Office of Inspector General | United States Postal Service

Audit Report

Cybersecurity Incident Detection and Response Capability

Report Number 19-012-R20 | July 29, 2020

Table of Contents

Cover
Highlights 1
Objective 1
Findings 1
Recommendations 2
Transmittal Letter 3
Results 4
Introduction/Objective 4
Background 4
Finding #1: [redacted] Not Detected 5
Recommendation #1 6
Finding #2: Metrics to Measure the Incident Response Capability Not Defined 6
Recommendation #2 6
Finding #3: Incident Response Investments Not Tracked 7
Recommendation #3 7
Finding #4: Identified [redacted] 7
Recommendation #4 7
Recommendation #5 7
Finding #5: Cybersecurity Incident Response Tickets Not Closed 8
Recommendation #6 8
Management's Comments 8
Evaluation of Management's Comments 9
Appendices 10
Appendix A: Additional Information 11
Scope and Methodology 11
Prior Audit Coverage 12
Appendix B: Examples of Incident Management Metrics 13
Appendix C: Management's Comments 14
Contact Information 21

Highlights

Objective

Our objective was to determine if the U.S. Postal Service has a cybersecurity incident response capability to effectively detect, analyze, and respond to cyber threats.

The Postal Service faces ongoing cyber threats and challenges that directly impact customers, partners, and employees. These threats could cause harm to information resources in the form of destruction, disclosure, adverse modification of data, or denial of services. For example, the Postal Service suffered a significant data breach in 2014 that exposed the personal data of about 800,000 current and former career and non-career employees. The breach cost the Postal Service [redacted] million in known costs. Currently, there are over [redacted] active user accounts with access to the network; therefore, it is critical to have a robust cybersecurity incident detection and response capability to address continuous threats.

As a result of the 2014 breach, the Corporate Information Security Office (CISO) was established to safeguard the Postal Service's network. The CISO then established the Cybersecurity Operations Center (CSOC) to detect and respond to cyber events and incidents.

To support a sound cybersecurity foundation, the Postal Service approved [redacted] million in 2017 through the Cybersecurity Decision Analysis Report (DAR) III, Enhancement and Maturity. According to the DAR, this investment would support the continued ability to recruit, develop, and retain a cybersecurity workforce capable of supporting continuous threat monitoring, threat remediation and response, vulnerability management, and incident response activities that are critical to the Postal Service's success.

We conducted a test during February and March 2020 to determine whether the Postal Service could identify and respond to known cyber threats. We also reviewed the CISO's Cybersecurity Incident Response Plan, CSOC tickets initiated between March 1 and September 30, 2019, and Cybersecurity DAR III to determine compliance with policy, procedures, or industry best practices. We did not review post-incident activities as the CSOC did not declare any cybersecurity incidents during our scope period.

We planned our fieldwork before the President of the United States issued the national emergency declaration concerning the novel coronavirus outbreak (COVID19) on March 13, 2020. The results of this audit do not reflect operational changes and/or service impacts that may have occurred as a result of the pandemic.

Findings

The Postal Service does [redacted] The CSOC detected very little of the [redacted] we introduced to the Postal Service network as a test procedure from February 18 through March 6, 2020. While the CSOC detected [redacted] activity, they were unable to detect any of the [redacted] other activities executed multiple times. For example, they did not detect the activities associated with [redacted] of [redacted] across the network and a [redacted] launched on the network. Without appropriate [redacted], active threats could go undetected, possibly leading to theft and modification of data or impact on the availability of critical systems.

> *"The Postal Service* [redacted]

We also found the CISO had not developed metrics to measure the effectiveness of their incident response capability. Best practices adopted from Carnegie Mellon recommend common metrics such as Mean Time to Detect, Mean Time to Respond, and Percentage of Events Declared as Incidents. Without effective metrics, management cannot make informed decisions to improve the incident response plan or enhance their incident response capability.

In addition, the CISO did not track or monitor investments by project as specified in DAR III. In our prior audit issued in November 2018, we identified a similar issue with tracking investments related to Cybersecurity DAR II, Improvements. Without tracking detailed project expenditures, management is unable to ensure that funds are allocated appropriately, budgets are not overspent, and enhancement projects are executed on-time.

