



Office of Inspector General | United States Postal Service

Audit Report

Procurement and Management of Cybersecurity Tools

Report Number 21-129-R22 | August 25, 2022

A background graphic featuring a person's hands interacting with a tablet displaying various data charts and graphs. The scene is overlaid with a large, glowing blue circular graphic containing the text "CYBER SECURITY". Surrounding this central graphic are several circular icons: a shield with a keyhole, a globe with clouds, a server rack with arrows, a padlock, and a group of people. The overall color scheme is blue and white with a glowing effect.

CYBER SECURITY

Table of Contents

Cover		
Highlights.....	1	
Background.....	1	
What Did We Do.....	1	
What We Found.....	1	
Recommendations.....	1	
Transmittal Letter	2	
Results.....	3	
Introduction/Objective	3	
Background.....	3	
Findings Summary	3	
Finding #1: [REDACTED] Procurement and Implementation.....	4	
The [REDACTED] Acquisition	4	
Recommendation #1	4	
The [REDACTED] Intended Functionality.....	5	
Recommendation #2.....	5	
Finding #2: Ordering Procedures on the [REDACTED] Contract.....	5	
Recommendation #3.....	6	
Finding #3: Clauses and Provisions on the [REDACTED] Contract	6	
Recommendation #4.....	7	
Recommendation #5.....	7	
Finding #4: Contract Document Maintenance	7	
Recommendation #6.....	7	
Management's Comments.....	8	
Evaluation of Management's Comments	9	
Appendices	10	
Appendix A: Additional Information.....	11	
Scope and Methodology.....	11	
Prior Audit Coverage.....	11	
Appendix B: Management's Comments.....	12	
Contact Information	18	

Highlights

Background

The U.S. Postal Service has one of the largest computer networks in the world, known as the ██████████ network, supporting its workforce and customers. The agency also has an extensive mail processing network critical to processing facilities nationwide. The Chief Information Officer oversees the Postal Service's Information Technology organization. Two groups in this office are Network and Compute Technology (Telecom) and the Corporate Information Security Office (CISO). Telecom manages the network infrastructure and CISO protects and defends the network. To procure cybersecurity tools, CISO works closely with Supply Management, which is responsible for procuring goods and services for the Postal Service.

What Did We Do

Our objective was to evaluate Postal Service controls over the procurement and management of cybersecurity tools. We judgmentally selected two tools, ██████████ and ██████████, that the Postal Service acquired to protect its digital assets from attacks. We also reviewed three contracts for the purchase and maintenance of these tools to determine the effectiveness of the Postal Service's procurement and management guidelines.

What We Found

The Postal Service successfully implemented ██████████ on the ██████████ network and ██████████ on the ██████████

██████████. However, for ██████████ on the ██████████ network, the agency did not ensure procurement guidelines were followed, did not meet the intended purpose of the acquisition, and did not apply key contract procedures. Specifically, we found that key stakeholders were not in agreement regarding the ██████████ acquisition and CISO did not use the tool as intended. This occurred because there were no internal controls for the CIO to approve cybersecurity purchases when there are conflicting stakeholder interests. Further, the Supply Management group did not effectively manage the three contracts we reviewed or adhere to internal controls for contractual compliance due to a lack of management oversight. We estimated the Postal Service incurred unsupported questioned costs and funds put to better use of approximately \$46.5 million related to these issues.

Recommendations

We made six recommendations, including that management determine whether additional oversight is needed to facilitate key stakeholder concurrence, complete the current evaluation of ██████████ on the ██████████ network and, if necessary, renegotiate the terms of the contract, follow ordering procedures, modify contract language or document a deviation approval to comply with policy, and verify all contract documentation is stored in the document management system.

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

August 25, 2022

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

HEATHER L. DYER
VICE PRESIDENT, CHIEF INFORMATION SECURITY
OFFICER

MARK A. GUILFOIL
VICE PRESIDENT, SUPPLY MANAGEMENT

Margaret B. McDavid

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

SUBJECT: Audit Report – Procurement and Management of
Cybersecurity Tools (Report Number 21-129-R22)

This report presents the results of our audit of the Procurement and Management of Cybersecurity Tools.

