Review of the Postal Regulatory Commission's Compliance With the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024

AUDIT REPORT

Report Number 24-097-R24 | September 27, 2024

Highlights

Background

This report presents a review of the United States Postal Regulatory Commission's (PRC) information security program and practices for fiscal year (FY) 2024. The Federal Information Security Modernization Act of 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 objective was to determine the effectiveness of the PRC's information security program and practices in five framework function areas: Identify, Protect, Detect, Respond, and Recover.

What We Found

The PRC has opportunities to improve its information security program. Specifically, the PRC began to draft and implement policies, procedures, and processes to manage its information security program. However, KPMG determined that these initiatives were not completed. As a result, the Core Metrics and Supplemental Group 2 Metrics were rated an Ad-Hoc (Level 1) maturity level for the five framework functions. KPMG identified one finding (see Section III) pertaining to the functions and their respective nine metric domains.

Recommendations and Management's Comments

KPMG made nine recommendations to address the issues identified in the report across the nine FISMA metric domains. The PRC agreed with all recommendations. KPMG considers management's comments responsive to all recommendations, as corrective actions should resolve the issues identified in the report. See Appendix B for management's comments in their entirety.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

September 27, 2024

MEMORANDUM FOR: ERICA BARKER,
SECRETARY AND CHIEF ADMINISTRATIVE OFFICER

FROM: Wilvia Espinoza
Deputy Assistant Inspector General
for Inspection Service, Technology, Services

SUBJECT: Audit Report – Review of the Postal Regulatory Commission's Compliance With the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024 (Report Number 24-097-R24)

This report presents the results of our audit of the United States Postal Regulatory Commission's (PRC) Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024.

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

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Vasilios Grasos, Director, Cybersecurity & Technology, 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 2024

September 27, 2024

Contents

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 2024

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 April 1, 2024, through July 31, 2024, and our results are through the period of October 1, 2023, through July 31, 2024.

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 objective of this performance audit was to determine the effectiveness of the PRC's information security program. Specifically, we evaluated the five Cybersecurity Framework security functions outlined in the Office of Budget and Management's (OMB's) Fiscal Year (FY) 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics (FY 2024 IG FISMA Reporting Metrics):

- Identify, which includes questions pertaining to Risk Management and Supply Chain Risk 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.

As a result, we reported one finding and assessed the PRC's information security program as Ad-hoc (Level 1), which was ineffective according to OMB's FY 2024 IG FISMA Reporting Metrics guidance.

When implemented, the nine recommendations we made should strengthen 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

September 27, 2024

II. Background, Objective, Scope, and Methodology

Background[1]

KPMG performed the FY 2024 independent FISMA evaluation under contract with USPS OIG as a performance audit in accordance with GAGAS and AICPA Consulting Services Standards. The USPS OIG monitored our work to ensure we met professional standards and contractual requirements.

Agency Overview

The PRC is an independent agency that exercises regulatory oversight of the USPS.[2] It is comprised of five commissioners and supported by approximately 70 employees, and its mission is to ensure transparency and accountability of the Postal Service and foster a vital and efficient universal mail system.[3] 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.

Program Overview

In August 2020, the PRC began the process of developing an IT security program by onboarding a Chief Information Security Officer (CISO) to oversee the program. In May 2021, the PRC hired its first Chief Information Officer (CIO) and in 2023, added a cybersecurity specialist position to result in a two-person cybersecurity team. PRC officials stated they are working to attain additional resources to support its FISMA responsibilities. As of April 2024, the PRC had recently experienced a vacancy in the CISO[4] role and was operating with a single cybersecurity specialist.

The CIO and the CISO oversee the management and security of information technology (IT) at the PRC. Together, the department consists of five individuals. The CIO manages the IT security program by overseeing the security posture of IT systems and devices throughout their lifecycle, 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 consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the PRC. These positions report to the Secretary and Chief Administrative Officer, who oversees the day-to-day functions of budgeting and accounting, human resource management, records and data management, contracts and audits, facilities, and IT.