Also, during our review of the Cybersecurity Incident Response tickets in [redacted], we found [redacted] active CSOC module users have the ability to [redacted] Without proper [redacted], users can introduce [redacted] to the Postal Service network, potentially [redacted]. Lastly, we reviewed a sample of [redacted] cybersecurity tickets initiated between March 1 and September 30, 2019, to determine compliance with the incident response plan and standard operating procedures. CSOC analysts appropriately closed [redacted] of the [redacted] internal tickets, and the [redacted] remaining tickets were reassigned to a group outside of the CSOC for further investigation. These tickets remained open for over a year with no status update. Without a process to update the status of open tickets and resolve issues presented in tickets, the possibility exists for compromised information resources and disrupted operations due to unresolved cyber threats.

Recommendations

We recommend management:

- Complete the [redacted] project implementation as identified in Cybersecurity DAR III and implement the necessary [redacted] to detect internal malicious activity.
- Determine which incident detection and response metrics are meaningful to the organization and establish a process to measure the effectiveness of the incident detection and response capability.
- Track one-to-one alignment of actual investments with Cybersecurity DAR III requests for each project.
- Develop procedures for the safe handling of [redacted] or develop a risk acceptance letter.
- Create a notification within the Cybersecurity Operations Center module in [redacted] notifying users of potential [redacted]
- Develop a process to regularly review unresolved tickets transferred to another office for resolution, verify status, and ensure timely closure.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

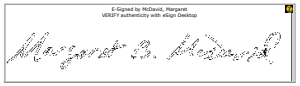
July 29, 2020

MEMORANDUM FOR: SCOTT R BOMBAUGH
ACTING CHIEF INFORMATION OFFICER AND EXECUTIVE VICE PRESIDENT

GREGORY S. CRABB
VICE PRESIDENT, CHIEF INFORMATION SECURITY OFFICER

PRITHA MEHRA
VICE PRESIDENT, INFORMATION TECHNOLOGY

SHAHPOUR ASHAARI
ACTING VICE PRESIDENT, ENGINEERING SYSTEMS



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

SUBJECT: Audit Report – Cybersecurity Incident Detection and Response Capability (Report Number 19-012-R20)

This report presents the results of our audit of the U.S. Postal Service's Cybersecurity Incident Detection and Response Capability.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Mary K. Lloyd, Director, Information 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 Cybersecurity Incident Detection and Response Capability (Project Number 19-012). Our objective was to determine if the Postal Service has a cybersecurity incident response capability to effectively detect, analyze, and respond to cyber threats. We intended to review post-incident activities, however the Cybersecurity Operations Center (CSOC)[1] did not declare any cybersecurity incidents during our scope period.

We planned our fieldwork before the President of the United States issued the national emergency declaration concerning the novel coronavirus disease outbreak (COVID19) on March 13, 2020. The results of this audit do not reflect operational changes and/or service impacts that may have occurred as a result of the pandemic.

Background

The Postal Service faces ongoing cyber threats that directly impact the agency's customers, partners, and employees. Cyber threats could cause harm to information resources in the form of destruction, disclosure, adverse modification of data, or denial of services. For instance, the Postal Service suffered a significant data breach in fiscal year 2014 that exposed the personal data of about 800,000 current and former career and non-career employees.[2] The breach cost the Postal Service [redacted] million in known costs. Currently, there are over [redacted] with an active user account that allows access to the Postal Service network. Therefore, it is critical to have a robust cybersecurity[3] incident detection and response capability to address continuous threats.

The Corporate Information Security Office (CISO) was founded in response to the 2014 breach and was established to safeguard the Postal Service's network. The CISO established the CSOC to monitor, detect, and respond to cyber threats, and proactively hunt for threats. In addition, the CISO created the *Cybersecurity Incident Response Plan*[4] as a guide to detecting and responding to cybersecurity events[5] and incidents[6] and to conduct post-incident activities.[7] The plan states that it aligns with the principles of Carnegie Mellon University's CERT™ Resilience Management Model (CERT-RMM)[8] and is comprised of a series of steps collectively known as the Cybersecurity Incident Response Process. This process consists of the seven phases shown in Figure 1.

Figure 1. Overview of the Cybersecurity Incident Response Process

Source: USPS Cybersecurity Incident Response Plan, Version 4.0.