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 Procurement and Management of Cybersecurity Tools (Project Number 21-129). Our objective was to evaluate U.S. Postal Service controls over the procurement process and management of their cybersecurity tools. See [Appendix A](#) for additional information about this audit.

Background

The Postal Service's administrative network, known as the [REDACTED] network, is one of the largest in the world with over 176,000 workstations and approximately 5,000 servers supporting its workforce and customers. The agency also has an extensive [REDACTED] comprised of systems that are critical to about 300 [REDACTED] nationwide.

The Chief Information Officer (CIO) acts as the senior information technology (IT) decision maker and oversees the people, processes, and technologies in the Postal Service's IT organization. Two groups in this office include Network and Compute Technology (Telecom) and the Corporate Information Security Office (CISO). Telecom manages the network infrastructure and CISO protects and defends the network. In 2017, to improve its cybersecurity posture, the Postal Service approved a \$232 million investment in cybersecurity tools¹ and procured several tools including:

- [REDACTED]
- [REDACTED]

CISO contracted with the companies [REDACTED] and [REDACTED] to administer the [REDACTED] and the company [REDACTED]. CISO worked closely with Supply Management, which is responsible for procuring goods and services for the Postal Service.

Findings Summary

The Postal Service successfully procured and implemented [REDACTED] on the [REDACTED] network and [REDACTED] on the [REDACTED]. For example, CISO demonstrated successful use of [REDACTED] to conduct [REDACTED] and successful use of [REDACTED] on the [REDACTED] for [REDACTED]. However, the agency did not follow procurement guidelines for [REDACTED] on the [REDACTED] network. Further, the Postal Service did not ensure the tool's acquisition met its intended purpose, or that a key contract procedure was applied. Specifically, CISO and Telecom were not in agreement regarding the [REDACTED] network [REDACTED] acquisition, and CISO did not use the tool as intended. Further, Supply Management did not effectively manage the [REDACTED] and [REDACTED] contracts or adhere to the agency's internal controls for contractual compliance and oversight.



¹ [REDACTED]

Finding #1: [REDACTED] Procurement and Implementation

While CISO successfully implemented [REDACTED] on the [REDACTED], we identified two issues with CISO's acquisition and implementation of [REDACTED] on the [REDACTED] network. First, CISO acquired the tool without obtaining agreement from key internal stakeholders. Second, while CISO procured [REDACTED] to enforce [REDACTED]² and [REDACTED]³ on the [REDACTED] network, they were ultimately unable to fully use the tool for those capabilities.

“The Postal Service spent approximately \$30 million to acquire [REDACTED] without assurance that it could be implemented on the network.”

The [REDACTED] Acquisition

CISO acquired [REDACTED] through a non-competitive purchase without obtaining agreement from key internal stakeholders. Specifically, when CISO acquired [REDACTED] in December 2017, Telecom opposed it noting that:

- Telecom was already two years into implementing a similar product for the same purpose. At the time of the [REDACTED] acquisition, Telecom had the tool [REDACTED] which had the capability to enforce [REDACTED] and [REDACTED], the same intended functionalities of [REDACTED].
- [REDACTED] was not a good fit for the Postal Service environment due to the large infrastructure and scope of the [REDACTED] network. Telecom stated that [REDACTED] had complex, distributed installation requirements whereas [REDACTED] could be installed on existing network devices.

CISO went forward with the purchase, as they believed that [REDACTED] design, ability to provide integration with multiple vendors, and ease of installation and operation in large networks confirmed [REDACTED] as the best choice. They also compared [REDACTED] functionalities to other tools and decided [REDACTED] was the better option.

Postal Service policy states that it is important to assess the interests of internal stakeholders who may represent different client groups and resolve conflicting needs before making a purchase.⁴ The CIO, in conjunction with other Postal Service executives, approved funding to purchase cybersecurity tools.⁵ That approval included proposed solutions, such as [REDACTED], but did not identify specific tools to purchase. CISO acquired [REDACTED] despite Telecom's opposition because there was no additional control for the CIO to approve the purchase of specific cybersecurity tools when there are conflicting stakeholder interests within the CIO organization. The CIO, as the senior IT decision maker,⁶ while not required, may want to be further involved in future cybersecurity acquisitions, especially on high-value or high-visibility procurements.

