Review of the Postal Regulatory Commission's Compliance With the Federal Information Security Modernization Act of 2014 for Fiscal Year 2025

AUDIT REPORT

Report Number 25-043-R25 | September 26, 2025

Highlights

Background

This report presents a review of the U.S. Postal Regulatory Commission's (PRC) information security program and practices for fiscal year (FY) 2025. The Federal Information Security Modernization Act, amended in 2014 (FISMA) requires agencies to develop, implement, and document agencywide information security programs and practices. FISMA also requires inspectors general to conduct annual reviews of their agencies' information security programs and report the results to the Office of Management and Budget.

What We Did

To meet the annual review requirement, we contracted with KPMG LLP (KPMG) to conduct this audit subject to our oversight. The audit objectives were (1) to determine the effectiveness of the PRC's information security program and practices in six framework function areas: Govern,[1] Identify, Protect, Detect, Respond, and Recover, and (2) to follow up on the status of corrective actions taken by the PRC to implement the prior year performance audit recommendations and determine whether corrective actions for open FISMA recommendations were effectively implemented.

What We Found

The PRC has made incremental advancements in its information security program since the FY 2024 FISMA audit. However, it has opportunities to continue to improve its information security program. While the PRC has developed plans of actions and milestones to address all of the recommendations from FY 2024's FISMA audit finding, policies, procedures, and processes to manage its information security program are not finalized or implemented. As a result, the IG FISMA Metrics were rated a Defined (Level 2) maturity level for the six framework functions. KPMG reported one repeat finding (see Section III) pertaining to the functions and their respective 10 metric domains.

Recommendations and Management's Comments

KPMG made two new recommendations and referenced the six open prior recommendations to address the issues identified in the report across the 10 FISMA metric domains. The PRC agreed with all recommendations. KPMG considers management's comments responsive to all recommendations, and corrective actions should resolve the issues identified in this report. See Appendix B for management's comments in their entirety.

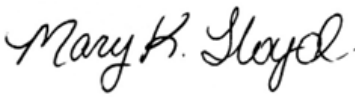
1 In FY 2025, the Office of Management and Budget (OMB) and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) introduced the Govern function, which included cybersecurity governance and cybersecurity supply chain risk management domains.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

September 26, 2025

MEMORANDUM FOR: ERICA BARKER
Secretary and Chief Administrative Officer



FROM: Mary Lloyd
Deputy Assistant Inspector General
for Operations, Performance, and Services.

SUBJECT: Audit Report – Review of the Postal Regulatory Commission's Compliance With the Federal Information Security Modernization Act of 2014 for Fiscal Year 2025 (Report Number 25-043-R25)

This report presents the results of our audit of the U.S. Postal Regulatory Commission's (PRC) Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2025.

All recommendations require U.S. Postal Service Office of Inspector General's (OIG) concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. All recommendations should not be closed in the Postal Regulatory Commission's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

We appreciate the cooperation and courtesy provided by your staff. If you have any questions or need additional information, please contact Vasilios Grasos, Director, Technology Operations, or me at 703-248-2100.

Attachment

INDEPENDENT PERFORMANCE AUDIT ON THE EFFECTIVENESS OF THE U.S. POSTAL REGULATORY COMMISSION'S INFORMATION SECURITY PROGRAM AND PRACTICES REPORT

FISCAL YEAR 2025

September 26, 2025

Contents

I. KPMG Letter 7

II. Background, Objective, Scope, and Methodology 9

Background 9

Agency Overview 9
Program Overview 9
FISMA 10
FISMA Inspector General Metrics and Reporting 10

Objective, Scope, and Methodology 13

Objective 13
Scope 13
Methodology 13
Criteria 14

III. Overall Results and Recommendations 15

Finding: Maturity Levels for Cybersecurity Functions 15
Govern 16

Cyber Governance 16
Supply Chain Risk Management 17

Identify 17

Risk Management 18

Protect 19

Configuration Management 19
Identity and Access Management 20
Data Protection and Privacy 20
Security Training 21

Detect 21

Information Security Continuous Monitoring 21

Respond 22

Incident Response 22

Recover 22

Contingency Planning 23

IV. Conclusions 24

V. Status of Prior Recommendations 25

VI. Agency Comments – Management Response to the Report 27

Appendix A – Glossary 28

Appendix B – Management's Comments 29

KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

I. KPMG Letter

United States Postal Service Office of Inspector General
1735 N. Lynn Street
Arlington, VA 22209

Secretary/Chief Administrative Officer
Postal Regulatory Commission
901 New York Avenue NW, Suite 200
Washington, DC 20268

Independent Performance Audit on the Effectiveness of the United States Postal Regulatory Commission's Information Security Program and Practices Report – Fiscal Year 2025

This report presents the results of our independent performance audit of the Postal Regulatory Commission (PRC) information security program and practices. We conducted our performance audit from February 5, 2025, through July 31, 2025, and our results are through the period of October 1, 2024, through August 1, 2025. We discussed our observations and conclusions with management on August 20, 2025, and included its comments where appropriate.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the performance audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our finding and conclusions based on our performance audit objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our performance audit objectives.

In addition to GAGAS, we conducted this performance audit in accordance with the Consulting Services Standards established by the American Institute of Certified Public Accountants (AICPA). This performance audit did not constitute an audit of financial statements, or an attestation level report as defined under GAGAS and the AICPA standards for attestation engagements.

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), the objectives of this performance audit were to:

1. Evaluate the effectiveness of the PRC's overall information technology (IT) security program by evaluating the six Cybersecurity Framework security functions outlined in the Office of Management and Budget's (OMB) Fiscal Year (FY) *2025 Inspector General (IG) Federal Information Security Modernization Act of 2014 Reporting Metrics* (IG FISMA Metrics):

    - Govern, which includes questions pertaining to Cybersecurity Governance and Cybersecurity Supply Chain Risk Management.
    - Identify, which includes questions pertaining to Risk and Asset Management.
    - Protect, which includes questions pertaining to Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training.

- Detect, which includes questions pertaining to Information Security Continuous Monitoring.
- Respond, which includes questions pertaining to Incident Response.
- Recover, which includes questions pertaining to Contingency Planning.