FISMA

On December 17, 2002, President George W. Bush signed FISMA[5] 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

[1]The information in this section of the report is as of September 6, 2024, and is based on information obtained from a written response from PRC and documentation provided during the course of the engagement.
[2] About the PRC (prc.gov/about).
[3] Mission, Vision, Guiding Principles, and Strategy (prc.gov/mission).
[4] The CISO departed PRC in April 2024.
[5]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.

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, 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 24-04, Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements. The FY 2024 Inspector General FISMA Reporting Metrics are aligned with the five information security functions outlined in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. The Council of the Inspectors General on Integrity and Efficiency maintained the maturity models for the following nine FISMA Metric Domains: Risk Management (RM), Supply Chain Risk Management (SCRM), 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 2024 IG FISMA Reporting Metrics.

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

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

Source: FY 2024 IG FISMA Reporting Metrics, dated February 10, 2023, page 5.

Consistent with FY 2023, 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 2024 IG FISMA Reporting Metrics, dated February 10, 2023, page 7.

The FY 2024 IG FISMA Reporting Metrics represent a continuation of the work started in FY 2022, when the IG metrics reporting process was transitioned to a multi-year cycle. The FY 2024 IG FISMA Reporting Metrics included Core Metrics and Supplemental Metrics, as depicted in **Table 3.**

Table 3: FY 2024 FISMA Reporting Metrics

Core Metrics	Supplemental Metrics
• System Inventory • Hardware Inventory • Software Inventory • Enterprise Risk Management & Risk Assessments • RM Dashboards and Reporting • SCRM Processes • Configuration Settings • Flaw Remediation • MFA - General Users • MFA - Privileged Users • Privileged User Account Management • Encryption • Data Exfiltration and Network Defenses • Workforce Assessment • ISCM Strategy • ISCM Processes • Incident Response Tools and Detection • Incident Response Tools and Handling • Business Impact Analysis • ISCP Test, Training, and Exercise	• Enterprise Architecture and System Categorization • Information System Security Architecture • SCRM Counterfeit Components • CM Roles and Responsibilities • Enterprise-Wide Configuration Management Policy • Application Configuration Change Control • Personnel Risk Designations • Data Breach Response Plan • Privacy Awareness Training • Cybersecurity Awareness Training • Specialized Security Training • ISCM Performance Measures • Incident Response Policies and Procedures • IR Roles and Responsibilities and Training • Incident Response Reporting and Communication • Information System Contingency Plan • Backups

Source: Analysis performed by KPMG from inspecting pages 12 – 60 of the FY 2023-2024 IG FISMA Reporting Metrics, dated February 10, 2023, and determining the FY 2024 IG FISMA Metric questions in scope.

According to the FY 2024 IG FISMA Reporting 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 2024, a calculated average scoring model was used in which Core Metrics and Supplemental Metrics Group 2 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 Group 2 are used as a data point to support the risk-based determination of overall program and function level effectiveness. Other data points considered include the:

- Results of cybersecurity evaluations, including system security control reviews conducted during the review period.
- Security incidents reported during the review period.

IGs should use the CyberScope[6] 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 evaluate the effectiveness of the PRC's overall IT security program by evaluating the five cybersecurity framework security functions outlined in the OMB's FY 2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics:

- Identify, which includes questions pertaining to Risk Management and Supply Chain Risk 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.

The period for the performance audit was October 1, 2023, through July 31, 2024. Specifically, we assessed the PRC's performance in the five cybersecurity functions outlined in the FY 2024 IG FISMA Reporting Metrics. Our results for this testing are as of July 31, 2024. We conducted our fieldwork from April 1, 2024, through July 31, 2024. As part of our performance audit, we responded to the FY 2024 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 2024 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 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

[6] The Department of Homeland Security uses CyberScope, a web-based application, to collect data that OMB uses to assess federal agencies' IT security. Agencies are required to use CyberScope to submit reporting metrics, including the annual IG FISMA Metrics. IGs are also required to input an independent assessment of the overall effectiveness of their respective agency's information security program. Results for FY 2024 IG FISMA Reporting Metrics were required to be submitted in CyberScope no later than July 31, 2024.