Due to the lack of coordination, the Postal Service spent approximately \$30 million to acquire [REDACTED] without assurance that it could be implemented on the network, which may not have been in the best financial interest of the agency. For three years subsequent to the purchase, the agency spent an additional \$26 million attempting to implement the product. However, management ultimately decided to stop the [REDACTED] implementation and use the tool Telecom implemented, [REDACTED].

Recommendation #1

We recommend the **Chief Information Officer and Executive Vice President**, determine whether additional oversight is needed to facilitate key stakeholder concurrence on future high-value or high-visibility cybersecurity tool procurements, and if necessary, develop policy to implement additional oversight or controls.

² Noncompetitive Purchase Request, [REDACTED] Cybersecurity-Network Security, dated May 10, 2016.

³ [REDACTED] Expansion, Statement of Work, dated December 15, 2017.

⁴ Supplying Principles & Practices (SP&P), Section 1-3, Identify Key Stakeholders, dated August 7, 2015, and updated on June 20, 2020.

⁵ [REDACTED]

⁶ Postal Service Handbook AS-805-A, Information Resource Certification and Accreditation (C&A) Process, states the Chief Information Officer is the senior IT decision maker and corporate change agent to securely integrate the key components of business transformation: technology, processes, and people.

The [REDACTED] Intended Functionality

After spending \$56 million and over four years attempting to implement [REDACTED] on the [REDACTED] network, CISO could not use the tool for all of its intended functionalities. The original procurement documentation states that [REDACTED] was intended to enforce [REDACTED] and [REDACTED] on the [REDACTED] network. In late 2019, CISO management stopped attempting to use [REDACTED] to implement [REDACTED] and in late 2021, stopped attempts to use it to implement [REDACTED].

Currently, [REDACTED] is only being used for [REDACTED],⁷ one of the components of [REDACTED]. The existing [REDACTED] tool uses the asset data from [REDACTED] to enforce [REDACTED] policies.

CISO could not implement [REDACTED] because Telecom had another tool already on the network to enforce [REDACTED] and [REDACTED] and the two tools could not operate simultaneously.⁸ As previously mentioned, CISO acquired [REDACTED] despite Telecom's opposition because there were no internal controls for the CIO to approve cybersecurity purchases when there are conflicting stakeholder interests.

“Supply Management made a business decision to issue contract modifications instead of delivery orders to expedite the procurement process.”

By not using [REDACTED] for its intended functionality, [REDACTED] and [REDACTED], the Postal Service may have wasted funds and is at risk of unnecessarily spending additional funds on the contract. For example, an October 2021 internal document stated that the Postal Service has three similar products that, when combined, could provide the needed capability. The document also noted the product's negative

return on investment did not justify its cost and recommended replacement of [REDACTED]. In June 2022, management stated they are performing further evaluation of [REDACTED] current use on the network and had not yet made a final determination of whether to continue its use. We determined that the Postal Service committed to spend an additional \$11 million through FY 2024 for [REDACTED] maintenance and support, funds which could be put to better use.

Recommendation #2

We recommend the **Vice President, Chief Information Security Officer**, complete the current evaluation of [REDACTED] on the [REDACTED] network and if necessary, coordinate with the **Vice President, Supply Management**, to attempt to renegotiate the terms of the contract accordingly.

Finding #2: Ordering Procedures on the [REDACTED] Contract

Supply Management did not follow ordering procedures on one of the three contracts reviewed. They issued contract modifications⁹ for four of 10 [REDACTED] purchases (40 percent) while the contract specified that delivery orders¹⁰ must be used.¹¹

Supply Management made a business decision to issue contract modifications instead of delivery orders to expedite the procurement process. Management stated that they continued this practice to remain consistent, avoid confusion, and shorten the process. However, Supply Management systems categorize contract expenses using delivery orders, so using contract modifications can make it difficult for staff to manage contract costs. For example, in this case, the audit team could not easily differentiate between [REDACTED] purchases for the [REDACTED] and [REDACTED] networks. If Supply Management wanted to identify the costs for each individual implementation, they would have to undergo a manual process of comparing information in the contract modifications. Pending the results of the assessed business need as part of recommendation #2,

7 [REDACTED]
8 While [REDACTED] and [REDACTED] have the ability to integrate, only one tool can be used to enforce [REDACTED] policies.

