Office of Inspector General | United States Postal Service

Audit Report

State of Cybersecurity

Report Number 21-205-R22 | August 15, 2022

Table of Contents

Highlights

Background

Cybersecurity, a major enterprise risk consideration, is the practice of protecting systems, networks, and programs from cyberattacks. Cyberattacks targeting the critical infrastructure are increasing in frequency and sophistication, making a well-defined, proactive cybersecurity approach critical. To address these threats, the U.S. Postal Service's Corporate Information Security Office (CISO) focuses on five cybersecurity strategic objectives: protect, monitor, respond, manage, and innovate.

What We Did

Our objective was to assess the effectiveness of the Postal Service's state of cybersecurity, specifically evaluating its (1) risk profile and organizational alignment with the cybersecurity strategy, (2) cybersecurity risk management process and vulnerability management program for consistency and appropriateness, and (3) enterprise security architecture processes for alignment with best practices.

What We Found

The Postal Service has made positive strides in implementing improvements to its risk management program, cybersecurity strategy, and organizational structure. However, its state of cybersecurity lacks maturity, which limits its ability to fully understand its risk exposure and protect the agency from cyberattack.

Specifically, we found the Postal Service did not establish a cybersecurity [redacted] in accordance with agency guidance. We observed that the CISO could not perform [redacted] because they did not have the necessary tools. We also found that formal risk acceptance of [redacted] exceptions was not always conducted in accordance with policy. We further observed applications could operate in [redacted] application owners did not always provide access support for [redacted], and cybersecurity mitigation plans were not consistently managed. This occurred because, although CISO identifies and informs stakeholders of instances of noncompliance, there were no practices to compel compliance.

Recommendations

We made six recommendations, including that management establish a cybersecurity [redacted], implement ongoing [redacted] activities for all technology, establish centralized oversight and documentation of enterprise security architecture processes, implement practices to provide assurance cybersecurity [redacted], enforce requirements that reflect risk acceptance expectations, and update policies and formal guidance accordingly.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

August 15, 2022

MEMORANDUM FOR: PRITHA N. MEHRA
EXECUTIVE VICE PRESIDENT, CHIEF INFORMATION OFFICER

THOMAS J. MARSHALL
EXECUTIVE VICE PRESIDENT, GENERAL COUNSEL

HEATHER L. DYER
VICE PRESIDENT, CHIEF INFORMATION SECURITY OFFICER

FROM: Margaret B. McDavid
Deputy Assistant Inspector General
for Inspection Service and Cybersecurity & Technology

SUBJECT: Audit Report – State of Cybersecurity
(Report Number 21-205-R22)

This report presents the results of our audit of the U.S. Postal Service's State of Cybersecurity.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Laura Roberts, Acting Director, Cybersecurity & Technology, or me at 703-248-2100.

Attachment

cc: Postmaster General
Corporate Audit Response Management

Results

Introduction/Objective

This report presents the results of our self-initiated audit of the U.S. Postal Service's state of cybersecurity (Project Number 21-205). Our objective was to assess the effectiveness of the Postal Service's state of cybersecurity. Specifically, we assessed the Postal Service's cybersecurity risk management, strategy, and organizational structure in terms of alignment with best practices and ability to meet business needs and objectives. See Appendix A for additional information about this audit.

Background

The Postal Service is instrumental in the secure delivery of the nation's mail, including election mail, Social Security Administration benefits and notices, free COVID-19 tests, and official mail sent from other federal agencies. To collect, process, and deliver the nation's mail, the Postal Service uses a vast network of people and technologies. The Postal Service connects more than 1.1 million devices on one of the world's largest networks and has one of the world's largest material-handling systems for mail, comprised of over 8,500 pieces of equipment.[1] See Figure 1 for more information on the Postal Service's technology.

"The Postal Service connects more than 1.1 million devices on one of the world's largest networks and has one of the world's largest material-handling systems for mail, comprised of over 8,500 pieces of equipment."

