U.S. International Trade Commission
OFFICE OF INSPECTOR GENERAL

FISCAL YEAR 2024 FISMA AUDIT

Report No AR-25-02

November 12, 2024

OFFICE OF INSPECTOR GENERAL

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

November 12, 2024 IG-WW-017

Commissioners:

I am pleased to transmit the U.S. International Trade Commission's (USITC) Federal Information Security Modernization Act of 2014 (FISMA) audit report (OIG-AR-25-02) detailing the results of our audit of the USITC information security program.

As prescribed by FISMA, the USITC Inspector General is required to conduct an annual assessment of USITC's security programs and practices, and to report to the Office of Management and Budget (OMB) the results of this audit. The OIG contracted with the independent certified public accounting firm, Harper, Rains, Knight & Company, P.A., to conduct an audit of USITC's information security program in support of FISMA.

Harper, Raines, Knight determined that the Commission's FY 2024 information security program was effective. USITC has maintained a managed and measurable information security program and practices, consistent with applicable FISMA requirements, Office of Management and Budget policy and guidance, Department of Homeland Security guidance, and National Institute Standards and Technology standards and guidelines. Harper, Raines, Knight identified two findings where USITC can better protect the confidentiality, integrity, and availability of its information and information systems and made two recommendations.

Harper, Rains, Knight & Company is solely responsible for the audit report dated September 17, 2024, and the conclusions expressed in the report. In connection with this contract, we reviewed Harper, Rains, Knight & Company's draft and final report and related documentation and made inquiries of its representatives. Our involvement in the audit process included monitoring audit activities, participating in discussions, reviewing audit plans, and inspecting selected documentation, conclusions, and results. Our involvement and review of Harper, Rains, Knight

& Company's work disclosed no instances where they did not comply, in all material respects, with the U.S. generally accepted government auditing standards.

Thank you for the cooperation and courtesies extended to Harper, Rains, Knight & Company and my staff during this audit.

Sincerely,

Rashmi Bartlett

Rashmi Bartlett
Inspector General

Harper, Rains, Knight & Company

PERFORMANCE AUDIT REPORT

U.S. INTERNATIONAL TRADE COMMISSION
FEDERAL INFORMATION SECURITY MODERNIZATION ACT
OF 2014 (FISMA)

FOR THE FISCAL YEAR ENDING
SEPTEMBER 30, 2024

Harper, Rains, Knight & Company, P.A.
1425 K ST NW, Suite 1120
Washington, DC 20005
202-558-5163
www.hrkcpa.com

Harper, Rains, Knight & Company

TABLE OF CONTENTS

HRK

Harper, Rains, Knight & Company

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

Rashmi Bartlett
Inspector General
U.S. International Trade Commission

This report presents the results of our independent performance audit of the U.S. International Trade Commission's (USITC) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires Federal agencies, including USITC, 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 USITC Office of Inspector General (OIG) contracted with Harper, Rains, Knight & Company, PA (HRK) to conduct a performance audit of USITC's information security program and practices for Fiscal Year (FY) 2024.

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

The objective of this performance audit was to assess the effectiveness of the USITC's information security program and practices for FY 2024. As part of our audit, we responded to the core metrics and supplemental metrics identified in the *FY 2023 -2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics (IG Metrics)*, the associated *FY 2024 Inspector General FISMA Metrics Evaluator's Guide*, and assessed the maturity levels on behalf of the USITC OIG to be managed and measurable, which we determined to be effective. We also considered applicable OMB policy and guidelines, National Institute of Standards and Technology's (NIST) standards and guidelines, and the NIST *Cybersecurity Framework (CSF), February 26, 2024*.

We determined USITC established and maintained a managed and measurable (Level 4) 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 USITC Office of the Chief Information Officer (OCIO) information security program can better protect the confidentiality, integrity, and availability of its information and information systems:

- *Lack of Business Impact Analysis Policy, Results, and Incorporation into Contingency Planning Efforts; and*
- *Lack of Security Awareness and Privacy Awareness Training*

Addressing these identified current year findings strengthens the USITC'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 USITC personnel extended to us during the execution of this performance audit.