9 A written alteration in the specifications, delivery point, rate of delivery, contract period, price, quantity, or other terms of an existing contract.

10 An order issued to a supplier to deliver goods under an existing indefinite-delivery contract.

11 Contract Modification 6 stated that delivery orders will be used going forward. The four modifications we identified were issued after Modification 6.

management should follow its contracting guidelines should additional purchases be required against the [REDACTED] contract.

Recommendation #3

We recommend the **Vice President, Supply Management**, instruct the contracting officer to follow the terms of the contract to issue delivery orders for purchases during the remaining life of the [REDACTED] contract.

Finding #3: Clauses and Provisions on the [REDACTED] Contract

Supply Management did not include required clauses and provisions or document deviation approvals on one of the three contracts reviewed. Some of the missing clauses on the [REDACTED] contract included equal opportunity language designed to prohibit the contractor from discriminating against veterans and workers with disabilities. In addition, a missing provision related to information technology was meant to ensure compliance with information technology standards, policies, and general Postal Service guidance (see Table 1).

Table 1. Missing Clauses and Provision in the [REDACTED] Contract

Equal Opportunity Clauses	Information Technology Provision
<ul style="list-style-type: none"> • Clause 9-9: Equal Opportunity Preaward Compliance of Subcontracts • Clause 9-13: Equal Opportunity for Workers with Disabilities • Clause 9-14: Equal Opportunity for VEVRAA Protected Veterans 	<ul style="list-style-type: none"> • Provision 4-7: Postal Computing Environment

Source: OIG analysis of the [REDACTED] contract.

The Postal Service’s Supplying Principles & Practices (SP&P) stipulate that these specific clauses and provisions must be included in the contract unless a deviation is approved.¹² However, the incomplete contracting practices occurred because there was no requirement that management review contract language or verify that contracting officers¹³ documented a deviation approval prior to execution. Management acknowledged that they may need to provide additional oversight on high-visibility contracts.

“Without the ‘Equal Opportunity for Workers with Disabilities’ clause, the Postal Service is at risk of a discrimination claim and related monetary damages.”

Without the information technology provision, the Postal Service does not have any contractual remedy from the supplier if the supplier fails to follow standards, policies, and general guidance (handbooks, technical bulletins, etc.) for tools to meet Postal Service business requirements. Further, without the equal opportunity clauses, the Postal Service could face significant financial loss. For example, without the “Equal Opportunity for Workers with Disabilities” clause, the Postal Service is at risk of a discrimination claim and related monetary damages. The Postal Service could also be at risk of fees and penalties if proven that it failed to comply with Department of Labor regulations regarding the fair treatment of veterans. Lastly, these clauses help the Postal Service meet its commitment to promote diversity and inclusion of its employees, customers, and suppliers.¹⁴

We determined the Postal Service spent \$35.5 million on goods and services under this contract and consider this amount as unsupported questioned costs.¹⁵

¹² SP&P, Section 7-6.1, effective August 7, 2015, and updated on June 20, 2020.

¹³ Postal Service officials responsible for carrying out the solicitation, award, management, and termination of contracts.

¹⁴ Postal Service diversity and inclusion statement.

¹⁵ Costs that are called into question because of missing or incomplete documentation, or because of failure to follow required procedures. In this case, we do not mean the costs were unnecessary, rather unsupported by proper documentation.

Recommendation #4

We recommend the **Vice President, Supply Management**, instruct the contracting officer to attempt to modify the [REDACTED] contract to incorporate the required clauses and provision, or document a deviation approval as required by policy.

Recommendation #5

We recommend the **Vice President, Supply Management**, establish a management review process to verify that required clauses and provisions are included in high-visibility and high-value contracts, and establish a contract value threshold to trigger this process.

Finding #4: Contract Document Maintenance

Supply Management did not maintain required procurement process documents for two of three contracts we reviewed. Key documents for the [REDACTED] and [REDACTED] contracts were missing from the document management system and Supply Management could not locate copies outside of the system (see Table 2 for details).