Figure 1. Postal Service Technology at a Glance

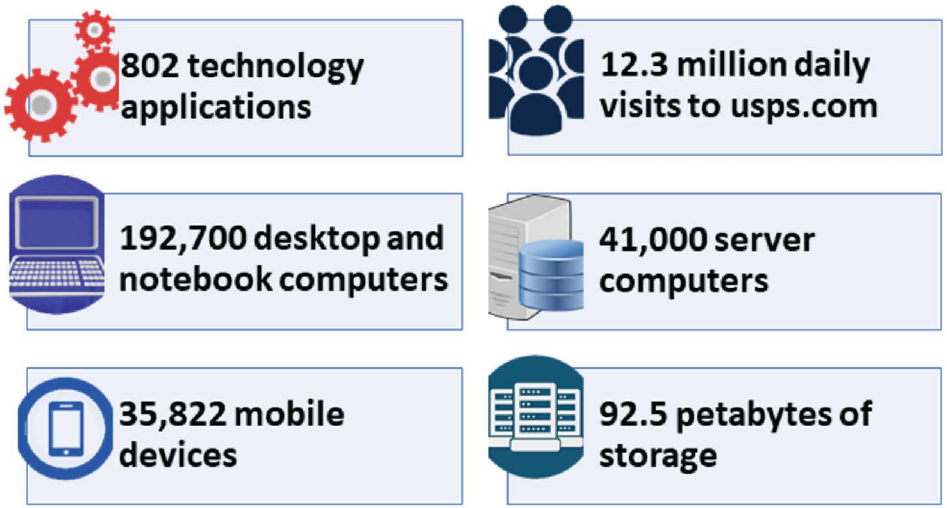


Figure reflects technology applications in Production status as of January 13, 2022.
Sources: Postal Facts as of February 2022 and Postal Service Corporate Information Security Office's (CISO) Assessment and Authorization Tracking Information as of January 13, 2022.

Organizational Structure

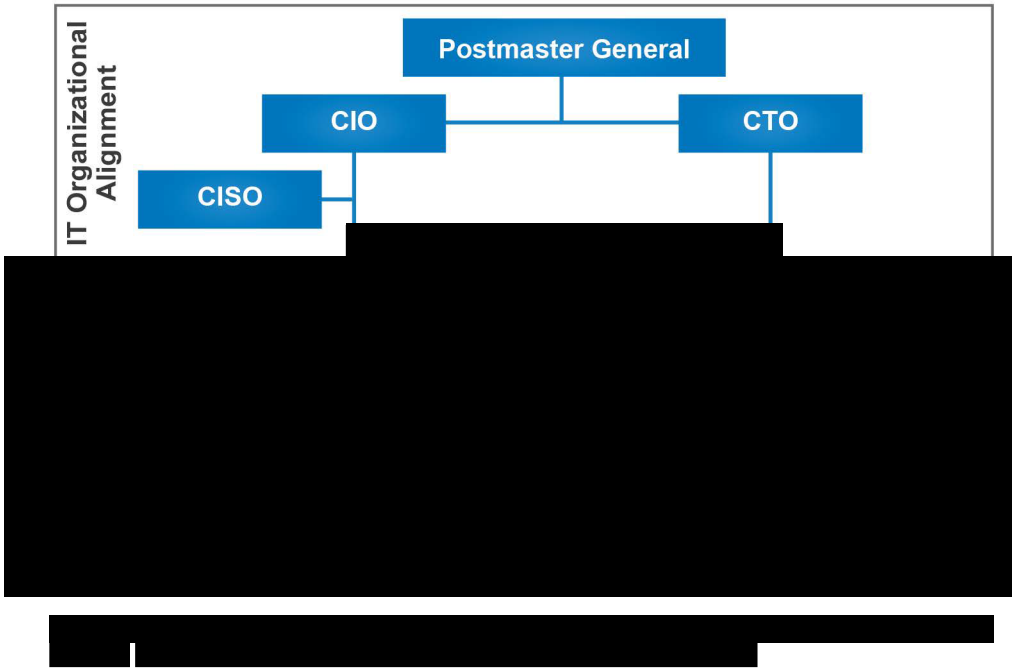
Both the Chief Information Office (CIO) and the Chief Technology Office (CTO) are owners of information technology (IT) resources at the Postal Service. Generally, the CIO is accountable for the IT infrastructure and non-mail processing applications and services on the administrative and commercial IT environment known as *Blue*. The CIO also acts as the senior IT decision maker and change agent for the organization. The CTO is accountable for IT resources related to mail processing and mail handling (MPE/MHE) applications and resources on the Industrial Environment.

