
> Changing authenticators prior to the delivery and installation of system components extends the requirement for organizations to change default authenticators upon system installation by requiring developers and/or installers to provide unique authenticators or change default authenticators for system components prior to delivery and/or installation. However, it typically does not apply to developers of commercial off-the shelf information technology products. Requirements for unique authenticators can be included in acquisition documents prepared by organizations when procuring systems or system components.

CWE-1393: Use of Default Password
The product uses default passwords for potentially critical functionality. It is common practice for products to be designed to use default passwords for authentication. The rationale is to simplify the manufacturing process or the system administrator's task of installation and deployment into an enterprise. However, if admins do not change the defaults, then it makes it easier for attackers to quickly bypass authentication across multiple organizations. There are many lists of default passwords and default-password scanning tools that are easily available from the World Wide Web.

<u>Cause</u>:

EEOC does not have an effective policy and procedures in place to enforce NIST 800-53, Rev 5, IA-5(5) and does not periodically perform checks manually (or automated) to ensure updates/patches have not reset the default password, if applicable.

Effect:

The remote system can be accessed using default credentials with root or administrator level privileges. Administration includes the creation, modification, and deletion of users. When logging into the application, the admin user account has access to data stored in the application. This access may potentially expose PII. (For additional details please see **Attachment D**, Finding E1)

Recommendation:

We recommend that EEOC:

- Review all devices and systems and ensure default credentials are not in use.
- Implement the use of complex credentials for all systems.
- Review system for potential malicious access.
- If it is not possible to change passwords to something complex, consider isolating the device on a separate network segment and implementing ACLs that limit what devices and who may attach to the system.
- Determine if the application should be publicly available. If not, implement NSG rules within Microsoft Azure or ACLs within firewalls to limit or block all external applications to the site.
- Ensure it has a policy in place that addresses NIST 800-53, Rev 5, IA-5(5).
- Ensure procedures are written in such a way to accomplish what is written in the policy.
- Ensure it has people in assigned a role to follow and evaluate default credentials.
- Consider how new or existing technologies it has can assist in these efforts:
  - Tracking all new systems and software being deployed;
  - Require the evaluation of the specific policy addressing NIST 800-53, Rev 5, IA-5(5);
  - Prevent systems in violation of the policy from being deployed;
  - Periodically perform checks (manually or automated) to ensure updates/patches have not reset the default password.

Managements' Response:

OIT concurs with the basis of these findings and the associated recommendations. OIT has investigated options to further validate and mitigate this finding. The assessment included a technical mitigation to restrict internal and public access to the portal. Subsequent enhancements include an added technical database remediation with associated managerial controls for consistent implementation.

For managements' complete response see ***Appendix B***.

Auditors' Response:

FY 2024 performance audit procedures will be performed to determine if the corrective actions being taken have been implemented and address this finding.

2023-007-AOIG, External Penetration Testing Finding - Medium Level Severity Vulnerability: *Eclipse BIRT Unauthorized File Creation*

Condition:

After a review of source code from arc.eeoc.gov, external penetration testing identified URLs related to an internal IP address. Those URLs referenced "nxg" and "birtweb". Testing the nxg hosts to see if the birtweb path existed, we identified that each of the three (3) servers are running the Eclipse Business Intelligence Reporting Tool (BIRT) Viewer 4.3.1 Java Servlet via Apache Tomcat. This version and ones including and prior to version 4.12, suffer from a vulnerability that allows for the creation of files on the web server with JSP code in them and potentially the execution of that code from within those files.

Criteria:

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, establishes controls for systems and organizations, including the minimum controls required by the provisions of FISMA to protect federal information and information systems.

SI-2, Flaw Remediation: (*NIST SP 800-53, Rev. 5*)
The need to remediate system flaws applies to all types of software and firmware. Organizations identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Security-relevant updates include patches, service packs, and malicious code signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of risk factors, including the security category of the system, the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw), the organizational risk tolerance, the mission supported by the system, or the threat environment. Some types of flaw remediation may require more testing than other types. Organizations determine the type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software or firmware updates is not necessary or practical, such as when implementing simple malicious code signature updates. In testing decisions, organizations consider whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

Common Weakness Enumeration (CWE) 434: Unrestricted Upload of File with Dangerous Type
The product allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment. Used in vulnerability databases and elsewhere, but it is insufficiently precise. The phrase could be interpreted as the lack of restrictions on the size or number of uploaded files, which is a resource consumption issue.

CWE 20: Improper Input Validation
The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly. Input validation is a frequently-used technique for checking potentially dangerous inputs in order to ensure that the inputs are safe for processing within the code, or when communicating with other components. When software does not validate input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.

Cause:

EEOC does not have an effective policy and procures in place to enforce NIST 800-53, Rev 5, SI-2 which allowed for the BIRT viewer to not be updated in a timely manner.

Effect:

Eclipse BIRT versions 4.8.0 and earlier, an attacker can use query parameters to create a JSP file which is accessible from remote (current BIRT viewer directory) to inject JSP code into the running instance. (For additional details please see **Attachment D**, Finding E2.)