1 A dedicated operations center where enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops, and other endpoints) are monitored, assessed, and defended.
2 Postal Service career and non-career employees nationwide include those working for the Postal Regulatory Commission and the OIG.
3 Measures to provide information assurance, improve resilience to cyber incidents, and reduce cyber threats.
4 *The USPS Cybersecurity Incident Response Plan*, Version 4.0, dated September 20, 2019.
5 An event is one or more occurrences, possibly minor, that affect organizational assets and have the potential to disrupt operations. An event may or may not become an incident.
6 An incident is an event that causes a functional, informational, or recoverability impact.
7 Post-incident activities consist of After Action Reports which document the lifecycle of a cybersecurity incident.
8 Carnegie Mellon University's Software Engineering Institute, CERT-RMM, is the foundation for a *Process Improvement Approach To Operational Resilience Management*, Version 1.2, dated February 2016. The collection is broken down into 26 process areas.

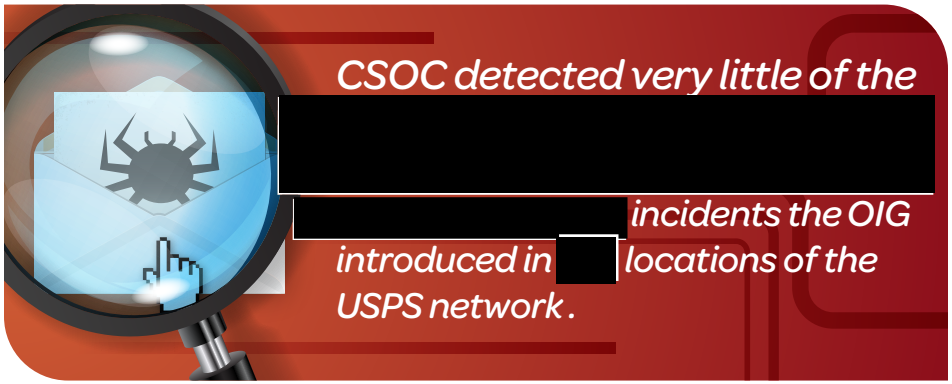
- Alert & Scope – Confirm receipt of a potential cybersecurity event or incident, determine if it is a cybersecurity incident.
- Investigate – Determine extent of compromise and escalate or de-escalate as appropriate.
- Contain – Minimize the spread of compromise.
- Eradicate & Mitigate – Remove artifacts of compromise and prevent future compromise.
- Recover – Return assets to operational-ready state.
- Report – Document the incident and make notifications as required.
- Lessons Learned – Improve future security posture by learning from previous experiences.

To support a sound cybersecurity foundation, the Postal Service approved an investment of [redacted] million in 2017 through Cybersecurity Decision Analysis Report (DAR) III.[9] According to the DAR, this investment would support the continued ability to recruit, develop, and retain a cybersecurity workforce capable of supporting continuous threat monitoring, threat remediation and response, vulnerability management, and incident response activities that are critical to the Postal Service's success.

We found that the Postal Service does [redacted]

Finding #1: [redacted] Not Detected

We conducted an incident response test from February 18 through March 6, 2020, designed to [redacted] and executing



tactics, techniques, and procedures[10] from [redacted] Postal Service locations. Over the testing period, the CSOC detected very little of the [redacted] activity that we introduced to the Postal Service network. While their tool detected [redacted] activity, they were unable to detect any of the [redacted] other activities executed multiple times. For example, Postal Service did not detect activities associated with:

- [redacted]
- [redacted].
- [redacted]

This occurred because [redacted] project was not fully implemented as specified in Cybersecurity DAR III. Segmentation helps identify the strategic placement of [redacted] needed to detect potential malicious activity. The [redacted] project expected completion date of January 16, 2020 has been delayed until September 2021.

9 *Cybersecurity DAR III, Enhancement and Maturity,* dated December 11, 2017.

10 Tactics, techniques, and procedures (TTP) can be used as a means of profiling threat actors. Tactics represent the "why" of a technique and describe what an adversary is trying to accomplish. Techniques represent how the threat actor achieves a tactical objective. Procedures detail how an adversary would implement the technique to achieve an objective.

11 [redacted]

12 [redacted]

13 [redacted]

According to Postal Service policy,[14] the network infrastructure must be protected at a level commensurate with its value to the Postal Service. Such protection must include implementation of the physical, administrative, and [redacted] and processes that safeguard the confidentiality, availability, and integrity of the network and the data in transit. Without these [redacted], active threats could go undetected, possibly leading to theft of Personally Identifiable Information, modification of data, or an impact on the availability of critical systems.