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 2024 IG FISMA Reporting Metrics to help us gain a better understanding of how the organization implemented relevant security controls and processes for the 37 metrics in scope. The PRC's responses allowed us to focus our meetings and confirm gaps that it 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 April 1, 2024, through July 31, 2024. 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 2024 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 2024 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 2024 by performing the following actions:

- Drafted a plan for continuous monitoring that includes an active scanning program to identify threats.
- Monitored security awareness training for all employees.
- Established a policy for addressing a personally identifiable information (PII) breach and a continuity of operations plan.
- Leveraged Department of Justice's Security Operations Center Shared Services for monitoring the PRC general support system (GSS) for cybersecurity incidents and implemented a process for Department of Justice to report incidents to the PRC.

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/domain area (Identify, Protect, Detect, Respond, and Recover). **Table 3** below depicts assessed maturity levels for each cybersecurity function.

PRC management stated that these policies, procedures, and processes were not fully implemented because the CISO departed the agency in April 2024, and PRC had limited resources that were tasked with performing operational activities. The policies and procedures have been drafted, but not approved by PRC leadership.

Table 3: Maturity Levels for Cybersecurity Functions

Cybersecurity Function / Metric Domains	Assessed Maturity Level
Identify (RM and SCRM)	Ad-hoc (Level 1)
Protect (CM, IAM, DPP, and ST)	Ad-hoc (Level 1)
Detect (ISCM)	Ad-hoc (Level 1)
Respond (IR)	Ad-hoc (Level 1)
Recover (CP)	Ad-hoc (Level 1)

Source: CyberScope IG FISMA Report, dated July 31, 2024.

Identify

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 and SCRM control 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. Risk management (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 the various 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 plan of action and milestones of weaknesses they self-identified through system accreditation and assessments and other internal and external reviews.

However, the PRC has not designed or implemented agency-wide RM policies, procedures, or processes that address NIST SP 800-53, Revision (Rev.) 5.1, Release (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 cloud service providers [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 system security plan 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 plan of action and milestones has been created for this 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 in a manner 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 assessment and system security plan 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 exposes 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 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.

Supply Chain Risk Management

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 CSPs) adherence to PRC security requirements. This would include reviewing relevant security information on defined timeframes.
- Has not provided training to individuals on how to detect counterfeit system components or does not have processes to determine if equipment or software purchased contains counterfeit components.

OMB 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 outline the security control requirements and documentation needed (SA-4).
- Establish policy, management plan, processes, 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 are not meeting the PRC's information security requirements. In addition, the PRC could be using counterfeit components that could put PRC data at risk.

Recommendation 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.

Protect

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 organizations' 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 baseline 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 plan of action and milestones, 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. When performing and reviewing vulnerability scans, but not documenting the reviews and actions taken, there is a risk that a patch and/or configuration changes may be inappropriately applied to the system.

Recommendation 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.

Identity and Access Management

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 for privileged and non-privileged that require user multi-factor authentication. We also did not identify any testing exception with the PRC's remote access controls.

However, PRC management has not designed or implemented agency-wide IAM policies, procedures, and processes that address NIST SP 800-53, Rev. 5.1, Rel 5.1.1, control requirements. Specifically, management has not documented account management procedures for access provisioning, review and reauthorization, and removal.

NIST SP 800-53, Rev 5.1, Rel. 5.1.1, requires that organizations develop and implement access control policies (AC-1) and account management (AC-2). These two controls set the foundation for the policies, procedures, and processes for identity and access management that include controls for access provisioning, review and reauthorization, and removal.

