



**U.S. International Trade Commission  
OFFICE OF INSPECTOR GENERAL**



# **FISCAL YEAR 2025 FISMA AUDIT**



THE INSPECTOR GENERAL



WASHINGTON, DC 20436

September 26, 2025

IG-XX-010

Commissioners:

I am pleased to transmit the U.S. International Trade Commission's (USITC or Commission) Federal Information Security Modernization Act of 2014 (FISMA) audit report (OIG-AR-25-09) 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 Office of Inspector General contracted with the independent certified public accounting firm, Harper, Rains, Knight & Company, P.A. (HRK), to conduct an audit of USITC's information security program in support of FISMA.

HRK determined that the Commission's Fiscal Year 2025 information security program was effective. USITC has maintained a managed and measurable information security program and practices, consistent with applicable FISMA requirements, OMB policy and guidance, Department of Homeland Security guidance, and National Institute of Standards and Technology standards and guidelines. HRK was able to close both findings from the [Fiscal Year 2024 audit report](#) and had no new findings in Fiscal Year 2025.

HRK is solely responsible for the audit report dated September 19, 2025, and the conclusions expressed in the report. In connection with this contract, we reviewed HRK's draft and final reports 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 HRK'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 HRK and my staff during this audit.

Sincerely,

A handwritten signature in blue ink that reads "Rashmi Bartlett". The signature is written in a cursive style with a large initial 'R'.

Rashmi Bartlett  
Inspector General

# PERFORMANCE AUDIT REPORT

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

FOR THE FISCAL YEAR ENDING  
SEPTEMBER 30, 2025

Harper, Rains, Knight & Company, P.A.  
1425 K ST NW, Suite 1120  
Washington, DC 20005  
202-558-5163  
[www.hrkcpa.com](http://www.hrkcpa.com)

# TABLE OF CONTENTS

<b>Independent Auditors' Performance Audit Report on the u.s. International Trade Commission's Compliance with Federal Information Security Modernization Act for Fiscal Year 2025 .....</b>	<b>1</b>
<b>Background .....</b>	<b>3</b>
<b>Objective, Scope, and Methodology .....</b>	<b>5</b>
<b>Results .....</b>	<b>7</b>
<b>Findings and Recommendations.....</b>	<b>8</b>
<b>Appendix A – Status of Prior Findings.....</b>	<b>9</b>
<b>Appendix B – USITC Management’s Response .....</b>	<b>10</b>





**INDEPENDENT AUDITORS' PERFORMANCE AUDIT REPORT ON THE U.S.  
INTERNATIONAL TRADE COMMISSION'S COMPLIANCE WITH FEDERAL  
INFORMATION SECURITY MODERNIZATION ACT FOR FISCAL YEAR 2025**

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) 2025.

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 2025. As part of our audit, we responded to the core metrics and supplemental metrics identified in the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics (IG Metrics)*, the associated *FY 2025 Inspector General FISMA Metrics Evaluator's Guide*, and assessed the maturity levels on behalf of the USITC OIG to be managed and measured 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) 2.0*.

**Certified Public Accountants • Consultants • [hrkcpa.com](http://hrkcpa.com)**

1052 Highland Colony Parkway, Suite 100  
Ridgeland, MS 39157  
p: 601-605-0722 • f: 601-605-0733

1425 K Street NW, Suite 1120  
Washington, DC 20005  
p: 202-558-5162 • f: 601-605-0733

Inspector General  
U.S International Trade Commission (continued)

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.

We were able to close both findings from our 2024 audit report and HRK had no new findings in FY25.

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 19, 2025

## 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 Department 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, OIG must submit to DHS the “Inspector General FISMA Reporting Metrics” that depicts the effectiveness of the agency’s information security program.

## **Fiscal Year 2025 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 2025 IG FISMA Reporting Metrics*. The *FY 2025 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.
- *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices (M-23-16)*, which reinforces the requirements established in M-22-18, reaffirms the importance of secure software development practices, and provides supplemental guidance on the scope of M-22-18’s requirements for agencies’ use of Plans of Actions and Milestones (POA&Ms) when a software provider cannot provide the required attestation, but plans to do so.

The IG FISMA metrics are aligned with the six function areas in the NIST Cybersecurity Framework 2.0: govern, identify, protect, detect, respond, and recover. The Cybersecurity Framework provides agencies with a common structure for managing and reducing their 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, 2024, through June 30, 2025. As part of our audit, we responded to the core metrics identified in the *FY 2025 Inspector General FISMA Reporting Metrics*, the associated *FY 2025 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, 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 USITC information security program and practices in accordance with Inspector General reporting requirements:

- Cybersecurity Governance (Govern)
- Cybersecurity Supply Chain Risk Management (Govern)
- Risk and Asset Management (Identify);
- Configuration Management (Protect);
- Identity 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*).