Table 2. Missing Contract Documentation

Contract	Contract Number	Missing Documentation
[REDACTED]	[REDACTED]	Contracting Officer Representative (COR) Letter of Appointment
[REDACTED]	[REDACTED]	Advanced Notification of Contracts Award
[REDACTED]	[REDACTED]	Unsuccessful Supplier Notification

Source: OIG analysis of [REDACTED] and [REDACTED] contracts.

According to the SP&P,¹⁶ Supply Management is responsible for keeping contract documentation up to date and relevant in the documentation management

system.¹⁷ However, there was no requirement for management to verify all required contract documentation for these contracts was timely uploaded. Management stated that due to workload and time constraints, they did not have enough resources to upload the required documentation. Furthermore, they stated that due to an email system change, some emails containing important contract documentation were lost.

Without evidence of required documentation, management cannot ensure that contracting activities were properly executed and that business processes were in place to attain best value. For example, the contracting officer representative letter of appointment ensures a qualified representative is assigned to manage the contract. Without this letter documented, management cannot be assured that qualified personnel are managing contracts. Additionally, the unsuccessful supplier notification ensures that suppliers who did not win the contract were notified promptly. Without documented proof of timely notification, management cannot be assured that supplier relationships are preserved, which could put the Postal Service’s reputation and brand at risk.

“Without documented proof of timely notification, management cannot be assured that supplier relationships are preserved, which could put the Postal Service’s reputation and brand at risk.”

Recommendation #6

We recommend the **Vice President, Supply Management**, verify all required contract documentation for the [REDACTED] and [REDACTED] contracts are stored in the document management system.

¹⁶ SP&P, Section 3-6, effective August 7, 2015, and updated on September 1, 2021.
¹⁷ Contract Authoring and Management System (CAMS).

Management's Comments

Management agreed with findings 2, 4, and 5 and generally agreed, with exceptions, to findings 1 and 3. Management agreed with recommendations 1, 2, 3, and 6, and partially agreed with recommendations 4 and 5. Management disagreed with the monetary impact.

Regarding finding 1, management objected to the OIG's assertion that key internal stakeholder agreement was not obtained, and that policy is needed for additional oversight. They noted that there are multiple oversight controls for acquisition and investment such as the Decision Analysis Report, non-competitive purchase request, and eBuyPlus funding and approval processes. Management also stated that they considered Telecom's input throughout the purchase process and that the Vice President, IT, who oversaw Telecom at the time, reviewed and concurred with the Decision Analysis Report.

Regarding finding 3, management stated that the IT provision cited in the report relates to the solicitation phase and the provision is not required to be in the contract. In relation to the equal opportunity clauses, management stated that the contracting officer obtained an equal opportunity pre-award clearance from the U.S. Department of Labor and confirmation of the supplier's filing of their 2021 VETS-4212 report related to veterans.

Regarding recommendation 1, management stated that the CIO will review existing controls for high-dollar value cybersecurity tool procurements and develop additional oversight processes if determined necessary. The target implementation date is February 28, 2023.

Regarding recommendation 2, management will complete their current evaluation of [REDACTED] on the [REDACTED] network and, if necessary, attempt to renegotiate the terms of the contract. The target implementation date is February 28, 2023.

Regarding recommendation 3, management will issue a formal communication to the contracting officer to follow the terms of the contract to issue delivery orders for purchases during the remaining life of the [REDACTED] contract. The target implementation date is October 31, 2022.

Regarding recommendation 4, management will issue a formal communication to the contracting officer to attempt to modify the [REDACTED] contract to incorporate the required clauses. The target implementation date is December 31, 2022.

Regarding recommendation 5, management will establish a process to verify that any required clauses that may be added in the future to the contracts assessed in this audit are included and establish certain triggers to activate the process. The target implementation date is December 31, 2022.

Regarding recommendation 6, management will verify that all required contract documentation for the [REDACTED] and [REDACTED] contracts are stored in CAMS. The target implementation date is December 31, 2022.

Regarding the monetary impact related to recommendation 2, management stated that funds were not wasted or at risk of being wasted in the future. Furthermore, management disagreed with the statement that there are three similar products that, when combined, could provide the capability needed in lieu of [REDACTED]. Management also stated that the supplier stated that the cost would be the same regardless of full deployment of the capabilities and the Postal Service has a contractual obligation for FY 2023 and FY 2024 maintenance costs. Regarding the monetary impact related to recommendation 4, management disagreed and stated that it does not represent a true monetary loss.