2. Follow up on the status of corrective actions taken by the PRC to implement the prior year performance audit recommendations and determine whether corrective actions for open FISMA recommendations were effectively implemented.[2]

As a result of our evaluation, the prior year finding remains open and we assessed the PRC's information security program as Defined (Level 2), which was ineffective according to the FY 2025 IG Metrics guidance. The PRC did close two recommendations during the year and we closed/updated one prior year recommendation; however, six remained open and we provided one new recommendation. When implemented, the eight recommendations that we made should strengthen the PRC's information security program, if effectively addressed by management.

We caution that projecting the results of our performance audit to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

This report is intended solely for the use of the PRC, the U.S. Postal Service Office of Inspector General (OIG), Department of Homeland Security, Government Accountability Office, and OMB and is not intended to be and should not be relied upon by anyone other than these specified parties.

KPMG LLP

Washington, DC
September 26, 2025

[2] Audit Report 24-097-R24, *Review of the Postal Regulatory Commission's Compliance With the Federal Information Security Modernization Act of 2014 for Fiscal Year 2025*.

II. Background, Objective, Scope, and Methodology

Background[3]

KPMG performed the FY 2025 independent FISMA evaluation under contract with United States Postal Service Office of Inspector General (USPS OIG) as a performance audit in accordance with GAGAS and AICPA Consulting Services Standards. The USPS OIG monitored our work to ensure that we met professional standards and contractual requirements.

PRC Overview

The PRC is an independent agency that exercises regulatory oversight of the United States Postal Service.[4] It is comprised of five commissioners and supported by approximately 90 employees, and its mission is to ensure transparency and accountability of the Postal Service and foster a vital and efficient universal mail system.[5] The PRC was created by the Postal Reorganization Act and assumed expanded responsibilities as a result of the Postal Accountability and Enhancement Act of 2006. The PRC regulates and approves postal rates consistent with legal criteria, advises Postal Service decision-makers on strategic decisions that could impact the nation, collects and publishes cost and service performance data, and analyzes and reports on the Postal Service's strategic plans and finances.

IT and Cybersecurity Program Overview

In August 2020, the PRC onboarded a chief information security officer (CISO) to develop and oversee its cybersecurity program. The CISO departed in April 2024 and the new CISO is expected to start August 24, 2025. In 2023, the PRC added a cybersecurity specialist to support its information security program. As of July 2025, the PRC has one individual dedicated to the cybersecurity program until the new CISO onboards.

In May 2021, the PRC hired its first chief information officer (CIO). The CIO oversees the management of information technology (IT) at the PRC. While the CISO role was vacant, the CIO managed the IT security program by overseeing the security posture of IT systems and devices throughout their lifecycle and applying government-wide IT security requirements, along with ensuring enterprise information systems are integrated and interoperable.

The CIO provides advice and assistance on IT acquisitions and ensures information resources are managed consistently with laws, executive orders, directives, policies, regulations, and priorities established by the head of the PRC. The CIO and CISO report to the Commission's Office of the Secretary and Administration, who is responsible for managing the agency's operational and administrative functions, ensuring the infrastructure and resources needed to support its mission effectively. This office oversees human resources, information technology and cybersecurity, facilities, records and privacy management, dockets management, data management, and strategic planning.

[3] The information in this section of the report is as of July 18, 2025, and is based on information obtained from a written response from the PRC and documentation provided during the course of the engagement.
[4] About the PRC (prc.gov/about).
[5] Mission, Vision, Guiding Principles, and Strategy (prc.gov/mission).

FISMA

On December 17, 2002, President George W. Bush signed FISMA[6] into law as part of the E-Government Act of 2002 (Public Law 107-347, Title III). The purpose of this act was to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets and provide a mechanism for improved oversight of federal agency information security programs. FISMA was amended on December 18, 2014, (Public Law 113-283). The amendment (1) included the reestablishment of the oversight authority of the Director of the OMB with respect to agency information security policies and practices, and (2) set forth the authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems. FISMA requires that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including assessing the risks and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems.

FISMA Inspector General Metrics and Reporting

OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), with review and feedback provided by several stakeholders, including the Federal Chief Information Officers and Chief Information Security Officers councils, released OMB's guidance for implementing the requirements outlined in OMB Memorandum (M) 25-05, Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements, outlined in the FY 2025 IG FISMA Metrics. The FY 2025 IG FISMA Metrics are aligned with the six information security functions outlined in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): Govern, Identify, Protect, Detect, Respond, and Recover. CIGIE maintained the maturity models for the following 10 FISMA Metric Domains: Cybersecurity Governance (CG), Cybersecurity Supply Chain Risk Management (CSCRM), Risk Management (RM), Configuration Management (CM), Identity and Access Management (IAM), Data Protection and Privacy (DPP), Security Training (ST), Information Security Continuous Monitoring (ISCM), Incident Response (IR), and Contingency Planning (CP). **Table 1** illustrates the alignment of the NIST Cybersecurity Framework to the FISMA Metric Domains within the FY 2025 IG FISMA Reporting Metrics.

[6] Federal Information Security Management Act of 2002 (FISMA), Pub. L. No.107-347, tit. III, Section 301, Subsection 3544(a)(1)(A), Dec. 17, 2002.

Table 1: Alignment of NIST Cybersecurity Framework to the FISMA Metric Domains

Cybersecurity Framework Functions	FISMA Metric Domains
Govern	Cybersecurity Governance Cybersecurity Supply Chain Risk Management
Identify	Risk Management
Protect	Configuration Management Identity and Access Management Data Protection and Privacy Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Source: FY 2025 IG FISMA Reporting Metrics, dated April 3, 2025, page 5.

Due to the significant changes to the IG FISMA Reporting Metrics year over year, we caution against comparing conclusions of the performance audit to previous or future years. In FY 2024, we tested the core and supplemental group 2 metrics. In FY 2025, OMB and CIGIE removed the supplemental questions in groups 1 and 2 and introduced five new supplemental metrics. Thus, in FY 2025, we tested the core metrics and the five new supplemental metrics.

Consistent with FY 2024, the models have five maturity levels: Ad-hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized. **Table 2** details the five maturity levels to assess the agency's information security program for each Cybersecurity Function.

Table 2: Inspector General Assessed Maturity Levels

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

Source: FY 2025 IG FISMA Reporting Metrics, dated April 3, 2025, page 8.