The CISO, a sub-organization of the CIO, is responsible for safeguarding the entire Postal Service network, including IT resources owned by both CIO and CTO. The CISO monitors cybersecurity threats, responds to incidents, and develops and disseminates cybersecurity security policies and guidance. The CISO sets the overall strategic and operational direction of the Postal Service's

1 USPS.com. *Postal Facts: Innovation in the Mail.*

information security program and implementation strategies and serves as the central contact for information security issues. The CISO also ensures compliance with cybersecurity policies and standards and escalates security issues to executive management as needed.[2] See Figure 2 for more information on ownership and security oversight of Postal Service IT resources.

Figure 2. Postal Service IT Ownership and Cybersecurity Oversight



The Postal Service is an independent establishment of the executive branch of the U.S. government[3] and, unlike other federal agencies, it is exempt from most federal cybersecurity requirements.[4] With the exception of Payment Card Industry Data Security Standards, the Postal Service exercises discretion in which other industry guidelines, cybersecurity standards, and federal requirements it adheres to.[5]

Cyber Threat Landscape

Cyberattacks on government agencies and threats against U.S. infrastructure continue to increase. In September 2014, the Postal Service was made aware that it was the victim of a cyber intrusion when a successful social engineering attack ultimately led to a data breach. Although the incident did not significantly impact Postal Service operations or mail delivery functions, both customer call center data and Postal Service employees' personally identifiable information were compromised. The investigation revealed that the attack had been specifically developed to exploit the Postal Service's computing environment and identified at least 91 compromised systems. Follow-up analysis found numerous cybersecurity issues, including lack of adherence to cybersecurity policies and lack of resources for important cybersecurity functions.[6] Attacks in recent years, such as the 2021 Colonial Pipeline shutdown and 2020 SolarWinds[7] hack, are evidence that attacks on infrastructure are a looming threat.[8] Given the Postal Service's large cyber presence and its status as an important part of U.S. infrastructure, it will continue to face threats to achieving its core function of providing secure, reliable delivery of mail.[9]

"Given the Postal Service's large cyber presence and its status as an important part of U.S. infrastructure, it will continue to face threats to achieving its core function of providing secure, reliable delivery of mail."

2 Handbook AS-805, *Information Security*, Section 2-2.5, Chief Information Security Officer, dated June 2021.
3 USPS.com. *A Half-Century of Operating Independently While Continuing to Bind the Nation Together,* dated July 1, 2021.
4 *U.S. Code Title 39*, Section 410(a).
5 Handbook AS-805, *Information Security*, Section 1-1, Purpose, dated June 2021.
6 Resources in terms of funding, number and skill level of personnel, equipment, tools, etc.
7 The SolarWinds hack affected multiple federal U.S. departments, including Defense, Homeland Security, State, and Treasury.
8 Jibilian, I and Canales, K. *The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal*, dated April 15, 2021.
9 USPS.com. *USPS Delivers the Facts*, dated July 2020.

Importance of Cybersecurity

To address present and future cybersecurity threats, the CISO focuses on five comprehensive cybersecurity strategic objectives: protect, monitor, respond, manage, and innovate.[10] Cybersecurity is a major strategic and enterprise risk consideration for an organization.[11] As with any other critical risks, cybersecurity should not be considered in isolation. Instead, organizational leadership must address cybersecurity as an enterprise-wide issue, not just an information technology issue. A proactive approach helps align cybersecurity with an organization's vision and investments in cyber threat prevention, detection, and response activities. Evaluation of an organization's state of cybersecurity includes reviewing risk management activities, cybersecurity strategy, and organizational structure to determine the organization's readiness to defend against attack.[12]

Specifically:

- A cybersecurity strategy is comprised of high-level plans for how an organization will secure its assets and minimize cyber risk.[13] A structured approach to developing a consistent and effective security architecture is integral to executing this strategy.
- Cybersecurity risk management allows an organization to identify and prioritize defensive measures to address flaws, threats, and attacks.[14] Key components of a risk management process include 1) developing a risk appetite, which describes the amount of risk an organization is willing to accept and is integral to managing risk and guiding operations;[15] 2) conducting ongoing risk assessment to identify risks; and 3) determining appropriate risk responses, which may include a decision to avoid, mitigate, transfer, or accept the risk.
- A cybersecurity organizational structure considers business objectives and should adequately cover monitoring, response, and governance activities for the enterprise.[16]

An effective cybersecurity approach is required to ensure organizational resiliency.[17] As the Postal Service continues investing in new technologies, these additional information resources provide more potential targets for cyberattacks.