Without having approved and implemented policies, procedures, and processes around account management or identification and authentication procedures and implementing processes, the risk could exist that unauthorized access could lead to inappropriate actions within the system.

Recommendation 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, controls requirements.

Data Protection and Privacy

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 PII depends on the safeguards in place for the information systems that process, store, and transmit this information. OMB Circular A-130, Managing Information as a Strategic Resource, 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 their 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. The PRC also 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 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.

Recommendation 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.

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.

Recommendation 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.

Detect

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 a draft ISCM plan that includes active scanning to identify threats. However, management has not formally established the plan and has not designed and implemented additional ISCM procedures and processes to address applicable NIST SP 800-53, Rev. 5, Rel. 5.1.1, control requirements. Specifically, PRC management has not defined, tailored, and implemented ISCM performance measures to determine the effectiveness of the PRC's security controls in place and its overall information security program. Additionally, management has not designed or implemented a process for conducting and maintaining security assessments and authorizations for its information systems, including the GSS, in accordance with NIST SP 800-37.

OMB Circular A-130, Appendix I, section 4, Specific Requirements, states that agencies shall:

- Develop and maintain an ISCM strategy to address information security risks and requirements across the organizational risk management tiers.
- Implement and update, in accordance with organization-defined frequency, the ISCM strategy to reflect the effectiveness of deployed controls and significant changes to information systems.
- Adhere to federal statues, policies, directives, instructions, regulations, standards, and guidelines.
- Establish and maintain an ISCM program that:
    - Provides an understanding of agency risk tolerance and helps officials set priorities and manage information security risk consistently throughout the agency.
    - Includes metrics that provide meaningful indications of security status and trend analysis at all risk management tiers.
    - Maintains awareness of threats and vulnerabilities that have the potential to affect security, including the mitigation of those threats and vulnerabilities.

NIST SP 800-37, Rev. 2 outlines risk management processes for agencies to follow for the development of security and privacy capabilities into information systems throughout the system development life cycle by 1) maintaining situational awareness of the security and privacy posture of those systems on an ongoing basis through continuous monitoring processes; and 2) providing information to senior leaders and executives to facilitate decisions regarding the acceptance of risk to organizational operations and assets.

The lack of an established ISCM program impedes the PRC's ability to appropriately assess the effectiveness of its security controls and overall information security program and to take the necessary actions to adjust the information security program, thereby potentially exposing PRC production data and computing resources to internal and external threats.

Recommendation 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.

Respond

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 entered into an agreement with the Department of Justice to provide security incident monitoring as of April 2024.

However, PRC management has not designed or 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, PRC management has not defined IR team roles and responsibilities; devised incident handling policy, procedures, or processes; and determined how IR information should be shared with internal and external stakeholders.

The Federal Information Security Management Act of 2014 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 Department of Justice, nor did they establish 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.

Recommendation 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.

Recover

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.

These issues occurred because the PRC did not establish CP policies and procedures. 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.

Recommendation 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.

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 five cybersecurity functions and nine FISMA metric domains during FY 2024. We assessed the PRC's information security program as not effective in CyberScope; this determination was made because the FY 2024 IG FISMA Reporting Metrics and the associated calculated averages for the metric domains and cybersecurity functions were assessed as Ad-Hoc (Level 1). We reported one finding that impacted each of the nine domains.

We recommend PRC management establish its RM, SCRM, CM, IAM, DPP, ST, ISCM, IR, and CP 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. In a written response, PRC management agrees with our finding and recommendations for strengthening their information security program (see Section V and Appendix B).

V. Agency Comments – Management Response to the Report

Postal Regulatory Commission Response

The Postal Regulatory Commission had no comment regarding the finding and agreed with recommendations 1 - 9.

For recommendation 1, management stated it will develop and implement a Risk Management policy, procedures, and processes to meet the control criteria outlined in National Institute of Standards and Technology (NIST) Special Publication 800-53, Rev.5.1, Rel. 5.1.1 for the General Support System (GSS).