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

Washington, D.C.
September 17, 2024

Background

The Office of the Chief Information Officer (OCIO) is responsible for planning, developing, implementing, and maintaining USITC's Information Technology (IT) program, policies, standards and procedures. The OCIO promotes the application and use of information technologies and administers policies and procedures within USITC to ensure compliance with related federal laws and regulations, to include information security. The Chief Information Officer (CIO) is the official responsible for carrying out the mission of the OCIO, which provides information technology leadership, a comprehensive services and applications support portfolio, and a sound technology infrastructure to the USITC and its customers. Organizational components include the Project Management, Software Engineering, Network Services, Service Delivery and Cybersecurity Divisions. Within the OCIO is the Chief Information Security Officer (CISO) who is the official responsible for carrying out the OCIO responsibilities under FISMA, including IT governance and security, and is the primary liaison to USITC'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 DHS authority to develop and oversee the implementation of binding operational directives to other agencies, in coordination and consistent with OMB policies and practices. FISMA also:

- Authorizes DHS to provide operational and technical assistance to other federal executive branch civilian agencies at the agency's request;
- Places the federal information security incident center (a function fulfilled by US-CERT) within DHS by law;
- Authorizes DHS technology deployments to other agencies' networks (upon those agencies' request);
- Directs OMB to revise policies regarding notification of individuals affected by federal agency data breaches;
- Requires agencies to report major information security incidents as well as data breaches to Congress as they occur and annually; and
- Simplifies existing FISMA reporting to eliminate inefficient or wasteful reporting while adding new reporting requirements for major information security incidents.

FISMA requires USITC to develop, document, and implement an agency-wide information security program to protect its information and information systems, including those provided or managed by another agency, contractor, or other source. FISMA also clearly places responsibility on each agency program office to develop, implement, and maintain a security program that assesses risk and provides adequate security for the operations and assets of programs and systems under its control.

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

Fiscal Year 2024 IG Metrics

FISMA requires each agency Inspector General (IG), or an independent external auditor, to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency. OMB, the Council of the Inspectors General on Integrity and Efficiency (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, with support from 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 USITC's information security program and practices for the period October 1, 2023, through June 30, 2024. 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 2024 Inspector General FISMA Metrics Evaluator's Guide*, and assessed the maturity levels on behalf of the USITC OIG. We also considered applicable OMB policy and guidelines, the NIST standards and guidelines, and the NIST *Cybersecurity Framework.*

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

Cybersecurity Framework Function Areas	IG FISMA Domains
Identify	Risk Management
	Supply Chain Risk Management
Protect	Configuration Management
	Identity and Access Management
	Data Protection and Privacy
	Security Training
Detect	Information Security Continuous Management
Respond	Incident Response
Recover	Contingency Planning

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

We reviewed USITC's general FISMA compliance efforts in the specific areas defined in DHS' guidance and the corresponding reporting instructions. We considered the internal control structure for USITC's systems in planning our audit procedures. Accordingly, we obtained an understanding of the internal controls over USITC'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 USITC'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; and
- Reviewed the status of recommendations in prior year FISMA evaluation reports.

The independent performance audit was conducted from April 10, 2024, through July 31, 2024. It covered the period from October 1, 2023, through June 30, 2024.