The FY 2025 IG FISMA Reporting Metrics included the removal of each Supplemental Metric from the FY 2023-FY 2024 IG FISMA Reporting Metrics. The Metrics still include both Core and Supplemental

Metrics; however, the Supplemental Metrics were tailored to the Administration's priorities. The FY 2025 IG Metrics included Core Metrics and Supplemental Metrics, as depicted in **Table 3.**

Table 3: FY 2025 FISMA Reporting Metrics

Core Metrics	Supplemental Metrics
5 - SCRM Processes	1 - Agency Cybersecurity Profiles
7 - System Inventory	2 - Cybersecurity Risk Management Strategy
8 - Hardware Inventory	3 - Cybersecurity Roles and Responsibilities
9 - Software Inventory	15 - Data Inventory
11 - Enterprise Risk Management & Risk Assessments	27 - System Integrity and Security Posture Monitoring
12 - Risk Management (RM) Dashboards and Reporting	
14 - Configuration Settings	
15 - Flaw Remediation	
17 - Multi-factor Authentication (MFA) - General Users	
18 - MFA - Privileged Users	
19 - Privileged User Account Management	
21 - Encryption	
22 - Data Exfiltration and Network Defenses	
24 - Workforce Assessment	
26 - ISCM Strategy	
28 - ISCM Processes	
30 - Incident Response Tools and Detection	
31 - Incident Response Tools and Handling	
33 - Business Impact Analysis	
34 - Information System Contingency Plan (ISCP) Test, Training, and Exercise	

Source: Analysis performed by KPMG from inspecting pages 14 – 37 of the FY 2025 IG FISMA Reporting Metrics, dated April 3, 2025.

According to the FY 2025 IG Metrics guidance, a security program is considered effective if the calculated average of the metrics in a particular domain is Managed and Measurable (Level 4) or higher. For FY 2025, a calculated average scoring model was used in which Core Metrics and Supplemental Metrics were averaged independently to determine a Domain's maturity calculation and provide data points for the assessed program and function effectiveness. The calculated averages of both the Core Metrics and Supplemental Metrics were used as a data point to support the risk-based determination of overall program and function level effectiveness. Other data points considered included the:

- Results of cybersecurity evaluations, including system security control reviews, vulnerability scanning, and penetration testing conducted during the review period.
- Progress made by agencies in addressing outstanding IG recommendations.
- Security incidents reported during the review period.

IGs should use the CyberScope[7] reporting tool to calculate the maturity levels for each cybersecurity function and domain and to submit the results of the IG Metrics evaluation. CyberScope provides supplementary fields to allow explanatory comments; IGs may use these fields to provide additional data supporting the Core Metrics evaluation results and ultimately provide the overall effectiveness of the agency's information security program.

Objective, Scope, and Methodology

Objective

Consistent with FISMA and OMB requirements, the objective of this performance audit was to determine the effectiveness of the PRC's information security program. Specifically, the performance audit objectives were to:

1. Evaluate the effectiveness of the PRC's overall IT security program by evaluating the six cybersecurity framework security functions outlined in the OMB's FY 2025 IG Metrics:

    - Govern, which includes questions pertaining to Cybersecurity Governance and Cybersecurity Supply Chain Risk Management.
    - Identify, which includes questions pertaining to Risk and Asset Management.
    - Protect, which includes questions pertaining to Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training.
    - Detect, which includes questions pertaining to Information Security Continuous Monitoring.
    - Respond, which includes questions pertaining to Incident Response.
    - Recover, which includes questions pertaining to Contingency Planning.

2. Follow up on the status of corrective actions taken by the PRC to implement the prior year performance audit recommendations and determine whether corrective actions for open FISMA recommendations were effectively implemented.[8]

The period for the performance audit was October 1, 2024, through July 31, 2025. Specifically, we assessed the PRC's performance in the six cybersecurity functions outlined in the FY 2025 IG Metrics. Our results for this testing are as of August 1, 2025. We conducted our fieldwork from February 5, 2025, through July 31, 2025. As part of our performance audit, we responded to the FY 2025 IG FISMA Reporting Metrics on the USPS OIG's behalf to assess maturity levels.

Scope

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation, FY 2025 IG FISMA Reporting Metrics, applicable NIST standards and guidelines, presidential directives, OMB memoranda referenced in the reporting metrics, and PRC information security policy directives. We assessed the PRC's information security program as well as the implementation of program-level policies and procedures for the PRC's information system selected for testing.

Methodology

We conducted this performance audit in accordance with GAGAS, which requires that we obtain sufficient, appropriate evidence to provide a reasonable basis for our finding and conclusions based on

[7] CyberScope, operated by DHS on behalf of OMB, is a web-based application designed to streamline information technology security reporting for Federal agencies. It gathers and standardizes data from Federal agencies to support FISMA compliance. In addition, Offices of Inspectors General provide an independent assessment of effectiveness of an agency's information security program. Offices of Inspectors General must also report their results to DHS and OMB annually through CyberScope.

[8] *Supra* note 1.

our audit objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objectives.

In addition to GAGAS, we conducted this performance audit in accordance with Consulting Services Standards established by the AICPA. This performance audit did not constitute an audit of financial statements, or an attestation level report as defined under GAGAS and the AICPA standards for attestation engagements.

We requested that PRC management provide a self-assessment of maturity levels for the FY 2025 IG Metrics to help us gain a better understanding of how the organization implemented relevant security controls and processes for the 25 metrics in scope. The PRC's responses allowed us to focus our meetings and confirm gaps that management identified. This also helped in requesting appropriate artifacts and meetings so that we could perform our audit procedures and conduct an independent assessment of the maturity levels.

Our procedures to assess the effectiveness of the information security program and practices of the PRC included the following:

- Inquiry of PRC CIO, system administrators, and other relevant control operators to walk through control processes applicable to each metric.
- Inspection of PRC information security policies, procedures, and guidelines established and disseminated by the PRC.

We conducted our fieldwork from February 5, 2025, through July 31, 2025. We provided updates during observations for each function and discussed the metric results with PRC management.

Criteria

We focused our FISMA performance audit approach on federal information security guidance developed by NIST, OMB, and the Government Accountability Office or applicable laws or presidential directives referenced in the FY 2025 IG FISMA Reporting Metrics. NIST Special Publications (SPs) establish guidelines that are essential to the development and implementation of federal security programs. We included the specific criteria applicable to each finding identified in FY 2025 in the "Overall Results and Recommendations" section of this report.