Recommendation #1

We recommend the **Vice President, Chief Information Office**, direct **Corporate Information Security Office, Information Technology**, and **Engineering**, to complete the [redacted] project implementation as identified in Cybersecurity DAR III and implement the necessary [redacted].

Finding #2: Metrics to Measure the Incident Response Capability Not Defined

We found the CISO had not developed or implemented metrics to effectively measure its incident response capability. Metrics are used to identify processes that are working well and those that need improvement. According to CERT-RMM, organizations should measure actual performance against the plan, review results, identify issues in the plan or the performance of the plan, and take corrective action. The model includes examples of over 20 common metrics shown in Appendix B. In addition, the National Institute of Standards and Technology Computer Security Incident Handling Guide[15] describes essential uses of metric data, including identifying the following:

> *"The Postal Service had not developed or implemented metrics to effectively measure its incident response capability."*

- Justification for additional funding
- Systemic security weaknesses
- Incident trends
- Need for additional [redacted]

The CISO explained that they are maturing in this area, using the CERT-RMM as a descriptive guideline; however, they have not yet determined which metrics are most meaningful to the organization and provided no timeline for doing so. Without effective metrics, management cannot make informed decisions to improve the incident response plan or enhance their incident response capability.

Subsequent to our audit fieldwork, CISO provided a dashboard to demonstrate that they are tracking metrics related to the incident response capability. Additionally, CISO provided daily and monthly slides that show cybersecurity operations statistics. However, the dashboard and slides only show the number of tickets opened and closed. Tracking this information speaks to the workload but does not provide insight into the effectiveness of the incident response capability that would enable management to make informed decisions to improve the incident response plan or enhance the incident response capability.

Recommendation #2

We recommend the **Manager, Cybersecurity Operations**, determine which incident detection and response metrics are meaningful to the organization and establish a process to measure the effectiveness of the incident detection and response capability.

14 *Handbook AS-805, Information Security*, Section 11, Network Security, dated November 2019.
15 *National Institute of Standards and Technology Special Publication 800-61*, Revision 2, dated August 2012. This publication is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems.

Finding #3: Incident Response Investments Not Tracked

"The CISO did not track or monitor investments by projects as specified in the Cybersecurity DAR III."

The CISO did not track or monitor investments by projects as specified in the Cybersecurity DAR III. The investments approved in this DAR are categorized into 10 cybersecurity capabilities, such as [redacted] We found that, while the CISO provided required quarterly reporting on the status of these investments, they have not developed a process to assess expenditures related to these capabilities. We identified a similar issue with tracking investments related to Cybersecurity DAR II[16] in our prior audit.[17] At that time, CISO management stated they developed a process to track detailed spending at the project level for DAR III and may use the process to continue DAR II tracking. However, during our current audit, the CISO stated they cannot track spending at the project level due to [redacted] of the Enterprise Data Warehouse (EDW);[18] therefore, the CISO only tracked spending at the levels available in EDW, such as finance number, financial performance report line, and general ledger account. Without tracking detailed project expenditures, management is unable to ensure funds are allocated appropriately, budgets are not overspent, and enhancement projects are executed on time.

Recommendation #3

We recommend the **Deputy, Corporate Information Security Office**, track one-to-one alignment of actual investments with Cybersecurity Decision Analysis Report III Enhancement and Maturity requests for each project.

Finding #4: [redacted] in [redacted]

During our review of the Cybersecurity Incident Response tickets in [redacted],[19] we found [redacted] active users of the CSOC module that have the ability to [redacted]. According to policy,[21] all Postal Service information resources must be protected against the introduction of viruses and other types of malicious code that can jeopardize information security by contaminating, damaging, or destroying information resources. Also, it is the organization's responsibility to review [redacted] and procedures; establish additional, appropriate corrective measures, if required; and reduce the likelihood of recurrence.

This occurred because the [redacted]. Management stated CSOC analysts are trained to handle the [redacted] and there is [redacted] for the [redacted]. Without proper [redacted] to the Postal Service network, potentially [redacted]

Recommendation #4

We recommend the **Manager, Cybersecurity Operations Center**, develop procedures for the safe handling of Cybersecurity Incident Response Ticket [redacted] or develop a risk acceptance letter.