Findings Summary

The Postal Service has made positive strides in implementing improvements to its risk management program, cybersecurity strategy, and organizational structure. However, its state of cybersecurity [redacted] Specifically, the agency lacks some basic components of [redacted] Together, these issues expose the agency to potential exploitation by threat actors, which could result in negative impacts such as data breaches, major disruption of operations, and reputation damage.

> *"The Postal Service has made positive strides in implementing improvements to its risk management program, cybersecurity strategy, and organizational structure."*

10 [redacted]
11 NIST Special Publication 800-39, *Managing Information Security Risk*, dated March 2011.
12 NIST *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1, dated April 16, 2018.
13 *Protection of Transportation Infrastructure from Cyber Attacks: A Primer,* Chapter 3, Cybersecurity Plans, Strategies, Establishing Priorities, Organizing Roles and Responsibilities, The National Academies Press, dated 2016.
14 NIST Special Publication 800-39, *Managing Information Security Risk*, dated March 2011.
15 Martens, Frank & Rittenberg, Larry. *Risk Appetite – Critical to Success*, COSO, dated May 2020.
16 Allen, Julia et al. *Structuring the Chief Information Security Officer Organization*, Carnegie Mellon Software Engineering Institute, dated October 2015.
17 Wong, Arthur. *Cybersecurity Readiness: A Must-Have for Digital Transformation Success*, dated August 29, 2019.

Finding #1: Improvements to Cybersecurity Program and Practices

Since the 2014 data breach, the Postal Service has taken positive steps to improve its overall state of cybersecurity in the areas of governance, risk management strategy, continuous security monitoring, identity management and access control, and awareness and training. These areas align with several core cybersecurity functions according to best practices.[18]

For example, the Postal Service approved investments totaling [redacted] to provide immediate funding for breach remediation, address major recommendations provided by industry experts, and build new capabilities to address ongoing risks. The agency elevated the Chief Information Security Officer position to the Vice President level to clarify overarching cybersecurity responsibilities. The agency also established the Cybersecurity Operations Center to monitor events, detect incidents, respond to incidents, hunt for cyber threats, and report findings to stakeholders. Additionally, it formalized a *Cybersecurity Strategic Plan*, implemented a security awareness program, established an Executive Cyber Risk Committee,[19] and transitioned to a continuous monitoring Assessment and Authorization (A&A)[20] process.

> *"While the Postal Service engages in activities such as risk assessment and response prioritization that contribute to consistency of its risk management practices, it has not defined its [redacted]"*

The Postal Service further enhanced its cybersecurity program by addressing opportunities for improvement identified by the Office of Inspector General (OIG). Over the last five years, postal management implemented 102 cybersecurity-related recommendations in areas such as password security, user accounts, software updates, and incident response. See Appendix B for additional information on prior OIG cybersecurity audit findings.

Finding #2: Cybersecurity [redacted]

While the Postal Service engages in activities such as risk assessment and response prioritization that contribute to consistency of its risk management practices, it has not defined its cybersecurity [redacted] Per policy,[21] the Executive Cyber Risk Committee, co-chaired by the CIO and General Counsel, is responsible for establishing and reviewing [redacted] According to best practices, [redacted] is an important part of corporate governance, strategic planning, and decision making.[22]

This issue occurred because committee chairs were not familiar with the concept of a [redacted]. Subsequently, Postal Service management stated that processes executed during [redacted] Specifically, the CISO considers [redacted].[23] However, heat scores are a tactical approach for prioritizing and responding to individual risks, are reactionary by nature, and do not address risk on an enterprise level. According to best practices, [redacted] is a proactive measure that informs business objectives and strategy, guides management decisions, and is communicated throughout the organization. Without a cybersecurity [redacted] potentially exposing the organization to cybersecurity threats that it is unequipped to manage.