III. Overall Results and Recommendations

Finding: Maturity Levels for Cybersecurity Functions

Overall, the PRC proactively improved its information security posture in FY 2025 by performing the following actions:

- Designed and implemented policies and procedures for IAM and ISCM.
- Continued to develop information security policies and procedures.
- Continued to draft and update the PRC's general support system (GSS) security plan (SSP).
- Leveraged Department of Justice's (DOJ) Security Operations Center (JSOC) Shared Services for monitoring the PRC GSS for cybersecurity incidents and implemented a draft process to respond and report incidents from DOJ JSOC.

However, based on the ratings for each metric and associated averages calculated in CyberScope, we identified areas of improvement for the PRC's information security program in each cybersecurity function (Govern, Identify, Protect, Detect, Respond, and Recover). **Table 4** below depicts assessed maturity levels for each cybersecurity function. Overall, the PRC has made incremental advancements in its information security program. Specifically, in the prior fiscal year, the PRC was assessed as Ad Hoc (Level 1), but this year it has improved to Defined (Level 2).

PRC management stated that information security policies, procedures, and processes were not fully implemented, but PRC is actively working on implementing them and to fill the CISO vacancy. PRC has limited resources that were tasked with performing operational activities. The policies and procedures have been drafted but not approved by PRC leadership.

Table 4: Maturity Levels for Cybersecurity Functions

Cybersecurity Function/Metric	Assessed Maturity
Govern (CG and SCRM)	Ad-hoc (Level 1)
Identify (RM)	Defined (Level 2)
Protect (CM, IAM, DPP, and ST)	Defined (Level 2)
Detect (ISCM)	Consistently Implemented (Level 3)
Respond (IR)	Consistently Implemented (Level 3)
Recover (CP)	Defined (Level 2)

Source: CyberScope IG FISMA Report, dated July 31, 2025.

Govern

According to the FY 2025 IG Metrics guidance, the objective of the Govern function in the NIST Cybersecurity Framework is to develop and implement organizational structure, policies, and procedures necessary to manage and oversee the cybersecurity risk management activities. It involves:

- Establishing and communicating the governance structure.
- Defining roles and responsibilities.
- Ensuring that policies and procedures are implemented and followed.
- Aligning cybersecurity risk management with business objectives.
- Monitoring and evaluating the effectiveness of governance activities.

This function is carried out through proper CG and SCRM control processes.

Cyber Governance

The FY 2025 IG metrics guidance states that CG requires agencies to develop policies, procedures, and programs to manage cybersecurity leadership, accountability, and alignment with organizational priorities. The overall goal is to create a robust governance structure that supports effective cybersecurity risk management and aligns with the organization's overall strategic goals.

Based on the results of our performance audit procedures, the PRC has not designed or implemented CG policies and procedures. Specifically, the PRC has not:

- Developed and implemented agency-wide CG policy, procedures, and processes that address the applicable NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations,* Revision (Rev.) 5.1, Release (Rel.) 5.1.1, control requirements.
- Implemented a cybersecurity risk management strategy and performance measures used to assess the effectiveness of their cybersecurity risk management strategy.
- Provided training to individuals on how to detect counterfeit system components or developed processes to determine if equipment or software purchased contains counterfeit components.

OMB Circular A-130 "Managing Information as a Strategic Resource" mandates organizations to establish comprehensive information management policies, including cybersecurity profiles to align cybersecurity efforts with organizational goals and support strategic priorities. It requires a risk management framework that integrates cybersecurity risk management into overall operational risk decisions, ensuring informed and supported decision-making processes. Additionally, the circular emphasizes the assignment of roles, responsibilities, and authorities in information security, promoting accountability and continuous improvement through regular evaluations and performance assessments to foster effective cybersecurity governance.

NIST SP 800-53, Rev. 5.1, Rel. 5.1.1, requires the PRC to implement controls that:

- Develop a comprehensive strategy to manage security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; implement the risk management strategy consistently across the organization; and review and update the risk management strategy to address organizational changes. (PM-9)
- Identify and document assumptions, constraints, and priorities affecting risk assessments, risk responses, and risk monitoring. (PM-28)
- Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance. (RA-8)

Without formally established CG policies, procedures, and processes, the PRC is not aligning its mission objectives with cybersecurity risk, tolerance, and mitigation strategies to minimize risk to PRC data and resources.

Recommendation 1
We recommend the Secretary and Chief Administrative Officer, in coordination with the Chief Information Security Officer, design and implement Cyber Governance policies, procedures, and processes that address National Institute of Standards and Technology Special Publication 800-53, Rev. 5.1, Rel. 5.1.1 control requirements and OMB Circular A-130.

Supply Chain Risk Management

According to the FY 2025 IG Metrics guidance, SCRM requires agencies to develop policies, procedures, and programs to manage supply chain risks associated with system development, acquisition, maintenance, and disposal. This includes monitoring third-party vendors and service providers and helping to ensure appropriate contractual requirements are included for acquisitions.

Based on the results of our performance audit procedures, the PRC has not designed or implemented SCRM policies and procedures. Specifically, the PRC:

- Has not developed and implemented agency-wide SCRM policy, procedures, and processes that address the applicable NIST SP 800-53, Rev. 5.1, Rel. 5.1.1, control requirements.
- Does not have a formal process to monitor third-party providers' (contractor system and cloud service providers [CSPs]) adherence to PRC security requirements. This would include reviewing relevant security information on defined timeframes.

OMB Circular A-130 requires that agencies implement information security programs that include the organization's security control requirements for contractor information systems used for the organization's mission.

The SECURE Technology Act of 2018 and OMB Memorandum 22-18, "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices," require an organization to develop an overall SCRM strategy and implementation plan, policy, and processes to guide and govern SCRM activities that include both hardware and software. NIST SP 800-53, Rev. 5.1, Rel. 5.1.1, requires the PRC to implement controls that:

- Require contracts for information services to outline the security control requirements and documentation needed (SA-4).
- Establish policy, management plan, tools, and assessment processes (SR-1 through SR-3, SR-5, and SR-6).

Without having formally established SCRM policies, procedures, and processes, the PRC could be using services from a third party that do not meet the PRC's information security requirements and be exposing its data and resources to threats and vulnerabilities. In addition, the PRC could be using counterfeit components that could put PRC data at risk.