Criteria

The criteria used in conducting this audit included:

- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- FY 2023 – 2024 Inspector General (IG) Federal Information Security Modernization Act (FISMA) Reporting Metrics;
- FY 2024 IG FISMA Metrics Evaluator's Guide, v 4.0, April 30, 2024;
- NIST SP 800-12, Rev. 1, *An Introduction to Computer Security*: *The NIST Handbook*;
- NIST SP 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*;
- NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments*;
- NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*;
- NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A system Life Cycle Approach for Security and Privacy;*
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*;
- NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Federal Information Systems and Organizations;*
- NIST *Framework for Improving Critical Infrastructure Cybersecurity* v1.1;
- NIST *Cybersecurity Framework* (CSF) v1.1;
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*;
- OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*;

- OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*;
- OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*;
- OMB Memorandum M-21-30, *Protecting Critical Software through Enhanced Security Measures*;
- OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*;
- OMB Memorandum M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*;
- OMB Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*;
- OMB Memorandum M-22-09, *Moving the U.S. Government to Zero Trust Cybersecurity Principles*;
- OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*;
- OMB Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements;*
- Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*;
- DHS CISA Binding Operational Directives (BODs) and Emergency Directives (EDs);
- Federal Cybersecurity Workforce Assessment Act of 2015;
- Federal Identity, Credential, and Access Management Roadmap Implementation Guidance;
- Federal Information Processing Standard (FIPS) Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors;* and
- Other criteria as appropriate.

Results

We determined USITC's information security program to be managed and measurable, which we concluded was effective. The results of our independent performance audit concluded that USITC's information security program is generally compliant with the FISMA legislation and is consistent with the functional areas outlined in the NIST Cybersecurity Framework.

Maturity Level Scoring

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

1. Level 1 (Ad-hoc): Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
2. Level 2 (Defined): Policies, procedures, and strategies are formalized and documented but not consistently implemented.
3. Level 3 (Consistently Implemented): Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
4. Level 4 (Managed and Measurable): Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
5. Level 5 (Optimized): Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

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

Exhibit 1 — USITC Overall Maturity Level Assessment by Functions Area for Core Metrics

FISMA NIST Cybersecurity Framework Function Area	IG FISMA Domains	FY 2024 Maturity Level (Core & Supplemental Metrics)	FY 2023 Maturity Level (Core & Supplemental Metrics)
Identify	Risk Management	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)
	Supply Chain Risk Management	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)
Protect	Configuration Management	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)
	Identify and Access Management	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)
	Data Protection and Privacy	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)

FISMA NIST Cybersecurity Framework Function Area	IG FISMA Domains	FY 2024 Maturity Level (Core & Supplemental Metrics)	FY 2023 Maturity Level (Core & Supplemental Metrics)
	Security Training	Consistently Implemented (Level 3)	Managed and Measurable (Level 4)
Detect	Information Security Continuous Monitoring	Managed and Measurable (Level 4)	Consistently Implemented (Level 3)
Respond	Incident Response	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)
Recover	Contingency Planning	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)

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

Findings and Recommendations

HRK has assessed the effectiveness of USITC information system security controls and identified weaknesses. The results of our performance audit identified areas in USITC's information security program that need improvement. The findings and their associated recommendations are discussed below.

Finding 1: Lack of Business Impact Analysis Policy, Results, and Incorporation into Contingency Planning Efforts

Condition:

USITC has not developed, defined, nor completed a Business Impact Analysis (BIA) to incorporate into its contingency planning efforts.

Criteria:

FY 2024 IG Metrics; Function Area – Recover; Domain – Contingency Planning; IG-Metric-61
To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts?

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.

CP-2, Contingency Plan: (NIST SP 800-53, Rev. 5)

a. Develop a contingency plan for the system that:

1. Identifies essential mission and business functions and associated contingency requirements;
2. Provides recovery objectives, restoration priorities, and metrics;
3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;
6. Addresses the sharing of contingency information; and
7. Is reviewed and approved by [Assignment: organization-defined personnel or roles];

b. Distribute copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];

c. Coordinate contingency planning activities with incident handling activities;

d. Review the contingency plan for the system [Assignment: organization-defined frequency];

e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];

g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and

h. Protect the contingency plan from unauthorized disclosure and modification.

RA-9, Criticality Analysis: (NIST SP 800-53, Rev. 5)
Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].

ID.RA-4, Risk Assessment: (NIST CSF v1.1)
Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded

Cause:

USITC does not have a policy or procedures requiring a BIA for inclusion in its contingency planning efforts.