Recommendation:

We recommend that EEOC:

- Update to a recent BIRT viewer component, well past version 4.12.
- Determine if the application should be publicly available. If not, implement NSG rules within Microsoft Azure or ACLs within firewalls to limit or block all external application to the site.
- Remove default and un-needed .rptdesign files that allow for passing a parameter with attacker controlled input.
- Ensure BIRT viewer component is proxied through an authenticated connection and not via direct calls to the NXG servers. Implement the use of complex credentials for all systems.
- Ensure it has a policy in place to address NIST 800-53, Rev 5, SI-2.
- Ensure procedures are written in such a way to accomplish what is written in the policy.
- Ensure it has people in assigned a role to remediate flaws in accordance with its policy and risk tolerance.
- Consider how new or existing technologies it has can assist in these efforts:
    - Tracking all new systems and software being deployed;
    - Require the evaluation of the specific policy addressing NIST 800-53, Rev 5, SI-2);
    - Create an at least monthly review of all flaw remediations that meet the risk tolerance threshold and have not been remediated, to include explanations for the deviation from policy.

<u>Managements' Response</u>:

OIT concurs with the basis of these findings and the associated recommendations. OIT will investigate options to further validate, acceptably mitigate or remediate these findings using technology enhancements to include managerial controls to address the subject discrepancies.

For managements' complete response see ***Appendix B***.

<u>Auditors' Response:</u>

FY 2024 performance audit procedures will be performed to determine if the corrective actions being taken have been implemented and address this finding.

2023-008-AOIG, External Penetration Testing Finding - Medium Level Severity Vulnerability: *Cradlepoint – Hardcoded Credential*

Condition:

External penetration testing identified that the Cradlepoint AER1600LPE at the IP address, 64.35.224.19, is running an old firmware revision, 6.0.2 (Mon Nov 30 12:26:37 MST 2015). This firmware revision is vulnerable to exploitation of a hardcoded manufacturer password on a hardware test page to pull system configuration data. The data pulled by accessing the page with the hardcoded password, "https://64.35.224.19:8443/plt?password=W6rqCjk5ijRs6Ya5bv55",. Especially of note are the WLAN_MAC and SERIAL_NUM. In this version of the firmware, the default password for the administrative account is the last eight digits of the WLAN_MAC, "441f7819". In later versions of the device/firmware, the Serial Number is used to create the default administrative password. We confirmed that neither default password was in use on the device's administrative account. Other potentially sensitive data in this output includes the MODEM_MDN (it's phone number, 1.202.802.6191), it's IMSI number, and IMEI number. The WLAN_MAC, and SSIDs (dlink131 and AER1600-819-5g) may help an attacker physically locate the device through a service like WiGLE.NET

Criteria:

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, establishes controls for systems and organizations, including the minimum controls required by the provisions of FISMA to protect federal information and information systems.

SI-2, Flaw Remediation: (*NIST SP 800-53, Rev. 5*)
The need to remediate system flaws applies to all types of software and firmware. Organizations identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Security-relevant updates include patches, service packs, and malicious code signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of risk factors, including the security category of the system, the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw), the organizational risk tolerance, the mission supported by the system, or the threat environment. Some types of flaw remediation may require more testing than other types. Organizations determine the type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software or firmware updates is not necessary or practical, such as when implementing simple malicious code signature updates. In testing decisions, organizations consider whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

Common Weakness Enumeration (CWE)-798: Use of Hard-coded Credentials
The product contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. Hard-coded credentials typically create a significant hole that allows an attacker to bypass the authentication that has been configured by the product administrator. This hole might be difficult for the system administrator to detect. Even if detected, it can be difficult to fix, so the administrator may be forced into disabling the product entirely. There are two main variations:

- Inbound: the product contains an authentication mechanism that checks the input credentials against a hard-coded set of credentials.
- Outbound: the product connects to another system or component, and it contains hard-coded credentials for connecting to that component.

In the Inbound variant, a default administration account is created, and a simple password is hard-coded into the product and associated with that account. This hard-coded password is the same for each installation of the product, and it usually cannot be changed or disabled by system administrators without manually modifying the program, or otherwise patching the product. If the password is ever discovered or published (a common occurrence on the Internet), then anybody with knowledge of this password can access the product. Finally, since all installations of the product will have the same password, even across different organizations, this enables massive attacks such as worms to take place.

The Outbound variant applies to front-end systems that authenticate with a back-end service. The back-end service may require a fixed password which can be easily discovered. The programmer may simply hard-code those back-end credentials into the front-end product. Any user of that program may be able to extract the password. Client-side systems with hard-coded passwords pose even more of a threat, since the extraction of a password from a binary is usually very simple.

Cause:

EEOC does not have an effective policy and procures in place to enforce NIST 800-53, Rev 5, SI-2 which allowed old, exploitable firmware to run on EEOC systems..

Effect:

The remote system can be accessed using default credentials to obtain configuration information. (For additional details please see **Attachment D**, Finding E3.)