The recommendation from FY 2024 to address this issue is still open (see Section V, Recommendation 2).

Identify

The FY 2025 IG Metrics guidance states that the objective of the Identify function in the NIST Cybersecurity Framework is to understand and manage cybersecurity risks to systems, people, assets, data, and capabilities within the PRC. Understanding cybersecurity risks enables an agency to focus and

prioritize efforts consistent with its risk management strategy and business needs. This function is carried out through proper RM processes.

Risk Management

FISMA requires federal agencies to establish an information security program that protects the systems, data, and assets commensurate with their risk environment. RM is the process of identifying, assessing, and controlling threats to an organization's operating environment. These threats or risks could stem from various sources, including budget uncertainty, natural disasters, and cybersecurity threats. A sound RM plan and program that addresses these risks can aid the PRC in establishing an information security program.

Based on the results of our performance audit procedures, we determined that PRC management implemented tools to monitor and collect information of hardware and software assets that are connected to the PRC network. PRC management is also tracking plans of actions and milestones (POA&M) of weaknesses management self-identified through system accreditation and assessments and other internal and external reviews. PRC developed a draft SSP that is still being reviewed and updated to reflect the current environment.

However, the PRC has not designed or implemented agency-wide RM policies, procedures, or processes that address NIST SP 800-53, Rev. 5.1, Rel. 5.1.1, Security and Privacy Controls for Information Systems and Organizations, security control requirements. Specifically:

- While PRC management documented its information systems used to support the mission in a flow chart, it does not have a policy in place that defines what is a PRC or contractor (third-party, including CSPs) information system or have an inventory with relevant information (for example, Federal Information Processing Standards rating, ownership, certification and accreditation status, and interconnections).
- The PRC does not have RM policies and procedures that identify baseline security controls and tailoring requirements for information systems.
- The PRC GSS SSP does not specifically address the relevant NIST SP 800-53, Rev. 5.1, Rel. 5.1.1., security controls for a Federal Information Processing Standards -199 Moderate information system. Furthermore, for the GSS, the PRC has not documented policies and procedures for all NIST SP 800-53 control families. However, a POA&M has been created for this control gap.
- The PRC did not perform or document a risk assessment for the GSS as part of the certification and accreditation process.
- The PRC does not use a cybersecurity risk register to provide stakeholders insight into the cybersecurity risks that impact the PRC enterprise risk.
- The PRC does not integrate its SCRM process with its security architecture to manage risk with new assets attached to the GSS.
- The PRC has not implemented a governance risk and compliance tool to provide a centralized enterprise-wide view of cybersecurity risk management.

NIST SP 800-39, *Managing Information Security Risk,* and NIST SP 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems,* outline the requirements for risk assessments and system security plans that are used in the authorization to operate process. OMB Circular A-130, Appendix I, Section 5, states, for non-national security programs and information systems, organizations must apply NIST guidelines unless otherwise stated by OMB. Also, for legacy information systems, organizations are expected to meet the requirements of and comply with NIST standards and guidelines within one year of their respective publication dates, unless otherwise directed by OMB.

The lack of RM policies, procedures, processes, and system security plans that address NIST SP 800-53, Rev 5.1, Rel 5.1.1, security requirements and other NIST and OMB guidance expose the PRC to

information security risks, including unauthorized access, data breaches, and non-compliance with federal standards and regulations. This may lead to financial loss and reputational damage due to the inability to adequately identify, access, and manage IT security risks.

Recommendation 2
We recommend the Secretary and Chief Administrative Officer, in coordination with the Chief Information Security Officer, design and implement risk management and general support system policies, procedures, and processes that address National Institute of Standards and Technology Special Publication 800-53, Rev. 5.1, Rel. 5.1.1 control requirements and standard industry practices from the National Institute of Standards and Technology Special Publications 800-39 and 800-18. This includes developing and implementing a system security plan for the Postal Regulatory Commission's general support system.

Protect

The FY 2025 IG Metrics states that the objective of the Protect function in the NIST Cybersecurity Framework is to develop and implement appropriate safeguards to ensure the delivery of critical services of organizations. The Protect function supports an organization's ability to limit, contain, or prevent the impact of a cybersecurity event. This function is carried out through proper CM, IAM, DPP, and ST processes.

Configuration Management

FISMA requires agencies to develop an information security program that includes policies and procedures to ensure compliance with minimally acceptable system security configuration requirements. CM refers to processes used to control changes or patches to information systems (for example, change management and patch management) to establish and maintain the integrity of the systems and their underlying data.

Based on the results of our performance audit procedures, we determined that the PRC has implemented tools to scan hardware assets for security baseline configuration compliance and vulnerabilities and to automate the security patching process.

However, the PRC has not designed or implemented agency-wide CM policies, procedures, and processes that address the applicable NIST SP 800-53, Rev. 5.1, Rel. 5.1.1, control requirements, including:

- CM roles and responsibilities.
- A process to review vulnerability scan results and the actions to take, including establishing POA&Ms, as necessary.

NIST SP 800-128, "Guide for Security-Focused Configuration Management of Information Systems," recommends that an organization apply CM standards for establishing baselines and for tracking, controlling, and managing many aspects of business development and operation of services. According to NIST SP 800-128, an agency is responsible for "including policies and procedures that ensure compliance with minimally acceptable system configuration requirements, as determined by the agency" within its information security program and the supporting controls CM-1 through CM-9 in NIST SP 800-53 Rev. 5.1, Rel. 5.1.1.

Without having approved and implemented policies, procedures, and processes around the roles and responsibilities, individuals may not be aware of their job responsibilities and inadvertently expose the PRC to internal and external threats and vulnerabilities. By not documenting reviews of vulnerability scans, PRC management does not have assurance that a patch and/or configuration changes may be appropriately applied to the GSS.

The recommendation from FY 2024 to address this issue is still open (see Section V, Recommendation 3).

Identity and Access Management

According to the FY 2025 IG Metrics, IAM requirements dictate that agencies implement capabilities to ensure that information system users can only access data required for their job functions (for example, "need-to-know"), in accordance with the principles of separation of duties and least privilege. Aspects of the IAM program include screening personnel, issuing and maintaining user credentials, and managing logical and physical access rights.