Effect:

Without a BIA, USITC may not correctly prioritize the resumption of mission and business functions, as well as make decisions regarding risk, priorities, security, and the budget can be impacted. Without a BIA, the CIO cannot identify and prioritize information systems and components critical to supporting the USITC's mission and business processes.

Recommendation:

We recommend that USITC:

1. Create an overall BIA policy, procedures, and processes or incorporate a BIA policy, procedures, and processes into its existing contingency planning documents.
2. Create a Template for completing BIAs consistently across the USITC following NIST SP 800-34, rev 1, Chapter 3.
3. Incorporate the BIA results into USITC's overall contingency planning efforts, as well decisions regarding risk, priorities, security, and the budget.

Managements' Response:

Management agrees with the findings and will develop management decisions to address the recommendations in the report.

For the complete response, please see Appendix A.

Finding 2: Lack of Security Awareness and Privacy Awareness Training

Condition:

HRK sampled ten USITC employees' Security Awareness Training results and found that no employees completed the training.

HRK sampled ten USITC employees Privacy Awareness Training results and found that two (2) of the ten (10) employees tested did not complete the training.

Criteria:

FY 2024 IG Metrics; Function Area – Protect; Domain – Data Protection and Privacy; IG-Metric-39
To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training?

(Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)

FY 2024 IG Metrics; Function Area – Protect; Domain – Security Training; IG-Metric-44
To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems?

(Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting)

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.

AT-1, Policy and Procedures: (*NIST SP 800-53, Rev. 5*)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
   1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and

c. Review and update the current awareness and training:
    1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
    2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

AT-2, Literacy Training and Awareness: (*NIST SP 800-53, Rev. 5*)

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):
    1. As part of initial training for new users and [Assignment: organization-defined frequency] thereafter; and
    2. When required by system changes or following [Assignment: organization-defined events];

b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques];

c. Update literacy training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

AT-3, Role-Based Training: (*NIST SP 800-53, Rev. 5*)

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities]:
    1. Before authorizing access to the system, information, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter; and
    2. When required by system changes;

b. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

PL-4, Rules of Behavior: (*NIST SP 800-53, Rev. 5*)

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;

b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;

c. Review and update the rules of behavior [Assignment: organization-defined frequency]; and

d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency]; when the rules are revised or updated].

PR.AT-2, Identity Management, Authentication, and Access Control: (*NIST CSF v1.1*) Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind

Cause:

Security Awareness Training wasn't completed because it was not rolled out via the USITC's internal Learning Management System (LMS); therefore, no employees were able to take nor complete the training.

Two (2) of the ten (10) employees sampled did not complete the required Privacy Awareness training. USITC had a breakdown in its process, where POCs monitor and follow up with employees who haven't completed the required training.

Effect:

Failure to maintain a security awareness and privacy awareness training program prevents USITC from influencing security and privacy behavior among the USITC workforce. An improperly skilled USITC workforce increases cybersecurity risks to the Commission.

Recommendation:

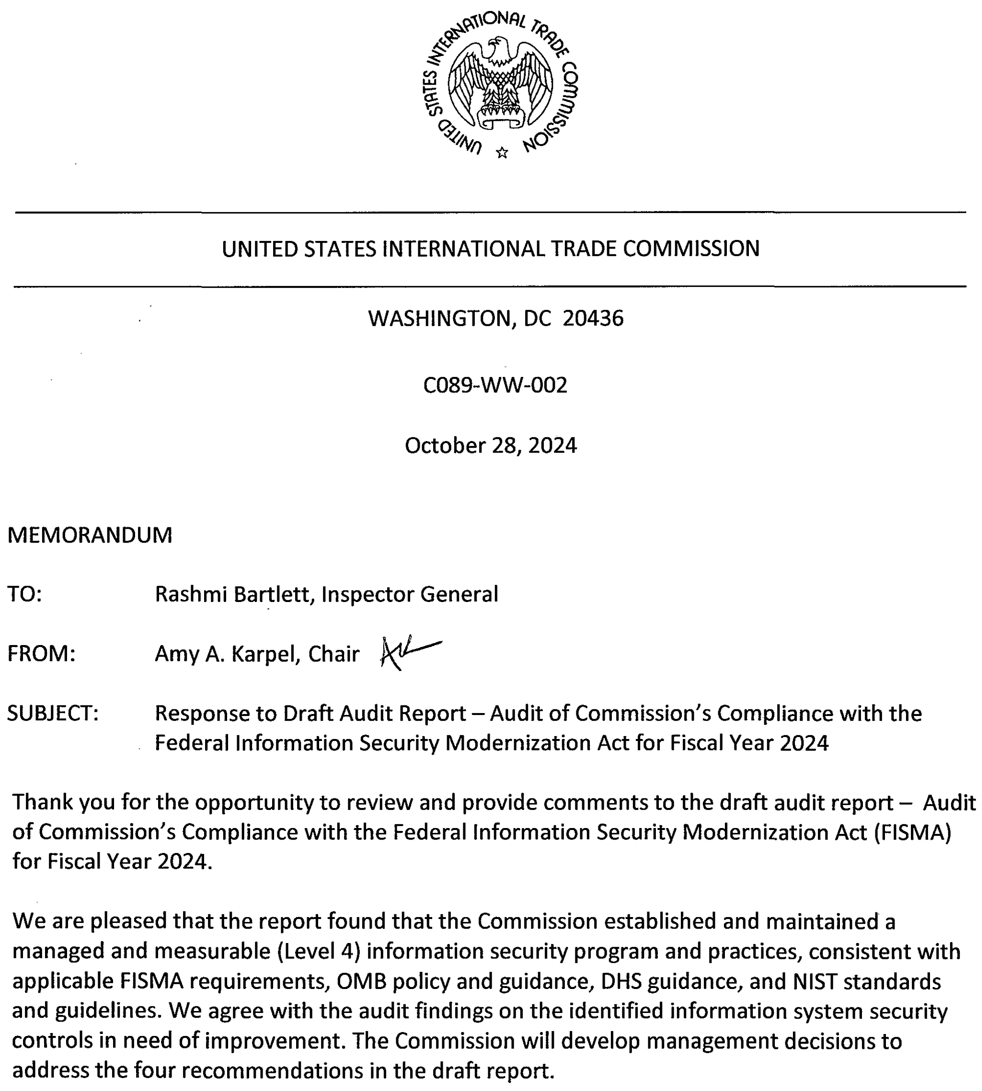
HRK recommends that USITC implement a monitoring process for required trainings at USITC so that the Commission can identify and address issues early, ensure the required trainings are delivered on time to all employees, and confirm completion.

Managements' Response:

Management agrees with the findings and will develop management decisions to address the four recommendations in the report.

For the complete response, please see Appendix A.

Appendix A — USITC Management's Response



UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

C089-WW-002

October 28, 2024

MEMORANDUM

TO: Rashmi Bartlett, Inspector General

FROM: Amy A. Karpel, Chair

SUBJECT: Response to Draft Audit Report – Audit of Commission's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2024

Thank you for the opportunity to review and provide comments to the draft audit report – Audit of Commission's Compliance with the Federal Information Security Modernization Act (FISMA) for Fiscal Year 2024.

We are pleased that the report found that the Commission established and maintained a managed and measurable (Level 4) information security program and practices, consistent with applicable FISMA requirements, OMB policy and guidance, DHS guidance, and NIST standards and guidelines. We agree with the audit findings on the identified information system security controls in need of improvement. The Commission will develop management decisions to address the four recommendations in the draft report.

U.S. International Trade Commission
Office of Inspector General
500 E Street, SW Washington, DC 20436

REPORT WASTE, FRAUD, ABUSE, OR MISMANAGEMENT

Hotline: 202-205-6542
OIGHotline@usitcoig.gov
usitc.gov/oig/hotline