Recommendation:

We recommend that EEOC:

- Review all devices and systems and ensure default credentials are not in use.
- Implement the use of complex credentials for all systems.
- It is not possible to change this password to something complex. Consider isolating the device on a separate network segment and implementing ACLs that limit what devices and who may attach to the system.
- Determine if the management page should be publicly available. If not, implement ACLs within firewalls to limit or block all external application to the site.

- Ensure it has a policy in place to address NIST 800-53, Rev 5, SI-2.
- Ensure procedures are written in such a way to accomplish what is written in the policy.
- Ensure it has people in assigned a role to remediate flaws in accordance with its policy and risk tolerance.
- Consider how new or existing technologies it has can assist in these efforts:
  - Tracking all new systems and software being deployed;
  - Require the evaluation of the specific policy addressing NIST 800-53, Rev 5, SI-2);
  - Create an at least monthly review of all flaw remediations that meet the risk tolerance threshold and have not been remediated, to include explanations for the deviation from policy.

Managements' Response:

OIT concurs with the basis of these findings and the associated recommendations. OIT will investigate options to further validate, acceptably mitigate or remediate these findings using technology enhancements to include managerial controls to address the subject discrepancies.

For managements' complete response see ***Appendix B***.

Auditors' Response:

FY 2024 performance audit procedures will be performed to determine if the corrective actions being taken have been implemented and address this finding.

2023-009-AOIG, External Penetration Testing Finding - Medium Level Severity Vulnerability: *Information Disclosure – Internal IP and Configuration*

Condition:

External penetration testing identified that the Cradlepoint AER1600LPE at the IP address, 64.35.224.19, is running an old firmware revision, 6.0.2 (Mon Nov 30 12:26:37 MST 2015). This firmware revision is out-of-date. The default administrative page discloses potentially sensitive network and device configuration information. (For additional details please see **Attachment D**, Finding E4.)

Criteria:

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, establishes controls for systems and organizations, including the minimum controls required by the provisions of FISMA to protect federal information and information systems.

NIST SP 800-53 also provides guidance on specialized assessments for identifying and mitigating cybersecurity weaknesses, such as vulnerability scanning and penetration testing.

SI-2, Flaw Remediation: (*NIST SP 800-53, Rev. 5*)
The need to remediate system flaws applies to all types of software and firmware. Organizations identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Security-relevant updates include patches, service packs, and malicious code signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of risk factors, including the security category of the system, the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw), the organizational risk tolerance, the mission supported by the system, or the threat environment. Some types of flaw remediation may require more testing than other types. Organizations determine the type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software or firmware updates is not necessary or practical, such as when implementing simple malicious code signature updates. In testing decisions, organizations consider whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

Common Weakness Enumeration (CWE)-200: Exposure of Sensitive Information to an Unauthorized User
The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information. There are many different kinds of mistakes that introduce information exposures. The severity of the error can range widely, depending on the context in which the

product operates, the type of sensitive information that is revealed, and the benefits it may provide to an attacker. Some kinds of sensitive information include:

- private, personal information, such as personal messages, financial data, health records, geographic location, or contact details
- system status and environment, such as the operating system and installed packages
- business secrets and intellectual property
- network status and configuration
- the product's own code or internal state
- metadata, e.g. logging of connections or message headers
- indirect information, such as a discrepancy between two internal operations that can be observed by an outsider

Information might be sensitive to different parties, each of which may have their own expectations for whether the information should be protected. These parties include:

- the product's own users
- people or organizations whose information is created or used by the product, even if they are not direct product users
- the product's administrators, including the admins of the system(s) and/or networks on which the product operates
- the developer

Information exposures can occur in different ways:

- the code **explicitly inserts** sensitive information into resources or messages that are intentionally made accessible to unauthorized actors, but should not contain the information - i.e., the information should have been "scrubbed" or "sanitized"
- a different weakness or mistake **indirectly inserts** the sensitive information into resources, such as a web script error revealing the full system path of the program.
- the code manages resources that intentionally contain sensitive information, but the resources are **unintentionally made accessible** to unauthorized actors. In this case, the information exposure is resultant - i.e., a different weakness enabled the access to the information in the first place.

It is common practice to describe any loss of confidentiality as an "information exposure," but this can lead to overuse of CWE-200 in CWE mapping. From the CWE perspective, loss of confidentiality is a technical impact that can arise from dozens of different weaknesses, such as insecure file permissions or out-of-bounds read. CWE-200 and its lower-level descendants are intended to cover the mistakes that occur in behaviors that explicitly manage, store, transfer, or cleanse sensitive information.

<u>Cause</u>:

EEOC does not have an effective policy and procures in place to enforce NIST 800-53, Rev 5, SI-2 which allowed old, exploitable firmware to run on EEOC systems.

<u>Effect</u>:

By allowing out-of-date firmware revisions, EEOC discloses potentially sensitive network information from the device’s administrative page’s source code.