Based on the results of our audit procedures, we determined that PRC management uses strong authentication mechanisms to the GSS for privileged and non-privileged users that require multi-factor authentication. We also did not identify any testing exception with the PRC's remote access controls. PRC did implement IAM policies and processes that addressed the prior recommendation. We performed authorization testing for a selection of new privileged and non-privileged GSS users and noted no exceptions. We also noted no exceptions with PRC's reauthorization of the privileged GSS users.

Data Protection and Privacy

Per the FY 2025 IG Metrics, DPP refers to a collection of activities focused on preserving the confidentiality, integrity, and availability of information systems and their underlying data through proper access restrictions and protections against unauthorized disclosure of information. Effectively managing risks associated with the creation, collection, use, maintenance, dissemination, disclosure, and disposal of personally identifiable information (PII) depends on the safeguards in place for the information systems that process, store, and transmit this information. OMB Circular A-130, requires federal agencies to develop, implement, and maintain enterprise-wide privacy programs that align with the NIST Risk Management Framework to protect PII and other sensitive data. The head of each federal agency is ultimately responsible for managing PII and ensuring that privacy is protected for the agency. Executive Order 13719, *Establishment of the Federal Privacy Council,* requires agency heads to designate a senior agency official for privacy who has agency-wide responsibility and accountability for the agency's privacy program.

Based on the results of our performance audit procedures, we determined that PRC management implemented controls to encrypt data at rest and in transit and implemented a data breach response plan and continuity of operations plan.

However, the PRC has not designed or implemented agency-wide DPP policies, procedures, and processes that address relevant NIST SP 800-53, Rev 5.1, Rel 5.1.1, control requirements. In addition, the PRC has not:

- Implemented security controls and tools to prevent sensitive data from being transferred from the PRC network.
- Provided role-based, privacy-based training to individuals that oversee and manage the privacy program.

Executive Order 14208, *Improving the Nation's Cybersecurity*, requires an organization to implement incremental improvements to security to protect the systems that process and store data. NIST SP 800-53. Rev 5.1, Rel 5.1.1., requires that an organization implement system monitoring controls to monitor inbound and outbound traffic (SI-4) and specialized training (AT 2 and 3).

Without implementing formal DPP policies, procedures, and processes, the PRC may not be aware if sensitive data is being removed in an unauthorized manner. Without role-based privacy training,

individuals responsible for resolving data privacy incidents may not know what they should do, who to contact, and what security measures they need to take to mitigate unauthorized disclosures.

The recommendation from FY 2024 to address this issue is still open (see Section V, Recommendation 5).

Security Training

ST is a cornerstone of a strong information security program, as it helps prepare both privileged and non-privileged information systems users to limit exposure of PRC systems and data to unnecessary risk while performing their job duties.

Based on the results of our performance audit procedures, we determined that PRC management provided and monitored ST training for all employees.

However, the PRC has not designed or implemented agency-wide ST policies, procedures, and processes that address relevant NIST SP 800-53, Rev 5.1, Rel 5.1.1, control requirements. Specifically, management has not performed a workforce assessment to identify gaps in skills, knowledge, abilities, and positions to support information security. Management also has not developed requirements for specialized security training requirements for individuals with significant security roles.

The Federal Cybersecurity Workforce Assessment Act of 2015 requires an organization to identify individuals that perform cybersecurity related functions and report to the Office of Personnel Management on an annual basis the critical needs to support the cybersecurity workforce. NIST SP 800-53, Rev 5.1, Rel. 5.1.1, requires providing organization-wide and role-based training for individuals that require specialized training (AT-2 and 3).

The absence of specialized training for key security roles leaves the PRC vulnerable to sophisticated threats, and personnel may not be equipped to perform the immediate actions required to address these issues, to protect the PRC's data and systems, and to ensure the ongoing integrity and security of its operations.

The recommendation from FY 2024 to address this issue is still open (see Section V, Recommendation 6).

Detect

According to the FY 2025 IG Metrics, the objective of the Detect function in the NIST Cybersecurity Framework focuses on the timely discovery of cybersecurity events. This function is critical to a robust information security program as the effects of cybersecurity events can be mitigated more quickly if they are identified in a timely manner. The NIST Cybersecurity Framework states that ISCM processes should be used to detect anomalies and continuously monitor information systems across the enterprise to identify events. The Detect function is carried out through ISCM tools and processes intended to promote timely identification of cybersecurity events.

To further enhance federal agencies' ISCM capabilities, Congress established the Continuous Diagnostics and Mitigation Program in 2012. The Continuous Diagnostics and Mitigation Program supports agency efforts to identify cybersecurity risks on an ongoing basis and prioritize risks based on potential impact.

Information Security Continuous Monitoring

Based on the results of our performance audit procedures, we noted that PRC management has implemented their ISCM plan that includes active scanning to identify threats. PRC is using the Department of Justice (DOJ) Justice Security Operations Center (JSOC) that performs monitoring an

analysis via Continuous Diagnostics and Mitigation (CDM) tools. This is in addition to the on-premises tools that the PRC CIO and team review on a weekly basis.

Respond

The FY 2025 IG Metrics states that the objective of the Respond function in the NIST Cybersecurity Framework is to develop and implement actions to be taken when a cybersecurity event has been detected. Such actions include establishing proper incident response (IR) plans and procedures to be executed during and after incidents, conducting analysis to determine the impact of incidents and mitigation to contain (i.e., prevent expansion) and resolve incidents, managing communications with relevant stakeholders during and after incidents, and incorporating lessons learned into the incident response program. FISMA requires agencies to document and implement an enterprise-wide IR program.

Incident Response

Based on the results of our performance audit procedures, we determined that PRC management is using the DOJ JSOC to monitor their GSS for security incidents. We tested all five security incidents that were reported to PRC for follow-up and determined that the PRC was following processes outlined in its draft policies and procedures.

However, PRC management has not implemented agency-wide IR policies, procedures, and processes that address applicable NIST SP 800-53, Rev. 5.1, Rel. 5.1.1, control requirements. Specifically, while the PRC is in the drafting stage of their IR strategy and is implementing these policies throughout their organization, PRC has not finalized these policies and procedures.

FISMA requires an agency to establish incident response capabilities that include:

- Creating an incident response policy and plan.
- Developing procedures for performing incident handling and reporting.
- Setting guidelines for communicating with outside parties regarding incidents.
- Selecting a team structure and staffing model.
- Establishing relationships and lines of communication between the incident response team and other groups, both internal (for example, legal department) and external (for example, law enforcement agencies).
- Determining what services the incident response team should provide.
- Staffing and training the incident response team.