For recommendation 2, management stated that it will develop and implement a Supply Chain Risk Management policy, procedure and processes to meet the control criteria outlined in NIST Special Publication 800-53, Rev.5.1, Rel. 5.1.1 for the GSS.

For recommendation 3, management stated it will develop and implement a Configuration Management policy, procedure and processes to meet the control criteria outlined NIST Special Publication 800-53, Rev.5.1, Rel. 5.1.1 for the GSS.

For recommendation 4, management stated it will develop and implement an Access Management policy, procedures, and processes to meet the control criteria outlined NIST Special Publication 800-53, Rev.5.1, Rel. 5.1.1 for the GSS.

For recommendation 5, management stated it will develop and implement a Data Protection and Privacy policy, procedure and processes to meet the control criteria outlined NIST Special Publication 800-53, Rev.5.1, Rel. 5.1.1 for the GSS.

For recommendation 6, management stated it will develop and implement a Security Training policy, procedure and processes to meet the control criteria outlined NIST Special Publication 800-53, Rev.5.1, Rel. 5.1.1 for the GSS.

For recommendation 7, management stated it will finalize and implement Information Security Continuous Monitoring plan, any additional procedures and processes to meet the control criteria outlined NIST Special Publication 800-53, Rev.5.1, Rel. 5.1.1 for the GSS.

For recommendation 8, management stated it will develop and implement an Incident Response policy, procedure and processes to meet the control criteria outlined NIST Special Publication 800-53, Rev.5.1, Rel. 5.1.1 for the GSS.

For recommendation 9, management stated it will develop and implement a Contingency Planning policy, procedure and processes to meet the control criteria outlined NIST Special Publication 800-53, Rev.5.1, Rel. 5.1.1 for the GSS.

KPMG Evaluation

Management's comments were responsive to recommendations 1 - 9 and corrective actions should resolve the issues identified in the report.

Appendix A – Glossary

Acronym	Definition
AICPA	American Institute of Certified Public Accountants
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
PRC	Postal Regulatory Commission
CP	Contingency Planning
DPP	Data Protection and Privacy
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
FY 2024 IG FISMA Reporting Metrics	2023-2024 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
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
Rel	Release
Rev	Revision
RM	Risk Management
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SP	Special Publication
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 20, 2024

John Chiota,
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 2024, Project Number 24-097

Dear Director Chiota,

The Commission has reviewed the findings and recommendations contained in the subject audit and agrees with the recommendations provided by the Inspector General. The Commission appreciates the efforts of the Inspector General and KPMG in reviewing the compliance of its information security program. The Commission looks forward to the reestablishment of the FISMA audit program under the Inspector General; this audit report represents the first FISMA audit of the Commission in over 14 years.[1]

As noted in the audit report, the Commission operates with an extremely small IT and cybersecurity team, having only recently established its IT Security Program with the appointment of a Chief Information Security Officer (a position which is presently vacant) in 2020 and Chief Information Officer in 2021. As part of its efforts to remedy significant underinvestment in information technology and security due to budget constraints, the Commission applied for and received two competitive Technology Modernization Fund (TMF) awards. With funding from the TMF, the Commission implemented numerous security upgrades to its systems and in March 2024 implemented the Department of Justice's Security Operations Center to assist in monitoring ongoing threats to the Commission's IT systems.

Despite these IT modernization efforts, the Commission has significant work ahead to close the nine recommendations provided by the Inspector General and is committed to improving its program. Due to the recent retirement of its CISO, the Commission is currently operating with one cybersecurity professional at the time of the audit and is

[1] In 2022, Congress enacted the Postal Reform Act of 2022, which, among other changes, transferred responsibility for OIG oversight of the Commission to the U.S. Postal Service Office of Inspector General (USPS OIG).