Recommendation:

We recommend that EEOC:

- Patch to the most recent version of firmware and confirm that this information is not disclosed from the administrative page source code.
- Determine if the management page should be publicly available. If not, implement ACLs within firewalls to limit or block all external application to the site.
- Ensure it has a policy in place to address NIST 800-53, Rev 5, SI-2.
- Ensure procedures are written in such a way to accomplish what is written in the policy.
- Ensure it has people in assigned a role to remediate flaws in accordance with its policy and risk tolerance.
- Consider how new or existing technologies it has can assist in these efforts:
    - Tracking all new systems and software being deployed;
    - Require the evaluation of the specific policy addressing NIST 800-53, Rev 5, SI-2);
    - Create an at least monthly review of all flaw remediations that meet the risk tolerance threshold and have not been remediated, to include explanations for the deviation from policy.

Managements' Response:

OIT concurs with the basis of these findings and the associated recommendations. OIT will investigate options to further validate, acceptably mitigate or remediate these findings using technology enhancements to include managerial controls to address the subject discrepancies.

For managements' complete response see ***Appendix B***.

Auditors' Response:

FY 2024 performance audit procedures will be performed to determine if the corrective actions being taken have been implemented and address this finding.

2023-010-AOIG, External Penetration Testing Finding - Medium Level Severity Vulnerability: *Information Disclosure – Internal IP and URLs*

Condition:

External penetration testing identified that various EEOC websites disclosed internal IP addresses and URLs. (See **Attachment D**, Finding E5 for where these items were identified and what additional paths are disclosed.)

Criteria:

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, establishes controls for systems and organizations, including the minimum controls required by the provisions of FISMA to protect federal information and information systems.

Common Weakness Enumeration (CWE)-200: Exposure of Sensitive Information to an Unauthorized User

The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information. There are many different kinds of mistakes that introduce information exposures. The severity of the error can range widely, depending on the context in which the product operates, the type of sensitive information that is revealed, and the benefits it may provide to an attacker. Some kinds of sensitive information include:

- private, personal information, such as personal messages, financial data, health records, geographic location, or contact details
- system status and environment, such as the operating system and installed packages
- business secrets and intellectual property
- network status and configuration
- the product's own code or internal state
- metadata, e.g. logging of connections or message headers
- indirect information, such as a discrepancy between two internal operations that can be observed by an outsider

Information might be sensitive to different parties, each of which may have their own expectations for whether the information should be protected. These parties include:

- the product's own users
- people or organizations whose information is created or used by the product, even if they are not direct product users
- the product's administrators, including the admins of the system(s) and/or networks on which the product operates
- the developer

Information exposures can occur in different ways:

- the code **explicitly inserts** sensitive information into resources or messages that are intentionally made accessible to unauthorized actors, but should not contain the information - i.e., the information should have been "scrubbed" or "sanitized"
- a different weakness or mistake **indirectly inserts** the sensitive information into resources, such as a web script error revealing the full system path of the program.

- the code manages resources that intentionally contain sensitive information, but the resources are **unintentionally made accessible** to unauthorized actors. In this case, the information exposure is resultant - i.e., a different weakness enabled the access to the information in the first place.

It is common practice to describe any loss of confidentiality as an "information exposure," but this can lead to overuse of CWE-200 in CWE mapping. From the CWE perspective, loss of confidentiality is a technical impact that can arise from dozens of different weaknesses, such as insecure file permissions or out-of-bounds read. CWE-200 and its lower-level descendants are intended to cover the mistakes that occur in behaviors that explicitly manage, store, transfer, or cleanse sensitive information.

Cause:

Source code and source code repositories are not reviewed and addressed for internal IP addresses and URLs and inappropriately stored information is not being removed.

Effect:

HTML and JavaScript source code disclosed potentially sensitive internal IP addresses and URLs.

Recommendation:

We recommend that EEOC:

- Review source code and source code repositories for code containing internal IP addresses and URLs.
- Remove inappropriately stored information from source code.

Managements' Response:

OIT concurs with the basis of these findings and the associated recommendations. OIT will investigate options to further validate, acceptably mitigate or remediate these findings using technology enhancements to include managerial controls to address the subject discrepancies.

For managements' complete response see ***Appendix B***.

Auditors' Response:

FY 2024 performance audit procedures will be performed to determine if the corrective actions being taken have been implemented and address this finding.

2023-011-AOIG, External Penetration Testing Finding - Medium Level Severity Vulnerability: *Amazon EKS API Externally Exposed – Version Information Disclosure*

Condition:

External penetration testing identified an HTTPS Service running on the IP address 54.172.87.31 associated with the Kubernetes API. A further review determined this to be a publicly exposed Amazon EKS API. (For additional details please see **Attachment D**, Finding E6.)

Criteria:

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, establishes controls for systems and organizations, including the minimum controls required by the provisions of FISMA to protect federal information and information systems.