PRC management did not fully assess the risk of not having formal policies, procedures, and processes defining IR roles and responsibilities for security incidents that are reported to management from the DOJ, and it did not finalize IR policy and procedures. Without a formally established IR program in place, the PRC may not appropriately identify incidents and respond to them in an appropriate manner to mitigate vulnerabilities, exposures, and attacks.

The recommendation from FY 2024 to address this issue is still open (see Section V, Recommendation 8).

Recover

According to the FY 2025 IG FISMA Metrics, the objective of the Recover function in the NIST Cybersecurity Framework is to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident or other disaster. Activities that are part of this function, such as contingency planning, support timely recovery to normal operations, and reduce the impact from an incident or disaster.

Contingency Planning

Based on the results of our performance audit procedures, we determined that PRC management completed the business impact analysis for the GSS. However, PRC management has not designed or implemented agency-wide CP policies, procedures, and processes that address NIST SP 800-53, Rev.5.1, Rel. 5.1.1, control requirements. Specifically, the PRC has not developed or documented the GSS CP, tested the plan for effectiveness, and made improvements to the CP based on the test results.

NIST SP 800-53, Rev. 5.1, Rel 5.1.1. requires an organization to develop, implement, and test its contingency plan and provide training to individuals that support the contingency plan when it is activated (CP-2 through 5). NIST SP 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems, provides an organization with the resources needed to develop and document an information system contingency plan to recover IT systems and resume business operations in the event of a disaster, major system outage, or large-scale security incident.

Without a formal CP program and developing and testing the GSS CP, management does not have assurance that it can recover IT systems and resume business operations in the event of a disaster, major outage, or large-scale security incident.

The recommendation from FY 2024 to address this issue is still open (see Section V, Recommendation 9).

IV. Conclusions

PRC management has maintained an information security program and practices based on informal policies and processes to manage security for its information system for the 6 cybersecurity functions and 10 FISMA metric domains. We assessed the PRC's information security program as not effective in CyberScope; this determination was made because the FY 2025 IG FISMA Reporting Metrics and the associated calculated averages for the metric domains and cybersecurity functions were assessed as Defined (Level 2). We reported one finding that impacted each of the 6 functions and 10 domains.

We recommend PRC management finalize its remaining draft policies, procedures, and processes and define qualitative and qualitative measures to evaluate the effectiveness of its information security program on a regular basis. In addition, the PRC should identify an individual to assume the CISO responsibilities to oversee the information security program and practices. Management's verbatim comments will be included in Appendix B.

V. Status of Recommendations

FY	Number	Recommendation	Status
2025	1	We recommend the **Secretary and Chief Administrative Officer**, in coordination with the **Chief Information Security Officer**, design and implement Cyber Governance policies, procedures, and processes that address National Institute of Standards and Technology Special Publication 800-53, Rev. 5.1, Rel. 5.1.1 control requirements and OMB Circular A-130.	Open
2025	2	We recommend the **Secretary and Chief Administrative Officer**, in coordination with the **Chief Information Security Officer**, design and implement risk management and general support system policies, procedures, and processes that address National Institute of Standards and Technology Special Publication 800-53, Rev. 5.1, Rel. 5.1.1 control requirements and standard industry practices from the National Institute of Standards and Technology Special Publications 800-39 and 800-18. This includes developing and implementing a SSP for the PRC GSS.	Open

FY	Number	Recommendation	Status
2024	1	We recommend the Secretary and Chief Administrative Officer, in coordination with the Chief Information Officer, design and implement risk management and general support system policies, procedures, and processes that address National Institute of Standards and Technology Special Publication 800-53, Rev. 5.1, Rel. 5.1.1, control requirements.	Closed
2024	2	We recommend the Secretary and Chief Administrative Officer, in coordination with the Chief Information Officer, design and implement Supply Chain Risk Management policies, procedures, and processes that address National Institute of Standards and Technology Special Publication 800-53, Rev. 5.1, Rel. 5.1.1, control requirements.	Open
2024	3	We recommend the Secretary and Chief Administrative Officer, in coordination with the Chief Information Officer, develop and implement agency-wide Configuration Management policies, procedures, and processes, that address applicable National Institute of Standards and Technology Special Publication 800-53, Rev. 5.1, Rel. 5.1.1, control requirements.	Open
2024	4	We recommend that the Secretary and Chief Administrative Officer, in coordination with the Chief Information Officer, develop and implement agency-wide identity access management policies, procedures, and processes that address applicable National Institute of Standards and Technology Special Publication 800-53, Rev 5, Rel. 5.1.1, control requirements.	Closed

FY	Number	Recommendation	Status
2024	5	We recommend that the Secretary and Chief Administrative Officer, in coordination with the Chief Information Officer, develop and implement agency-wide data protection and privacy policies, procedures, and processes that address applicable National Institute of Standards and Technology Special Publication 800-53, Rev. 5, Rel. 5.1.1 control requirements.	Open
2024	6	We recommend that the Secretary and Chief Administrative Officer, in coordination with the Chief Information Officer, develop and implement agency-wide Security Training policies, procedures, and processes that address applicable National Institute of Standards and Technology Special Publication 800-53, Rev. 5.1, Rel. 5.1.1, control requirements.	Open
2024	7	We recommend that the Secretary and Chief Administrative Officer, in coordination with the Chief Information Officer, finalize and implement its Information Security Continuous Monitoring plan and update the plan and any additional procedures and processes to address applicable National Institute of Standards and Technology Special Publication 800-53, Rev. 5, Rel. 5.1.1, control requirements.	Closed
2024	8	We recommend that the Secretary and Chief Administrative Officer, in coordination with the Chief Information Officer, develop and implement agency-wide incident response policies, procedures, and processes that address applicable National Institute of Standards and Technology Special Publication 800-53, Rev. 5, Rel 5.1.1, control requirements.	Open
2024	9	We recommend that the Secretary and Chief Administrative Officer, in coordination with the Chief Information Officer, develop and implement agency-wide contingency planning policies, procedures, and processes that address applicable National Institute of Standards and Technology Special Publication 800-53, Rev. 5, Rel 5.1.1, control requirements.	Open

VI. Agency Comments – Management Response to the Report

Postal Regulatory Commission Response

The Postal Regulatory Commission agreed to our finding and agreed with recommendations 1 and 2.