18 NIST *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, dated April 16, 2018.
19 This committee has overall responsibility for cybersecurity risks and ensures risks align with organizational goals.
20 The Assessment and Authorization process is used to evaluate the cybersecurity posture of information resources throughout their lifecycles in management of relevant cyber risks and threats.
21 Handbook AS-805, *Information Security*, Section 2-2.6, Executive Cyber Risk Committee, dated June 2021.
22 Martens, Frank & Rittenberg, Larry. *Risk Appetite – Critical to Success*, COSO, dated May 2020.
23 The heat score is determined based on the deficiencies' impact level and possibility of occurrence specified in the Cyber Risk Heat Score matrix. Scores range from 1 to 9, with 9 representing the highest risk.

Recommendation #1
We recommend the **Executive Vice President, Chief Information Officer**, in coordination with **Executive Vice President, General Counsel and Vice President, Corporate Information Security Office**, define its cybersecurity [redacted] and establish a process for periodically reviewing and communicating this information to personnel.

Finding #3: Ongoing Vulnerability Assessment of [redacted]

[redacted]

We found there was no process for the CISO [redacted]

> *"The CISO does not have the [redacted]*

This technology allows [redacted] on the postal network.

The Postal Service's [redacted] plays a vital role in the agency's ability to process nearly 130 billion mailpieces annually[25] across approximately 300 facilities nationwide.

This issue occurred because the [redacted]. Additionally, the CISO does not have the [redacted]

Policy[26] states that all technology applications should be subject to ongoing vulnerability assessments. Justifications for exceptions to conducting regular assessment activities, such as vulnerability scanning, should be documented.[27] Without full visibility into the Postal Service network, the [redacted]

Recommendation #2
We recommend the **Vice President, Corporate Information Security Office**, implement an [redacted]

Finding #4: Enterprise Security Architecture Approach

The Postal Service lacked centralized oversight of its enterprise security architecture (ESA). An ESA describes the structure and behavior for an enterprise's security processes, information security systems, personnel, and organizational sub-units. An ESA also maps business objectives to security requirements and deployed cybersecurity tools and processes. A well-developed ESA approach allows an organization to understand whether security needs are adequately addressed.[28]

During the audit, the Postal Service began developing summary information on its ESA approach; however, it lacked a formalized process to document and validate ESA coverage and completeness. This occurred because the Postal Service's ESA approach is an unstructured process with no single owner responsible for integrating and evaluating ESA information from various sources across the organization. Gartner recommends that "Security and risk management technical professionals tasked with implementing a security architecture framework or methodology: Ensure architecture traceability from business context to component controls; and build processes to review security architecture, beginning periodically and moving to continuous review, to ensure that emergent

24 [redacted]
25 *USPS Fiscal Year 2021 Annual Report to Congress.*
26 Handbook AS-805, *Information Security*, Section 10-4.6, Scanning Hardware and Software for Vulnerabilities, dated June 2021.
27 Management Instruction AS 810-2020-3, *Cyber Risk Enterprise Network Scanning: Customer Impact Resolution*, Responsibility Section, dated December 2020.
28 Arconati, Nick. *One Approach to Enterprise Security Architecture*, SANS Institute, dated 2021.

risks because of changes to business, technology or the threat landscape are addressed."[29]

Without a mature ESA approach that includes formal processes and consolidated information review, the Postal Service cannot ensure completeness of its security architecture, potentially resulting in unidentified cybersecurity gaps and inconsistent security practices across the enterprise.

Recommendation #3
We recommend the **Vice President, Corporate Information Security Office**, enhance the agency's current enterprise security architecture approach by implementing a centralized oversight function to identify gaps within the architecture, consolidating and formally documenting security architecture information, and documenting details on deployed security components.

Finding #5: Enforcement of Cybersecurity Policy

The CISO did not exercise its authority to ensure application owners [redacted] and complying with established cybersecurity policies. For example, we found several instances where cybersecurity policy was not enforced, highlighting a systemic issue. Specifically, we found that:

- Risk mitigation plans were not completed by the planned date. As a result, we issued *Management Alert – Mitigation of Findings Identified During the Assessment and Authorization Process* (Report Number 22-063-R22), in which we found applications with security control deficiencies that management was aware of as early as October 2020 continued to operate with no consequences for unaddressed deficiencies.[30]
- Applications could [redacted] as specified in the A&A process. We reviewed applications [redacted] per CISO A&A tracking as of November 21, 2021 and January 13, 2022. Of 802 applications reviewed, we identified four that were denied authorization because they did not meet minimum security requirements, and one application that did not complete the A&A process. Although five of 802 (0.6 percent) is a very small percentage, even one vulnerable application can present a significant risk to the network. The CISO [redacted].[32]
- Application owners did not consistently accommodate the CISO [redacted] Specifically, the [redacted] For example, we observed a [redacted]

"The CISO did not develop practices to ensure application owners took action to address cybersecurity risks."