Recommendation #5

We recommend the **Manager, Cybersecurity Operations Center**, create a notification within the Cybersecurity Operations Center module in [redacted] notifying users of potential Cybersecurity Incident Response Ticket [redacted]

16 *Cybersecurity DAR-II*, Improvements, dated July 27, 2015.
17 *Cybersecurity Decision Analysis Reports Review* (Report Number IT-AR-19-002, dated November 19, 2018).
18 The main Postal Service reporting platform is divided into [redacted]
19 [redacted]
20 [redacted]
21 *Handbook AS-805, Information Security*, Section 10-6, Protection Against Virus and Malicious Code, dated November 2019.
22 [redacted]
23 A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Finding #5: Cybersecurity Incident Response Tickets Not Closed

We reviewed a sample of [redacted] tickets[24] from [redacted] initiated between March 1 and September 30, 2019 to determine if CSOC analysts followed processes and procedures when responding to cyber threats. The analysts appropriately closed [redacted] of the [redacted] internal tickets,[25] and the [redacted] remaining tickets were reassigned to a group outside of the CSOC for further investigation. These tickets remained open for over a year with no status update. According to a CSOC Standard Operating Procedure (SOP),[26] it is the responsibility of the event or incident responder[27] to update the ticket regularly for the duration of the event or incident. Additionally, the CERT-RMM states the status of tickets should be reviewed regularly to determine whether to close them or take additional action. These [redacted] open tickets occurred because the CSOC did not have a process for reviewing open tickets transferred to another office for resolution.

Without a process to review open tickets and verify resolution, [redacted]

Recommendation #6

We recommend the **Manager, Cybersecurity Operations Center**, develop a process to regularly review, verify status, and ensure timely closure of unresolved tickets transferred to another office for resolution.

Management's Comments

Management disagreed with finding 2 and did not state whether they agreed or disagreed with the remaining findings. They agreed with recommendations 1, 4, 5, and 6 and disagreed with recommendations 2 and 3.

Management strongly disagreed with the OIG's overall assessment concerning the efficacy of the Postal Service's incident detection and response capabilities. They stated the simulation methodology behind the condition reported was flawed by design, which impaired the findings. Management believes the simulated activities the OIG performed did not support the report's broad generalization that the Postal Service lacks an effective cybersecurity incident response capability.

Regarding recommendation 1, management agreed, but stated the simulation does not demonstrate a business consequence to Postal Service assets, failing to impact sensitive data or critical systems. However, management stated they will implement the [redacted] by September 30, 2021.

Regarding recommendation 2, management notified us via email that they disagreed with this recommendation. The Postal Service engaged Carnegie Mellon University's Software Engineering Institute (SEI) to assess the OIG's finding. The SEI expert concurred with postal management and believes the metrics provided for review sufficiently meet OIG audit requirements.

Regarding recommendation 3, management disagreed and stated the capabilities described in DAR III were not intended to be tracked as individual "projects". Management stated they maintain the budget at the DAR and portfolio levels but do not track it at the capability level. They also stated that CISO submits quarterly compliance reports to address performance relating to the projects.

Regarding recommendation 4, management agreed and stated they have updated the SOP titled [redacted] to address the safe handling of [redacted] and they had completed training staff on these updated procedures by July 12, 2020. Management provided a copy of the updated SOP that includes guidance for handling [redacted]. They provided this with their response letter.

Regarding recommendation 5, management agreed and stated they will update the CSOC [redacted] banner and notify users of potential Cybersecurity Incident Response Ticket [redacted] by July 23, 2020. Management subsequently provided screenshots that caution users of the potential for [redacted] in [redacted] attachments.

24 [redacted]. Tickets may consist of events and incidents.
25 All [redacted] tickets were identified as events.
26 [redacted]
27 Event or incident responders are normally within the CSOC and are responsible for orchestrating response activities.

Regarding recommendation 6, management agreed and stated they implemented processes and procedures to regularly review, verify the status of, and ensure timely closure of unresolved tickets transferred to another office for resolution on July 21, 2020. Management provided evidence of the updated Ticket Closure Process that addresses the process for resolving tickets transferred to another office. They provided this with their response letter.

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

Evaluation of Management's Comments

The OIG considers management's comments responsive to recommendations 1, 4, 5, and 6 and non-responsive to recommendations 2 and 3. Actions planned to address recommendation 1 should address the issues identified.