Common Weakness Enumeration (CWE)-200: Exposure of Sensitive Information to an Unauthorized User

The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information. There are many different kinds of mistakes that introduce information exposures. The severity of the error can range widely, depending on the context in which the product operates, the type of sensitive information that is revealed, and the benefits it may provide to an attacker. Some kinds of sensitive information include:

- private, personal information, such as personal messages, financial data, health records, geographic location, or contact details
- system status and environment, such as the operating system and installed packages
- business secrets and intellectual property
- network status and configuration
- the product's own code or internal state
- metadata, e.g. logging of connections or message headers
- indirect information, such as a discrepancy between two internal operations that can be observed by an outsider

Information might be sensitive to different parties, each of which may have their own expectations for whether the information should be protected. These parties include:

- the product's own users
- people or organizations whose information is created or used by the product, even if they are not direct product users
- the product's administrators, including the admins of the system(s) and/or networks on which the product operates
- the developer

Information exposures can occur in different ways:

- the code **explicitly inserts** sensitive information into resources or messages that are intentionally made accessible to unauthorized actors, but should not contain the information - i.e., the information should have been "scrubbed" or "sanitized"
- a different weakness or mistake **indirectly inserts** the sensitive information into resources, such as a web script error revealing the full system path of the program.

- the code manages resources that intentionally contain sensitive information, but the resources are **unintentionally made accessible** to unauthorized actors. In this case, the information exposure is resultant - i.e., a different weakness enabled the access to the information in the first place.

It is common practice to describe any loss of confidentiality as an "information exposure," but this can lead to overuse of CWE-200 in CWE mapping. From the CWE perspective, loss of confidentiality is a technical impact that can arise from dozens of different weaknesses, such as insecure file permissions or out-of-bounds read. CWE-200 and its lower-level descendants are intended to cover the mistakes that occur in behaviors that explicitly manage, store, transfer, or cleanse sensitive information.

Cause:

EEOC does not limit access from specific IP addresses to the Amazon AWS EKS API and did not configure the AWS Control Tower's date residency controls to alert on publicly accessible Amazon EKS endpoints.

Effect:

The Amazon Elastic Kubernetes Service (EKS) API is publicly accessible. This allows for disclosure of the deployed version of the Kubernetes/EKS API and service health information and allows external access to the EKS environment.

Recommendation:

We recommend that EEOC:

- Limit access from specific IP addresses to the Amazon AWS EKS API.
- Configure AWS Control Tower's data residency controls to alert on publicly accessible Amazon EKS endpoints.
- If AWS Control Tower is not in use, create an AWS Config rule to detect whether an Amazon EKS endpoint is blocked from public access.

Managements' Response:

OIT concurs with the basis of these findings and the associated recommendations. OIT will investigate options to further validate, acceptably mitigate or remediate these findings using technology enhancements to include managerial controls to address the subject discrepancies.

For managements' complete response see ***Appendix B***.

Auditors' Response:

FY 2024 performance audit procedures will be performed to determine if the corrective actions being taken have been implemented and address this finding.

2023-012-AOIG, External Penetration Testing Finding - Low Level Severity Vulnerability: *Amazon EKS API Externally Exposed – Version Information Disclosure*

Condition:

External penetration testing identified that OpenText Big Data Analytics was running on federaldw.eeoc.org over the unencrypted HTTP protocol on port 8110. Since the port is not encrypted via TLS, all form fields posted to the host are unencrypted, including the username and password sent to the host during login. (For additional details please see **Attachment D**, Finding E7.)

Criteria:

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, establishes controls for systems and organizations, including the minimum controls required by the provisions of FISMA to protect federal information and information systems.

> **SC-8, Transmission Confidentiality and Integrity**: (*NIST SP 800-53, Rev. 5*)
> Protecting the confidentiality and integrity of transmitted information applies to internal and external networks as well as any system components that can transmit information, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of information can be accomplished by physical or logical means. Physical protection can be achieved by using protected distribution systems. A protected distribution system is a wireline or fiber-optics telecommunications system that includes terminals and adequate electromagnetic, acoustical, electrical, and physical controls to permit its use for the unencrypted transmission of classified information. Logical protection can be achieved by employing encryption techniques.
>
> Organizations that rely on commercial providers who offer transmission services as commodity services rather than as fully dedicated services may find it difficult to obtain the necessary assurances regarding the implementation of needed controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality or integrity services are available in standard, commercial telecommunications service packages. If it is not feasible to obtain the necessary controls and assurances of control effectiveness through appropriate contracting vehicles, organizations can implement appropriate compensating controls.

Common Weakness Enumeration (CWE)-319: Cleartext Transmission of Sensitive Information
The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors. Many communication channels can be "sniffed" (monitored) by adversaries during data transmission. For example, in networking, packets can traverse many intermediary nodes from the source to the destination, whether across the internet, an internal network, the cloud, etc. Some actors might have privileged access to a network interface

or any link along the channel, such as a router, but they might not be authorized to collect the underlying data. As a result, network traffic could be sniffed by adversaries, spilling security-critical data.

Applicable communication channels are not limited to software products. Applicable channels include hardware-specific technologies such as internal hardware networks and external debug channels, supporting remote JTAG debugging. When mitigations are not applied to combat adversaries within the product's threat model, this weakness significantly lowers the difficulty of exploitation by such adversaries.

When full communications are recorded or logged, such as with a packet dump, an adversary could attempt to obtain the dump long after the transmission has occurred and try to "sniff" the cleartext from the recorded communications in the dump itself. Even if the information is encoded in a way that is not human-readable, certain techniques could determine which encoding is being used, then decode the information.