These conditions occurred because, although policy authorizes the CISO to enforce cybersecurity expectations, the CISO did not develop practices to ensure application owners took action to address cybersecurity risks. Per policy, the CISO is responsible for ensuring compliance with information security policies and escalating security issues to executive management.[33] Policy further dictates that exceptions to exclude devices from vulnerability scanning activities must be formally approved via a risk acceptance letter.[34] Best practices suggest that a

29 Gartner, *Improve Your Security With Security Architecture*, Refreshed January 7, 2021, Published June 3, 2019. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.
30 *Mitigation of Findings Identified During Assessment and Authorization Process* (Report Number 22-063-R22, dated May 5, 2022).
31 [redacted]
32 [redacted]
33 Handbook AS-805, *Information Security*, Section 2-2.5, Chief Information Security Officer, dated June 2021.
34 Management Instruction AS 810-2020-3, *Cyber Risk Enterprise Network Scanning: Customer Impact Resolution*, Responsibility Section, dated December 2020.

single stakeholder should be identified as the ultimate authority for cybersecurity decisions.[35] Policies do not define consequences for noncompliance with security standards and requirements. Without a formal process to enforce adherence to cybersecurity standards, the agency cannot ensure applications meet minimum security controls to address risks.

In the management alert, we recommended the Postal Service implement a process that ensures security control deficiencies are remediated timely and in accordance with established remediation plans. According to the CISO, A&A processes will better align with best practices by September 2022 to ensure identified security control deficiencies are appropriately addressed. However, further opportunities remain to establish overall strategies to improve cybersecurity policy enforcement.

Recommendation #4

We recommend the **Vice President, Corporate Information Security Office**, implement procedures to provide assurance that application owners take necessary actions to address cybersecurity risks.

Recommendation #5

We recommend the **Vice President, Corporate Information Security Office**, update policies and other guidance to reflect procedures implemented to enforce cybersecurity compliance, including consequences for noncompliance.

Recommendation #6

We recommend the **Vice President, Corporate Information Security Office**, complete [redacted]

Management's Comments

Management agreed with all findings and recommendations.

Regarding recommendation 1, management agreed to define its cybersecurity [redacted] and tolerance statement and stated that they initiated research and drafting of both. The target implementation date is December 30, 2022.

Regarding recommendation 2, management agreed to implement an [redacted] The target implementation date is June 30, 2023.

Regarding recommendation 3, management agreed to implement centralized oversight for enterprise security architecture and formally document key security architecture information. The target implementation date is March 31, 2023.

Regarding recommendation 4, management agreed to implement a process to authorize information systems to operate in Production and stated that they have initiated this process. Management also agreed to implement a process, which the Executive Cyber Risk Committee will vote on, whether to remove those information systems that are in compliance failure status from Production. The target implementation date is December 30, 2022.

Regarding recommendation 5, management agreed to update policy to reinforce the importance of compliance and consequences for noncompliance. The target implementation date is December 30, 2022.

Regarding recommendation 6, management agreed to implement a process for formally accepting [redacted]. The target implementation date is March 31, 2023.

See Appendix C for management's comments in their entirety.

35 Kantor, Bob. *The RACI matrix: Your blueprint for project success,* dated January 30, 2018.

Evaluation of Management's Comments

The OIG considers management's comments responsive to recommendations 1, 2, 3, 4, and 6 in the report. Action plans to address these recommendations should resolve the issues identified in this report. We consider management's comments partially responsive to recommendation 5.

Regarding recommendation 5, the action plan to update policy to reinforce the importance of compliance and the consequences of noncompliance should partially resolve the issues identified in this report. However, management should also update policies and other guidance to reflect procedures implemented to enforce cybersecurity compliance per the management response/action plan for recommendations 4 and 6.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. Recommendations 1-6 should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

Appendices

Click on the appendix title below to navigate to the section content.