For recommendation 1, management agreed and stated it will design and implement cyber governance policies, procedures, and processes that meet the National Institute of Standards and Technology Special Publication 800-53, Rev. 5.1, Rel. 5.1.1 control requirements and OMB circular A-130. The target implementation date is September 11, 2026.

For recommendation 2, management agreed and stated it will design and implement risk management and general support system policies, procedures, and processes that meet the National Institute of Standards and technology Special Publication 800-53, Rev 5.1, Rel. 5.1.1 control requirements and standard industry practices form the National Institute of Standards and Technology Special Publications 800-39 and 800-18. This includes developing and implementing an SSP for the PRC GSS. The target implementation date is September 11, 2026.

KPMG Evaluation

Management's comments were responsive to recommendations 1 and 2, and corrective action should resolve the issues identified in the report.

Appendix A – Glossary

Acronym	Definition
AICPA	American Institute of Certified Public Accountants
CDM	Continuous Diagnostics and Mitigation
CG	Cybersecurity Governance
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
CP	Contingency Planning
CSCRM	Cybersecurity Supply Chain Risk Management
CSP	Cloud Service Provider
DPP	Data Protection and Privacy
DOJ	Department of Justice
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IG FISMA Metrics	Office of Management and Budget's Fiscal 2025 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics
GAGAS	Generally Accepted Government Auditing Standards
GSS	General Support System
IAM	Identity and Access Management
IG	Inspector General
IR	Incident Response
ISCM	Information Security Continuous Monitoring
IT	Information Technology
JSOC	Justice Security Operations Center
KPMG	KPMG LLP
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POA&M	Plans of Actions and Milestones
PRC	Postal Regulatory Commission
Rel	Release
Rev	Revision
RM	Risk Management
SP	Special Publication
SSP	System Security Plan
ST	Security Training
USPS	United States Postal Service

Appendix B – Management's Comments

U.S. POSTAL REGULATORY COMMISSION
Washington, DC 20268-0001

Office of the Secretary and Administration

September 12, 2025

Laura Lozon
Director, Audit Services
U.S. Postal Service Office of Inspector General (USPS OIG)

RE: Audit Review of the Postal Regulatory Commission's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2025, Project Number 25-043

Dear Director Lozon,

The Commission has reviewed the findings and recommendations outlined in the audit and concurs with the conclusions provided by the Office of the Inspector General. We appreciate the diligent efforts of both the Inspector General and KPMG in evaluating the Commission's information security program. The Commission remains committed to strengthening its cybersecurity practices and supports the continued implementation of the reinstated FISMA audit program under the oversight of the Inspector General.

The Commission has made meaningful progress in its information security posture; from last year's Ad Hoc rating to operating at the Defined (Level 2) maturity level, indicating that foundational processes are being established and documented. This year's audit resulted in **two new findings** highlighting areas where additional improvements are needed to strengthen the effectiveness and resilience of our cybersecurity program.

While the Commission has made meaningful progress in modernizing its IT and security infrastructure, additional work is needed to fully meet the recommendations issued by the Office of the Inspector General. Since last year's audit, three of the nine recommendations have been successfully closed. While the Commission has made measurable progress in strengthening its information security program, continued effort is required to fully address all outstanding audit findings.

At the time of the audit, the recent retirement of the Chief Information Security Officer (CISO) had temporarily reduced the Commission's cybersecurity capacity, leaving only one cybersecurity professional on staff. A new CISO has now been appointed, and with this leadership in place, the Commission is well-positioned to accelerate progress in strengthening its security posture and expects to close additional POA&Ms in the coming months.

As part of its broader IT and security modernization efforts, the Commission has developed and formally approved three policies aligned with the twenty NIST control families. An additional seven policies are nearing completion and are currently undergoing final review for implementation within the General Support System (GSS). These initiatives reflect the Commission's ongoing commitment to maturing its cybersecurity governance and addressing both existing and newly identified risks.

Fiscal Year 2025 Recommendations:

Recommendation 1: We recommend the Secretary and Chief Administrative Officer, in coordination with the Chief Information Security Officer, design and implement cyber governance policies, procedures, and processes that address National Institute of Standards and Technology Special Publication 800-53, Rev. 5.1, Rel. 5.1.1 control requirements and OMB Circular A-130.

Response: The Commission agrees with this recommendation and will design and implement cyber governance policies, procedures, and processes that meet the National Institute of Standards and Technology Special Publication 800-53, Rev. 5.1, Rel. 5.1.1 control requirements and OMB Circular A-130.

Target Implementation Date: 09/11/2026

Recommendation 2: We recommend the Secretary and Chief Administrative Officer, in coordination with the Chief Information Security Officer, design and implement risk management and general support system policies, procedures, and processes that address National Institute of Standards and Technology Special Publication 800-53, Rev. 5.1, Rel. 5.1.1 control requirements and standard industry practices from the National Institute of Standards and Technology Special Publications 800-39 and 800-18. This includes developing and implementing an SSP for the PRC GSS.

Response: The Commission agrees with this recommendation and will design and implement risk management and general support system policies, procedures, and processes that meet the National Institute of Standards and Technology Special Publication 800-53, Rev. 5.1, Rel. 5.1.1 control requirements and standard industry practices from the National Institute of Standards and Technology Special Publications 800-39 and 800-18. This includes developing and implementing an SSP for the PRC GSS.

Target Implementation Date: 09/11/2026

The Commission appreciates the professionalism and collaborative approach demonstrated by the OIG audit team throughout the course of the review. As reflected in the Commission's response, the Commission concurs with the OIG's recommendations and remains committed to addressing the identified areas for improvement. Ensuring compliance with applicable standards and strengthening our information security posture continues to be a top priority for the Commission.

Sincerely,

ERICA BARKER Digitally signed by ERICA BARKER Date: 2025.09.12 10:13:54 -04'00'

Erica Barker
Secretary and Chief Administrative Officer

Contact us via our Hotline and FOIA forms. Follow us on social networks. Stay informed.

1735 North Lynn Street, Arlington, VA 22209-2020
(703) 248-2100

For media inquiries, please email press@uspsoig.gov or call (703) 248-2100