See [Appendix B](#) for management's comments in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations in the report and corrective actions should resolve the issues identified in the report.

Regarding finding 1, the OIG reviewed the Decision Analysis Report, non-competitive purchase request, and eBuyPlus controls established by management. As noted in the report, the Decision Analysis Report, while approved by the CIO and other executives, does not specify the tools to be purchased. Further, the non-competitive purchase request and eBuyPlus processes reviewed only included CISO approval and not the approval of the vice president who oversaw Telecom or the CIO. Although we recognize management's assertion that they completed the acquisition in accordance with existing Supply Management policies, these policies and the processes noted by management do not require CIO approval to purchase specific cybersecurity tools when there were conflicting stakeholder interests within the CIO organization. As noted in their response to the recommendation, management agreed to review existing controls for high-dollar value cybersecurity tool procurements, and this should address the concerns outlined in the report.

Regarding finding 3, we recognize that the provision related to IT was included in the solicitation. However, as noted in the Postal Service's purchasing manual, this provision must also be included in all IT contracts. Although we were provided the VETS-4212 report for the [REDACTED] contract, we were not provided the VETS-4212 or the pre-award clearance for the [REDACTED] contract. Further,

the VETS-4212 report does not cover the Equal Opportunity for Workers with Disabilities clause cited in the report, rather it relates to the Employer Reports on Employment of Protected Veterans clause. As noted in their response to the recommendation, management agreed to attempt to incorporate the required clauses or document a deviation approval, which should address the concerns identified in the report.

Regarding the monetary impact, management agreed to attempt to renegotiate the contract terms, if necessary, which could lead to potential future savings on the [REDACTED] contract. Management disagreed that funds were wasted; however, as noted in the report, CISO spent approximately \$56 million over four years on the [REDACTED] tool and could not fully implement its intended capabilities. Additionally, an internal CISO document stated that there are three tools that, if combined, could provide the needed capability. Therefore, we consider it appropriate to claim "funds put to better use" given the funds represent potential future savings. Furthermore, in response to management's assertion that the unsupported questioned costs claimed does not represent a true monetary loss, the report does not assert the costs were unnecessary, rather, that they were called into question because of incomplete documentation.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. The recommendations 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	11
Scope and Methodology	11
Prior Audit Coverage	11
Appendix B: Management’s Comments	12

Appendix A: Additional Information

Scope and Methodology

The scope of our audit covered two judgmentally selected cybersecurity tools of 82 total tools the Postal Service purchased to protect its systems, networks, and programs from digital attacks. To accomplish our objective, we:

- Reviewed the three contracts related to the two judgmentally selected tools and analyzed the contracts for compliance with policy.
- Evaluated the contract modifications and delivery orders executed under the selected contracts.
- Reviewed and evaluated the procurement process and management of the selected tools and related documentation.
- Reviewed policies and procedures related to internal controls for managing cybersecurity tools.
- Interviewed Supply Management officials to determine their process for providing oversight and management of the contract and delivery orders.
- Interviewed Supply Management, CISO, and Telecom officials to obtain information and documentation related to the procurement process, and use and maintenance of the cybersecurity tools.

We conducted this performance audit from June 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 15, 2022, and included their comments where appropriate.

We assessed the reliability of Contract Authoring and Management System data by testing its validity and having discussions with Postal Service officials. We assessed the reliability of the National Accounting Oracle Financials Application data by testing its completeness, accuracy, and validity, and having discussions with Postal Service officials.

Prior Audit Coverage

The OIG did not identify any prior audits or reviews related to the objective of this audit within the last five years.

Appendix B: Management's Comments



August 16, 2022

JOHN CIHOTA
DIRECTOR, AUDIT SERVICES

SUBJECT: Procurement and Management of Cybersecurity Tools (Project Number 21-129-DRAFT)

Thank you for the opportunity to provide comments to the Office of Inspector General's (OIG's) draft audit report entitled, "*Procurement and Management of Cybersecurity Tools (Project Number 21-129-DRAFT)*." Management has reviewed the report and generally agrees with the findings, recommendations, and monetary impact except as noted below.