Appendix A: Additional Information

Scope and Methodology

Our scope included review of the Postal Service's cybersecurity strategy, risk management, and organizational structure.

To accomplish our objective, we reviewed the CISO's current Cybersecurity Strategic Plan, Cybersecurity Decision Analysis Reports, incident after-action reports, and other Postal Service documents to gain an understanding of current security processes. We also interviewed key personnel to gain an understanding of cybersecurity risk management and assessment activities and organization of Postal Service cybersecurity functions, including oversight and authority of IT and MPE/MHE technology.

In addition, the audit team:

- Reviewed performance evaluation criteria and cash awards program documentation for incentivization of cybersecurity risk reduction.
- Reviewed internal cybersecurity incident reporting communications for appropriate levels of communication with leadership per policy and best practice.
- Evaluated cybersecurity policies for alignment with accepted frameworks and best practices.
- Selected [redacted], including the full population of [redacted] and a statistical sample of 156 non-business-critical applications, for evaluation of enterprise security architecture, risk assessment, and vulnerability scanning processes.
- Assessed the Postal Service's approach to developing enterprise security architecture for adherence to best practices.
- Evaluated risk management and assessment activities' compliance with Postal Service policy, adherence to accepted and best practices, and consistency of execution.
- Assessed the vulnerability scanning process for appropriate configuration and consistent execution.
- Analyzed prior audit findings and recommendations for trends related to root causes.

We conducted this performance audit from August 2021 through August 2022 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management on July 7, 2022 and included their comments where appropriate.

We assessed the reliability of computer-generated data by analyzing and reviewing the raw data, performing automated and manual reviews to supporting documents or systems, and interviewing personnel knowledgeable about the data. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

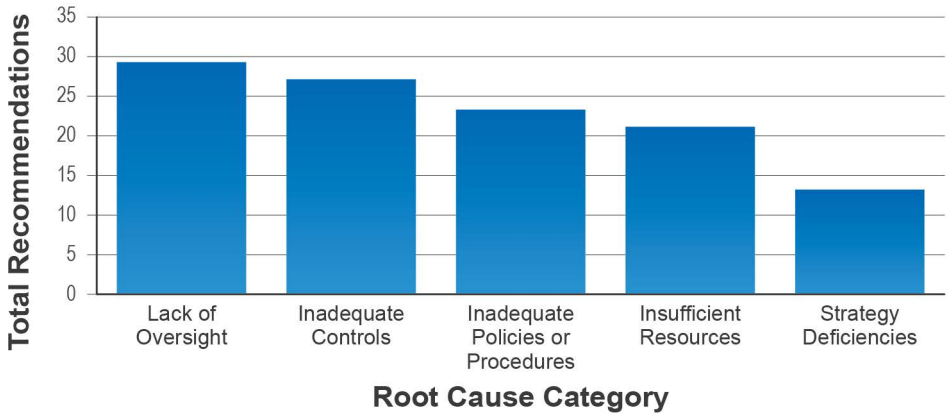
Report Title	Objective	Report Number	Final Report Date
Controls Over Retired Business Applications	Assess the effectiveness of the Postal Service's business application retirement process.	20-289-R21	7/7/2021
Cybersecurity Incident Detection and Response Capability	Determine if the Postal Service has a cybersecurity incident response capability to effectively detect, analyze, and respond to cyber threats.	19-012-R20	7/29/2020
Risks Associated with Information Technology Applications	Provide Postal Service officials immediate notification of the issues identified during our ongoing audit that require immediate attention and remediation.	20-251-R20	7/27/2020

Appendix B: Prior Audit Findings

During the last five fiscal years, the U.S. Postal Service Office of Inspector General (OIG) issued 38 audit reports with 137 recommendations of which 102 were closed as of April 2022. Recommendations are closed when Postal Service management implements recommended remediations or, in limited circumstances, agrees with the OIG to close without implementation. Analysis of associated audit findings revealed that top root cause categories were related to lack of cybersecurity oversight, inadequate controls, non-adherence to cybersecurity policy, lack of adequate monetary and/or staff resources, and deficiencies within management's cybersecurity strategy.