CWE-523: Unprotected Transport of Credentials
Login pages do not use adequate measures to protect the user name and password while they are in transit from the client to the server.

<u>Cause</u>:

EEOC does not have an effective policy and procedures in place to ensure all form fields posted to the host are encrypted, including the username and password sent to the host during login.

<u>Effect</u>:

The remote web server contains several HTML form fields containing an input of type 'password', which transmit their information to a remote web server in cleartext. An attacker eavesdropping on the traffic between the web browser and server may obtain the logins and passwords of valid users.

<u>Recommendation</u>:

- We recommend that EEOC ensures that every sensitive form transmits content over HTTPS.
- Ensure it has a policy in place that addresses and enforces protects the confidentiality and/or the integrity of transmitted information.
- Ensure procedures are written in such a way to accomplish what is written in the policy, to include compensating controls.
- Ensure it has people in assigned a role to enforce the policy and procedures in place to protect the confidentiality and/or the integrity of transmitted information..
- Consider how new or existing technologies it has can assist in these efforts:
  - Tracking all new systems and software being deployed;
  - Require the evaluation of the specific policy addressing NIST 800-53, Rev 5, SC-8;

- Periodically perform checks (manually or automated) to ensure every sensitive form is transmitting content encrypted, in accordance with the policy and procedures.

Managements' Response:

OIT concurs with the basis of these findings and the associated recommendations. OIT will investigate options to further validate, acceptably mitigate or remediate these findings using technology enhancements to include managerial controls to address the subject discrepancies.

For managements' complete response see ***Appendix B***.

Auditors' Response:

FY 2024 performance audit procedures will be performed to determine if the corrective actions being taken have been implemented and address this finding.

2023-013-AOIG, Internal Vulnerability Scanning Finding – *Flaw Remediation*

Condition:

EEOC has a significant number of Level 5 and Level 4 vulnerabilities which were identified through internal vulnerability scans, the vulnerabilities increased in numbers from FY2022 to FY2023. (For specific vulnerabilities see **Attachments A and B**)

Additionally, EEOC provided a CDM/Qualys scan as April 13, 2023, in which the results identified the following, which were out of compliance with its patch policy:

- 15,211 vulnerabilities with a CVSS score of 7.0 or higher and severity rating of 4 or 5 and more than 15 calendar days old. (For specific vulnerabilities see **Attachment C**)

External penetration testing identified three findings which were a direct result of not having patched outdated software (See **NFRs 007, 008, and 009**).

Criteria:

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, establishes controls for systems and organizations, including the minimum controls required by the provisions of FISMA to protect federal information and information systems.

NIST SP 800-53 also provides guidance on specialized assessments for identifying and mitigating cybersecurity weaknesses, such as vulnerability scanning and penetration testing.

RA-5, Vulnerability Scanning: (*NIST SP 800-53, Rev. 5*)

a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;
b. Employ vulnerability monitoring 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. Analyze vulnerability scan reports and results from vulnerability monitoring;
d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;
e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and
f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

SI-2, Flaw Remediation: (*NIST SP 800-53, Rev. 5*)
The need to remediate system flaws applies to all types of software and firmware. Organizations identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Security-relevant updates include patches, service packs, and malicious code signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of risk factors, including the security category of the system, the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw), the organizational risk tolerance, the mission supported by the system, or the threat environment. Some types of flaw remediation may require more testing than other types. Organizations determine the type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software or firmware updates is not necessary or practical, such as when implementing simple malicious code signature updates. In testing decisions, organizations consider whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

The EEOC Patch Management policy stipulates the following:

Vulnerability Rating Source/ Severity	Remediation/Mitigation Requirement	
	Public-Facing	Internal
CISA KEV or VDP, etc.[1]	10 calendar days	15 calendar days
Vulnerability Rating Source/ Severity	Remediation/Mitigation Requirement	
Critical or High[2]	15 calendar days	15 calendar days

[1] Remediate each vulnerability according to the timelines set forth in the CISA-managed vulnerability catalog, BOD 22-01. See: https://www.cisa.gov/binding-operational-directive-22-01. Superseding BOD 15-01 and BOD 19-02. See: https://www.cisa.gov/sites/default/files/publications/Reducing_the_Significant_Risk_of_Known_Exploited_Vulnerabilities_211103.pdf

[2] Severity is rated using Common Vulnerability Scoring System (CVSS)

Medium	45 calendar days	90 calendar days
Low	90 calendar days	180 calendar days

Preventing access to the network is authorized on a per instance basis contingent upon the expected impact to the Agency mission.

Cause:
EEOC does not have adequate procedures in place to enforce its policy.

Effect:

The exploitable security weaknesses generated by vulnerabilities with CVSS scores of 7.0 and above and level 4 and 5 severity threaten the agency's network. Examples of threats and their potential effects include:

- The exploit of these vulnerabilities could allow attackers to execute arbitrary code and obtain full control of systems or cause a reload of the affected device(s).
- Exposure to high-risk vulnerabilities can prevent devices from servicing legitimate requests.
- A remote, unauthenticated attacker could exploit these vulnerabilities to conduct cross-site scripting attacks, elevate their privileges, execute arbitrary code, or cause a denial-of-service condition on the targeted system.