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;
- Reviewed the status of recommendations in prior year FISMA audit reports;

The independent performance audit was conducted from April 3, 2025 through July 31, 2025. It covered the period from October 1, 2024, through June 30, 2025.

## Criteria

The criteria used in conducting this audit included:

- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- FY 2025 Inspector General (IG) Federal Information Security Modernization Act (FISMA) Reporting Metrics;
- FY 2025 IG FISMA Metrics Evaluator's Guide, v 1.0, May 5, 2025;
- 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)* v2.0;
- 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-23-16, Update to Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*;
- OMB Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*;
- Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*;
- DHS CISA Binding Operational Directives (BODs) and Emergency Directives (EDs);
- Federal Cybersecurity Workforce Assessment Act of 2015;
- Federal Identity, Credential, and Access Management Roadmap Implementation Guidance;
- Federal Information Processing Standard (FIPS) Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*; and
- Other criteria as appropriate.

## Results

We assessed USITC's information security program to be managed and measured, 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**. The five maturity model levels are *ad hoc*, *defined*, *consistently implemented*, *managed and measurable*, and *optimized*.

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

FISMA NIST Cybersecurity Framework Functions Area	FY 2025 Maturity Level (Core & Supplemental Metrics)	FY 2024 Maturity Level (Core & Supplemental Metrics)
Govern	Managed and Measurable	N/A
Identify	Managed and Measurable	Managed and Measurable
Protect	Managed and Measurable	Managed and Measurable
Detect	Managed and Measurable	Managed and Measurable
Respond	Managed and Measurable	Managed and Measurable
Recover	Consistently Implemented	Consistently Implemented

Ratings in FY 2025 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 (govern, 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 no new findings in FY25. The results of our audit found that USITC successfully remediated both findings from last year. The prior year findings and overview of their remediation is below.

## APPENDIX A – STATUS OF PRIOR FINDINGS

No.	Prior Year Finding	Remediation of Finding	Prior Year Recommendations	Status
1	<b>FY24 FISMA Finding No. 1:</b> Lack of Business Impact Analysis Policy, Results, and Incorporation into Contingency Planning Efforts.	HRK verified the USITC implemented a BIA process in FY25. They implemented a BIA policy, had BIAs performed on their systems, and used the results from the BIAs to update their Contingency Plans.	<p>1. Create an overall BIA policy, procedures, and processes or incorporate a BIA policy, procedures, and processes into its existing contingency planning documents.</p> <p>2. Create a Template for completing BIAs consistently across the USITC following NIST SP 800-34, rev 1, Chapter 3.</p> <p>3. Incorporate the BIA results into USITC's overall contingency planning efforts, as well decisions regarding risk, priorities, security, and the budget.</p>	<p>Closed</p> <p>Closed</p> <p>Closed</p>
2	<b>FY24 FISMA Finding No. 2:</b> Lack of Security Awareness and Privacy Awareness Training.	HRK pulled a sample of employees at USITC and verified all employees successfully completed the Security Awareness and Privacy Awareness trainings. The agency successfully monitored trainings via USITC's internal Learning Management System (LMS) and ensured all trainings were rolled out in FY25.	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.	Closed



## **APPENDIX B – USITC MANAGEMENT’S RESPONSE**

THIS PAGE INTENTIONALLY LEFT BLANK



---

## UNITED STATES INTERNATIONAL TRADE COMMISSION

---


WASHINGTON, DC 20436

C089-XX-008

September 19, 2025

### MEMORANDUM

TO: Rashmi Bartlett, Inspector General

FROM: Amy A. Karpel, Chair  Digitally signed by AMY  
KARPEL  
Date: 2025.09.19  
08:53:01 -04'00'

SUBJECT: Response to Draft Audit Report – Audit of the Commission’s Compliance with the Federal Information Security Modernization Act (FISMA) for Fiscal Year 2025

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 2025.

The Commission agrees with the audit findings and I am pleased that the report found that the Commission 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. I am also pleased that the Commission has remedied all prior year’s findings and we will continue to strengthen the effectiveness of the Commission’s information system security controls.



**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  
<https://usitcoig.oversight.gov/report-fraud-waste-or-abuse>