Finding #1: [REDACTED] Procurement and Implementation

The OIG details that while the Postal Service successfully implemented the [REDACTED] product on the [REDACTED] issues were identified from the Corporate Information Security Office (CISO) and that implementation of [REDACTED] on the [REDACTED] network has not been accomplished to date. The OIG asserts that CISO acquired the tool without obtaining agreement from key internal stakeholders and found that CISO was ultimately unable to use the full capabilities of [REDACTED] and [REDACTED] features despite procuring these tools to enforce [REDACTED] and [REDACTED] on the [REDACTED] network.

Management takes exception to the OIG's determination that agreement was not obtained from key internal stakeholders and disagrees with its resultant monetary impact and finding that the development of policy is needed for additional oversight or controls. The Postal Service already has in place multiple oversight controls for acquisitions and investments such as the Decision Analysis Report (DAR) tollgate and approval process, the Non-competitive Purchase Request (NPR) process, and the eBuyPlus requisition funding approval process. Each of these processes were properly implemented and executed for the [REDACTED] award and the acquisition was completed in accordance with existing Supply Management (SM) policies. The OIG identifies Network and Compute Technology (NCT) as the key stakeholder whose concurrence was not obtained. The OIG's characterization of this as a lack of control is unfounded. The Vice President of Information Technology, who oversaw NCT at the time, reviewed and provided concurrence on the DAR business case. While NCT's input was considered throughout the purchase process, it is the Chief Information Office (CIO), Telecom's parent organization, who possesses and exercised the ultimate authority to approve the purchase.

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260
WWW.USPS.COM

Finding #3: Clauses and Provisions on the [REDACTED] Contract

The OIG further found that, as concerns the [REDACTED] contract, the contracting officer did not include required clauses and provisions or document deviation approvals. The report's Table 1 cites missing clauses which included equal opportunity language designed to protect workers against discrimination by the supplier and a provision related to information technology meant to ensure compliance with information technology standards, policies, and general Postal Service guidance. Management takes issue with this finding and the associated monetary impact assessed. As stated during the exit meetings, provisions are used and relate to the solicitation phase of an acquisition and are not required to be included in the contract. Contract clauses pertain to the contract.

Concerning the Equal Opportunity clauses, the OIG asserts that the Postal Service could face significant financial loss and that, without the "Equal Opportunity for Workers with Disabilities" clause, the Postal Service is at risk of a discrimination claim and related monetary damages. A review of the contract file confirms the contracting officer did obtain an equal employment opportunity pre-award clearance from the U.S. Department of Labor (DOL), Office of Federal Contract Compliance Programs, as well as confirmation from DOL of the supplier's filing of their 2021 VETS-4212 report related to veterans. This documentation was provided to the OIG prior to the issuance of the draft audit report.

Monetary Impact

The Postal Service respectfully disagrees with the monetary impact assessed in the amount of approximately \$46.5 million, in connection with Recommendations #2 (\$11 million) and #4 (\$35.5 million). Regarding the \$35.5 million in unsupported questioned costs, management notes that this does not represent a true monetary loss as the OIG also mentions in Footnote 17 on page 6 of the report.

Management disagrees with the OIG's assertion that funds were wasted, or at risk of being wasted in the future, had three similar products been combined to provide the capability needed in lieu of [REDACTED]. The supplier has indicated that the cost would have been the same whether the Postal Service fully deployed [REDACTED] or [REDACTED] or not. Responding to specific previous events, and ensuring the ongoing security of our networks, the Postal Service appropriately contracted and is contractually obligated for the maintenance costs forecasted for FY23 and FY24. Given these facts and the robust asset visibility presently provided by [REDACTED] or [REDACTED] we object to the \$11 million monetary impact determination.

Management would like to thank the OIG for their review and recommendations. We appreciate the call for action to evaluate the contract and capabilities of [REDACTED].

Recommendation #1:

We recommend the **Chief Information Officer and Executive Vice President**, determine whether additional oversight is needed to facilitate key stakeholder concurrence on future high-value or high-visibility cybersecurity tool procurements, and if necessary, develop policy to implement additional oversight or controls.