Regarding management's disagreement with the overall assessment concerning the efficacy of the Postal Service's incident detection and response capabilities and the OIG simulation methodology related to recommendation 1, postal management signed off on the simulation test plan methodology. This included an agreement that the assessment, by design, would not impact sensitive data and critical systems. However, as agreed, the test plan methodology would simulate a threat actor with internal access to the network. Further, the OIG coordinated with postal management on the installation of endpoint security tools on the OIG devices. Management did not bring any of these matters to our attention at that time.

Regarding recommendation 2, the OIG requested metric status supporting the guidelines of the CERT-RMM but did not receive evidence of goal-oriented metrics. The reports management provided represented workload and ticket status and did not speak to the effectiveness of the incident response capability nor how management used the data to make informed decisions. During the audit, the OIG was not made aware of a USPS Incident Management and Control Process Plan. Upon receipt of management's comments, we requested a copy of this document and have not yet received it. Once received, we will evaluate the sufficiency of the document to address the recommendation.

Regarding recommendation 3, DAR III requires the CISO to track one-to-one alignment of actual investments with DAR III requests for each resource/project and conduct quarterly DAR III spending reviews. While they conduct the quarterly reports, the reports did not reflect the status of each project to ensure budgets are not overspent.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. Recommendations 1, 2, and 3 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. We consider recommendations 4, 5, and 6 closed with the issuance of this report.

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 12
Appendix B: Examples of Incident Management Metrics 13
Appendix C: Management's Comments 14

Appendix A: Additional Information

Scope and Methodology

Our audit scope covered the Postal Service's processes and procedures for detecting, analyzing, and responding to cyber incidents. We assessed the Postal Service's ability to execute cyber incident, detection, and response capabilities in the following areas:

- Preparation: The extent to which the Postal Service is prepared to identify potential threats to the network. This includes developing an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. In addition, this includes ensuring the systems, networks, and applications are sufficiently secure; and implementing appropriate safeguards to ensure delivery of critical services.
- Detection & Analysis: The extent to which the Postal Service can take appropriate action to identify the occurrence of a cyber incident.
- Response: Actions taken by an organization to prevent or contain the impact of a cybersecurity incident on its networks during and after the incident takes place. A response is also the extent to which the Postal Service documents the result of a cyber incident threat, identification of lessons learned, and collection and analysis of incident data for correlation and trend analysis.

Our review also required testing at five Postal Service locations:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

To accomplish our objective, we:

- Developed and conducted an incident response test during February and March 2020 to determine whether the Postal Service could identify and respond to known cyber threats. The test referenced the MITRE ATT&CK™ framework[28] and required a trusted agent[29] to coordinate technical activities associated with the assessment.
- Reviewed the CISO's incident response plan to determine compliance with policy, procedures, and alignment with industry best practices.
- Examined a statistical sample of Cybersecurity Incident Response Tickets data in [redacted] initiated between March 1, 2019 – September 30, 2019, to determine compliance with policy, procedures, and alignment with industry best practices.
- Reviewed the incident response capability investments identified in Cybersecurity DAR III, Enhancement and Maturity, to determine compliance with policy and procedures.

We conducted this performance audit from September 2019 through July 2020 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 June 15, 2020 and included their comments where appropriate.

28 A comprehensive matrix of tactics and techniques used by threat hunters, red teamers, and defenders to better classify attacks and assess an organization's risk. The OIG leveraged the framework obtained from MITRE during the month of February 2020.
29 Postal Service employee participating as member of the OIG testing team.

We assessed the reliability of Cybersecurity Incident Response Ticket data by ensuring the data for each sample ticket selected was complete and relevant to cybersecurity event and incident matters. 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	Monetary Impact
Postal Service's Response [redacted]	Determine if the U.S. Postal Service appropriately responded to and mitigated an [redacted] affecting the [redacted] application.	IT-AR-19-005	9/6/2019	None
Cybersecurity Decision Analysis Reports Review	Assess whether DAR I and DAR II cybersecurity investments' stated performance metrics aligned with the Corporate Information Security Office's strategic and cost objectives.	IT-AR-19-002	11/19/2018	None