1

actively working to fill the CISO role. Prior to this audit, as part of its Security and IT modernization efforts, the Commission began developing policies for all 20 control families for the General Support System (GSS).

Commission Chairman Michael Kubayanda notes "information security, and FISMA compliance in particular, are among the highest priorities for the Commission. The Commission's efforts to launch a mandatory information security program and other IT initiatives were previously slowed by multiple challenges. The challenges included a lack of funds for basic personnel and infrastructure, and a need for education about cybersecurity and FISMA. With funding through the TMF and a basic framework in place, the Commission plans to address the findings of this audit to guide progress as it fills the CISO position and implements a more robust information security program."

Fiscal Year 2024 Recommendations:

Recommendation 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.

Response: The Commission agrees with this recommendation and will develop and implement a Risk Management policy, procedures, and processes to meet the control criteria outlined in National Institute of Standards and Technology Special Publication 800-53, Rev.5.1, Rel. 5.1.1 for the General Support System (GSS). Target Implementation Date: September 10, 2025

Recommendation 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.

Response: The Commission agrees with this recommendation and will develop and implement a Supply Chain Risk Management policy, procedure and processes to meet the control criteria outlined in National Institute of Standards and Technology Special Publication 800-53, Rev.5.1, Rel. 5.1.1 for the General Support System (GSS). Target Implementation Date: September 10, 2025.

Recommendation 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.

Response: The Commission agrees with this recommendation. It will develop and implement a Configuration Management policy, procedure and processes to meet the control criteria outlined in National Institute of Standards and Technology Special Publication 800-53, Rev.5.1, Rel. 5.1.1 for the General Support System (GSS). Target Implementation Date: September 10, 2025.

Recommendation 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, controls requirements.

Response: The Commission will develop and implement an Access Management policy, procedures, and processes to meet the control criteria outlined in National Institute of Standards and Technology Special Publication 800-53, Rev.5.1, Rel. 5.1.1 for the General Support System (GSS). Target Implementation Date:
September 10, 2025.

Recommendation 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.

Response: The Commission agrees with this recommendation and will develop and implement a Data Protection and Privacy policy, procedures, and processes to meet the control criteria outlined in National Institute of Standards and Technology Special Publication 800-53, Rev.5.1, Rel. 5.1.1 for the General Support System (GSS). Target Implementation Date: September 10, 2025.

Recommendation 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.

Response: The Commission agrees with this recommendation. It will develop and implement a Security Training policy, procedure and processes to meet the control criteria outlined in National Institute of Standards and Technology Special Publication 800-53, Rev.5.1, Rel. 5.1.1 for the General Support System (GSS). Target Implementation Date: September 10, 2025.

Recommendation 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.

Response: The Commission agrees with this recommendation, and it will finalize and implement Information Security Continuous Monitoring plan, any additional procedures and processes to meet the control criteria outlined in National Institute of Standards and Technology Special Publication 800-53, Rev.5.1, Rel. 5.1.1 for the General Support System (GSS). Target Implementation Date: September 10, 2025.

Recommendation 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.

Response: The Commission agrees with this recommendation. The Commission will develop and implement an Incident Response policy, procedures, and processes to meet the control criteria outlined in National Institute of Standards and Technology Special Publication 800-53, Rev.5.1, Rel. 5.1.1 for the General Support System (GSS). Target Implementation Date: September 10, 2025.

Recommendation 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.

Response: Management agrees with this recommendation. The Commission will develop and implement a Contingency Planning policy, procedures, and processes to meet the control criteria outlined in National Institute of Standards and Technology Special Publication 800-53, Rev.5.1, Rel. 5.1.1 for the General Support System (GSS). Target Implementation Date:
September 10, 2025.

Sincerely,

ERICA BARKER Digitally signed by ERICA BARKER
Date: 2024.09.20 13:05:24 -04'00'

Erica Barker
Secretary and Chief Administrative Officer

4

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