Failure to protect the agency's internal computer network from high and critical vulnerabilities could compromise the confidentiality, integrity, and availability of EEOC's information & information systems.

Recommendation:

- Ensure it has a policy in place to address NIST 800-53, Rev 5, SI-2, Flaw Remediation.
- Ensure procedures are written in such a way to accomplish what is written in the policy, for example:
    - Procures to address high risk vulnerabilities defined by the CVSS score, the severity of the vulnerability, and how many systems/endpoints are impacted;
    - Procedures to review, at least monthly, with the CIO and CISO
    - Procedures to review all vulnerabilities meeting the EEOC determined criteria and exceeding the EEOC remediation schedule, be further discussed on an at least monthly basis to better identify how to address the vulnerabilities, why the have not been patched, and if OIT has risk accepted the vulnerability;
    - Procedures to document all risk accepted vulnerabilities that meet EEOC defined criteria for high/critical;

  - Procedures for an annual review of the metrics created to address flaw remediation to address any changes to EEOC systems, risks, and processes.
- Ensure it has people in assigned roles to remediate flaws in accordance with its policy and risk tolerance.
- Consider how new or existing technologies it has can assist in these efforts:
  - Tracking all new systems and software being deployed;
  - Require the evaluation of the specific policy addressing NIST 800-53, Rev 5, SI-2);
  - Create an at least monthly review of all flaw remediations that meet the risk tolerance threshold and have not been remediated, to include explanations for the deviation from policy.

Managements' Response:

OIT concurs with the basis of these findings and the associated recommendations. OIT will investigate options to further validate, acceptably mitigate or remediate these findings using technology enhancements to include managerial controls to address the subject discrepancies.

For managements' complete response see ***Appendix B***.

Auditors' Response:

FY 2024 performance audit procedures will be performed to determine if the corrective actions being taken have been implemented and address this finding.

Informational Observations

HRK has identified additional observations that do not raise to the level of severity for reporting and formal tracking as a finding in accordance with GAGAS, but should be considered by EEOC in their overall management of its information security program.

Breached Credential Identification

Employees often use their employer email to sign up for and log in to third-party services and applications. Hackers sometimes breach these services or applications and publicly disclose user information. There is an exceedingly high likelihood that other attackers will try to use this information for credential stuffing attacks to gain access to corporate systems such as email, VPN, and other SaaS applications.

EEOC should continue to review and revise, as needed, its password policies, to include a policy that bans using EEOC email for non-EEOC related internet sites. Additionally, when EEOC is notified of breached credentials it should require notification of and changing of the breached password.

TypoSquatting

Attackers often utilize TypoSquatting techniques to register a similar-looking domain to send phishing emails or host malicious websites. These tactics usually are not noticed by the recipient. Additionally, the TypoSquatted phishing emails will usually evade filters as the domain is not spoofed.

EEOC should review, block (if necessary) and continuously monitor the complete list of already registered TypoSquatted domains. Additionally, if EEOC does not expect the need to communicate with any of the unregistered TypoSquatted domains, those domains should be proactively blocked.

Information Disclosure

Sensitive or company confidential information may be intentionally or unintentionally placed online and exposed. "Google Dorking," also known as Google Hacking, uses advanced search terms and characters to discover search results that may not easily be discovered otherwise.

EEOC should maintain awareness of publicly available information that may be purposefully or unintentionally divulged. Where possible, EEOC should try to limit information disclosure.

Open Ports

We found open ports through myriad of scans, the identified open ports, for the in-scope IPs, did not have an excessive number of service listings, a lack of which presents a minimal attach surface to adversaries.

EEOC should put firewall rules or access control lists (ACLs) in place to limit access to identified ports and IPs and only allow approves source IP addresses.

Employee Contact Information

We identified, while browsing the EEOC website various business phone numbers and email addresses for individuals and mailing lists. This information can be used to generate a list of users for password spraying attacks, as the acquisition of employee contact information is a common goal for attackers. In addition, to password spraying attacks such information can be used in social engineering campaigns.

EEOC should ensure employees who are required to have their email address or phone number listed anywhere on the EEOC website receive additional security awareness training, as they are more likely to be targets. If the information is not required to be displayed, refrain from putting phone numbers and email addresses on publicly accessible websites associated with EEOC.

SSL/TLS Configuration

We found potential insecurity with the three domains. During the scanning phase, we identified three of the IP addresses with port 443 open for SSL/TLS protected services. We reviewed the current SSL/TLS implementations of the domain names associated with these IP addresses for insecure misconfigurations. We also identified four domains where the certificate name did not match the server hostname.

EEOC should, if possible, enable secure renegotiation in the TLS configuration and the servers should be configured to reject the TLS 1 and TLS 1.1 protocols.

Foreign Travel

EEOC has a foreign policy in place within its overall Account Management policy that denies access to Office 365 resources outside the United States, unless they are deemed to have a bonified business need.