Management Response/Action Plan:

Management agrees with this recommendation. The CIO will review existing controls for high dollar value cybersecurity tool procurements and develop additional oversight processes if determined necessary. As noted above, the Postal Service already has in place multiple oversight controls such as the DAR tollgate process, the NPR process, and the eBuyPlus funding approval process. Further, SM has several reviews and existing policies in place for high-level and high-value awards including the Competition Advocate review for noncompetitive awards, Law Department review, and the Contract Authoring Management System (CAMS) review and award release process.

Target Implementation Date:

February 28, 2023

Responsible Official:

Chief Information Officer and Executive Vice President

Recommendation #2:

We recommend the **Vice President, Chief Information Security Officer**, complete the current evaluation of ██████████ on the ██████████ network and if necessary, coordinate with the **Vice President, Supply Management**, to attempt to renegotiate the terms of the contract accordingly.

Management Response/Action Plan:

Management agrees with this recommendation. We will complete the current evaluation of ██████████ on the ██████████ network and, if necessary, attempt to renegotiate the terms of the contract accordingly.

Target Implementation Date:

February 28, 2023

Responsible Official:

Vice President, Chief Information Security Officer in coordination with the Senior Director, Technology Infrastructure Portfolio, Supply Management

Recommendation #3:

We recommend the **Vice President, Supply Management**, instruct the contracting officer to follow the terms of the contract to issue delivery orders for purchases during the remaining life of the [REDACTED] contract.

Management Response/Action Plan:

Management agrees with this recommendation. We will issue a formal communication to the contracting officer to follow the terms of the contract to issue delivery orders for purchases during the remaining life of the [REDACTED] contract.

Target Implementation Date:

October 31, 2022

Responsible Official:

Vice President, Supply Management
Senior Director, Technology Infrastructure Portfolio, Supply Management

Recommendation #4:

We recommend the **Vice President, Supply Management**, instruct the contracting officer to attempt to modify the [REDACTED] contract to incorporate the required clauses and provision, or document a deviation approval as required by policy.

Management Response/Action Plan:

Management agrees with this recommendation in part. As stated during the exit meetings, provisions relate to solicitations and are often not included in the contract, while clauses pertain to the contract. Management will issue a formal communication to the contracting officer to attempt to modify the [REDACTED] contract to incorporate the required clauses or document a deviation approval as required by policy.

Target Implementation Date:

December 31, 2022

Responsible Official:

Vice President, Supply Management
Senior Director, Technology Infrastructure Portfolio, Supply Management

Recommendation #5:

We recommend the **Vice President, Supply Management**, establish a management review process to verify that required clauses and provisions are included in high-visibility and high-value contracts, and establish a contract value threshold to trigger this process.

Management Response/Action Plan:

Management agrees with this recommendation in part. The OIG's audit pertained to three contracts. SM has existing review processes concerning the inclusion of required clauses into contracts drafted for award, including Law Department review. Therefore, management will establish a review process to verify that any required clauses that may be added to those specific contracts in the future are included, establishing certain triggers to activate the process.

Target Implementation Date:

December 31, 2022

Responsible Official:

Vice President, Supply Management
Director, Supply Management Infrastructure, Supply Management

Recommendation #6:

We recommend the **Vice President, Supply Management**, verify all required contract documentation for the [REDACTED] and [REDACTED] contracts are stored in the document management system.

Management Response/Action Plan:

Management agrees with this recommendation. We will verify all required contract documentation for the [REDACTED] and [REDACTED] contracts are stored in the Contract Authoring Management System (CAMS).

Target Implementation Date:

December 31, 2022

Responsible Official:

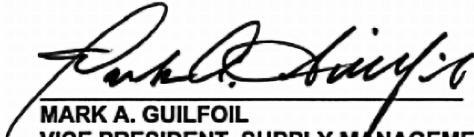
Vice President, Supply Management
Senior Director, Technology Infrastructure Portfolio, Supply Management

E-SIGNED by William.E Koetz
on 2022-08-16 10:51:03 CDT

PRITHA N. MEHRA
CHIEF INFORMATION OFFICER AND EXECUTIVE VICE PRESIDENT

E-SIGNED by Heather.L Dyer
on 2022-08-16 07:47:32 CDT

HEATHER L. DYER
VICE PRESIDENT, CHIEF INFORMATION SECURITY OFFICER



MARK A. GUILFOIL
VICE PRESIDENT, SUPPLY MANAGEMENT

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