See Figure 3 for summary of top trends in root causes for audit findings reported during the last five fiscal years.

Figure 3. Top Five Root Cause Categories for Audit Findings FYs 2017-2021



Source: U.S. Postal Service Office of Inspector General Reports issued from October 2016 through September 2021.

Appendix C: Management's Comments

UNITED STATES POSTAL SERVICE

July 29, 2022

JOHN CIHOTA
DIRECTOR, AUDIT SERVICES

SUBJECT: State of Cybersecurity (Project Number 21-205-DRAFT)

Management agrees with the overall findings provided in the audit report.

Recommendation #1:
We recommend the **Executive Vice President, Chief Information Officer,** in coordination with **Executive Vice President, General Counsel and Vice President, Corporate Information Security Officer**, define its cybersecurity [redacted] and establish a process for periodically reviewing and communicating this information to personnel.

Management Response/Action Plan:
Management agrees with this recommendation. CISO has initiated research and drafting of a [redacted] for review and concurrence from the Executive Cyber Risk Committee (ECRC).

Target Implementation Date:
12/30/2022

Responsible Official:
VP, Chief Information Security Officer

Recommendation #2:
We recommend the **Vice President, Corporate Information Security Officer** implement an ongoing [redacted] process for [redacted] is not supported.

Management Response/Action Plan:
Management agrees with this recommendation. CISO Risk will work with the VP, Engineering Systems to develop and implement the [redacted] based on enhancing the [redacted] where supported. For [redacted] the process will be modified to include regularly scheduled assessments for vulnerability.

Target Implementation Date:
6/30/2023

Responsible Official:
VP, Chief Information Security Officer

Recommendation #3:
We recommend the **Vice President, Corporate Information Security Officer**, enhance the agency's current enterprise security architecture approach by implementing a centralized oversight function to identify gaps within the architecture, consolidating and formally documenting security architecture information, and documenting details on deployed security components.

Management Response/Action Plan:
Management agrees with the recommendation and commits to enhancing our existing enterprise security architecture standards and practices by implementing a centralized oversight function to identify gaps within the architecture, consolidating and formally documenting security architecture information, and documenting details on deployed security components.

Target Implementation Date:
3/31/2023

Responsible Official:
VP, Chief Information Security Officer

Recommendation #4:
We recommend the **Vice President, Corporate Information Security Officer**, implement procedures to provide assurance that application owners take necessary actions to address cybersecurity risks.

Management Response/Action Plan:
Management agrees with this recommendation. CISO has initiated an Authority to Operate (ATO) as part of the Assessment & Authorization process. Under an ATO, the Authorizing Official, has the ability to revoke an information system's ability to operate. All information systems shall receive an ATO prior to moving into production status. The A&A process will continue to fully authorize, conditionally authorize, and issue compliance failures for applications. If a compliance failure exists for more than 30 days, the ECRC shall vote on whether the Authorizing Official shall accept the risk associated with the information system. If the ECRC does not agree to accept the risk, the information system shall be removed from production.

Target Implementation Date:
12/30/2022

Responsible Official:
VP, Chief Information Security Officer

Recommendation #5:

We recommend the **Vice President, Corporate Information Security Officer**, update policies and other guidance to reflect procedures implemented to enforce cybersecurity compliance, including consequences for noncompliance.

Management Response/Action Plan:
Management agrees with the recommendation. CISO will update policy to reinforce the importance of compliance and the consequences for not complying.

Target Implementation Date:
12/30/2022

Responsible Official:
VP, Chief Information Security Officer

Recommendation #6:
We recommend the **Vice President, Corporate Information Security Officer**, complete Risk Acceptance Letter approval for [redacted] identified for which there is not a valid risk acceptance letter.

Management Response/Action Plan:
Management agrees with the recommendation. CISO will work to implement a standardized acceptance process for [redacted]

Target Implementation Date:
3/31/2023

Responsible Official:
VP, Chief Information Security Officer

PRITHA MEHRA
CHIEF INFORMATION OFFICER

THOMAS MARSHALL
EXECUTIVE VICE PRESIDENT, GENERAL COUNSEL

HEATHER L. DYER
VICE PRESIDENT, CHIEF INFORMATION SECURITY OFFICER

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

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