EEOC should ensure that its policy is based on risk, not only of the traveler, the location being traveled to, and the reason for travel (i.e. personal versus business). EEOC should consider what system access a traveler needs to perform their duties while on business related travel. EEOC should consider deploying GFE devices that do not contain commission data and are only able to access predetermined systems of bonified need. Additionally, any GFEs devices used for foreign travel should be subject to additional security monitoring for a set period of time (e.g. 30 days). EEOC should ensure its foreign travel policy addresses NIST SP 800-53 rev 5, CM-2 (7) and related controls.

Chief Privacy Officer

EEOC handles significant amounts of sensitive data, including privacy, PII, and PHI, associated with the casework associated with its mission. In addition, within its operations it handles employee PII across multiple offices. Any spillage of sensitive data could negatively impact EEOC’s reputation with the public.

EEOC should explore creating a Chief Privacy Officer position and corresponding Office of the Chief Privacy Officer that reports directly to the Chair and assumes primary responsibility for all aspects of privacy, from identifying risks, controls, and mitigation solutions to policy, Agency-wide.

GAO issued report GAO-22-105065, Privacy, *Dedicated Leadership Can Improve Programs and Address Challenges*[3], where it recommends Congress consider legislation to designate dedicated, senior-level privacy officials[4]. GAO states in their report "*Congress should consider legislation to designate a senior privacy official, such as a chief privacy officer, at agencies that currently lack such a position. This position should have privacy as its primary duty, the organizational placement necessary to coordinate with other agency functions and senior leaders, and the authority to ensure that privacy requirements are implemented and privacy concerns are elevated to the head of the agency*." Additionally, Congress has been advancing the American Data Privacy and Protection Act throughout FY 2022 and into FY 2023.

Vulnerability Scans

Vulnerabilities were identified from Level 1 to Level 5, the latter being the most critical and need to be addressed by EEOC. However, vulnerabilities at lower risk levels should be reviewed for impact on EEOC's systems.

EEOC should have a process in place to review all vulnerabilities identified either by internal or external scans to ensure vulnerabilities are fully addressed and the combination of vulnerabilities cannot be exploited on EEOC's systems.

[3] https://www.gao.gov/products/gao-22-105065
[4] https://www.gao.gov/products/gao-22-105065#summary_recommend

Appendix A – Status of Prior Findings

No.	Prior Year Audit Recommendations	Status
1	**FY 2022-001 FISMA Audit Recommendation No. 1:** *We recommend that EEOC defines, communicates, and implements an organization-wide SCRM strategy to guide supply chain analyses, provide communication channels with internal/external partners and stakeholders, and assist in building consensus regarding the appropriate resources for SCRM.*	Open
2	**FY 2022-002 FISMA Audit Recommendation No. 2:** *We recommend that EEOC implement strong authentication mechanisms for privileged and non-privileged users in accordance with Federal guidance, to meet the required use of PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential of the agency's networks, including remote access sessions, in accordance with Federal targets. The agency should continue developing their plans for organization-wide use of strong authentication mechanisms for non-privileged users and require multifactor authentication to network access for all user accounts.*	Open
3	**FY 2022-003 FISMA Audit Recommendation No.3:** *We recommend that EEOC review and remediate the medium level severity vulnerabilities identified during external penetration testing by:* • *Disabling IKE Aggressive Mode if supported;* • *Refraining from the use of pre-shared authentication keys;* • *If using a pre-shared key cannot be avoided, use strong keys;* • *Do not allow VPN connections from an non-approved IP addresses, if possible.*	Closed

No.	Prior Year Audit Recommendations	Status
4	**FY 2022-004 FISMA Audit Recommendation No. 4:** *We recommend that EEOC:* • *Determine if listening ports or entire system should be blocked from public access;* • *Regularly review network device search engines for new systems belonging to EEOC or those that may be masquerading as EEOC systems;* • *Perform a forensic analysis on identified system to ensure no malicious access has taken place;* • *For authorized remote sessions, create a control to address remote access being left open after the session has concluded. The controls should at minimum require the session owner to ensure the remote session was closed at the conclusion of the session as well as an overall control run on a set basis that will identify any open remote sessions on endpoints;* • *Create an auditability feature that checks internally via an agent when a device with remote access is listening;* • *Create an auditability feature that checks for remote connection software being installed.*	Closed
5	**FY 2021-002 FISMA Audit Recommendation No. 2:** *We recommend that EEOC plans and prepares to meet the goals of the TIC initiative, consistent with OMB M-19-26. The agency should define and customize, as appropriate, a set of policies, procedures, and processes to implement TIC 3.0, including updating its network and system boundary policies, in accordance with OMB M-19-26. This includes, as appropriate, incorporation of TIC security capabilities catalog, TIC use cases, and TIC overlays.*	Open
6	**FY 2021-003 FISMA Audit Recommendation No. 3:** *We recommend that EEOC consistently utilize and document POA&Ms by employing centralized automated mechanisms to help ensure that the POA&Ms for agency information systems are regularly being completed, updated, and maintained.*	Open

Appendix B – EEOC Management's Response

THIS PAGE INTENTIONALLY LEFT BLANK