Appendix B: Examples of Incident Management Metrics

Percentage of	■ Staff (managers, users) who have not completed training and awareness to identify anomalies and report them in the required timeframe (initial, refresher) ■ Events triaged (reported vs. analyzed) ■ Events stalled or awaiting activity beyond an established threshold ■ Events whose documentation does not meet rules, laws, regulations, policies, or other requirements for forensic purposes ■ Events without a disposition ■ Events open beyond an established threshold ■ Change in the number of logged events ■ Events that recur and result in declared incidents ■ Events (or sets of related events) declared as incidents ■ Events declared as incidents that do not match the current incident declaration criteria ■ Incidents declared but not closed ■ Incidents exploiting existing vulnerabilities with known solutions, patches, or workarounds ■ Operational downtime due to incidents ■ Incidents that recur ■ Change in the number of incidents by incident type ■ Incidents requiring escalation ■ Change in the elapsed time of the incident life cycle by incident type (mean, median, ranges) ■ Incidents requiring the involvement of law enforcement ■ Incidents requiring the involvement of regulatory and governing agencies ■ Post-incident review recommendations that result in control changes or improvements to the process
Number of	■ Incidents by type ■ Incidents by type and impact ■ Incidents by type and root cause
Mean, Median Time	■ To close an event ■ Between event detection and related incident declaration ■ Between event detection and related incident response ■ Between event detection and related incident closure

Source: CERT® Resilience Management Model, Version 1.2, Incident Management and Control.

Appendix C: Management's Comments

UNITED STATES POSTAL SERVICE

July 21, 2020

Lazerick C. Poland
Director, Audit Operations

SUBJECT: Audit Report – *Cybersecurity Incident Detection and Response Capability* (Project Number 19-012-DRAFT)

Management has reviewed the "*Cybersecurity Incident Detection and Response Capability*" draft audit report, authored by the Postal Service Office of Inspector General (OIG); this letter provides the OIG management's response relative to the individual findings.

However, before addressing those findings, management expresses its strong disagreement with the OIG's overall assessment concerning the efficacy of the Postal Service's incident detection and response capabilities.

Management appreciates the challenges the OIG faced when creating sufficient and relevant tests of the Postal Service's incident detection and response capabilities, given the COVID-19 constraints. Yet, management asserts the simulation methodology behind the condition reported was flawed by design, which impairs the findings. The OIG team exploited an over-emphasized internal path known and available to them, leveraging authenticated and physical network access not representative of the environment available to a true threat actor. The simulation used OIG-procured equipment; while comparable to USPS network-provisioned equipment, [redacted] Therefore, the simulated activities performed by OIG do not support the report's broad generalization that the Postal Service [redacted]

The Postal Service's layered approach to incident response and detection relies upon a combination of tools, processes, expert collaboration, and human intellect, which includes:

- Embedding cybersecurity professionals from industry-leading firms, including [redacted] within critical Corporate Information Security Office (CISO) security processes;

- Staffing real-time monitoring operations for the USPS infrastructure every hour of every day, each week, responding to more than [redacted] cases on average, in each of the past three fiscal years;
- Employing a scoring model for each case to assess and prioritize response efforts, consistent with Department of Homeland Security (DHS) criteria and developed in collaboration with industry-leading security cybersecurity firms including the Software Engineering Institute at Carnegie Mellon University;
- Collaborating with federal law enforcement intelligence sharing and investigation initiatives, involving the U.S. Postal Inspection Service, FBI, DHS, and the National Cyber Investigative Joint Task Force—which provides an alliance of more than 20 partnering agencies from across law enforcement, the intelligence community, and DHS;
- Aligning and coordinating with DHS initiatives, including the [redacted]
- Escalating vulnerabilities, events and incidents through a structured reporting cadence to Postal Service executive leadership, quantified and tracked consistently in terms of the level of risk, and business and stakeholder impacts;
- Leveraging and prioritizing response efforts involving classified intelligence;
- Training annually, in each of the past four years, alongside hundreds of cyber professionals from across the U.S. Defense Department, other federal agencies and partner nations in cyber warfare simulations to enhance readiness and to build partnerships among those who would be called upon during a real-world event to keep malicious actors out of critical cyber infrastructure;
- Benchmarking incident detection and response capabilities against an independently-developed cyber resilience framework, employed by large organizations responsible for critical infrastructure; and
- Evaluating incident detection and response capabilities, processes, and performance by independent cyber experts against the benchmarking framework.

The assertion that these investments, as a whole, amount to an [redacted] is an unsupportable generalization—especially given the narrow scope of the audit findings. . Based on the narrowly prescriptive audit recommendations, management disputes the sufficiency of the audit findings to establish cause, criteria, or effect that would conclude the Postal Service's incident detection and response capabilities were [redacted] described within the report.

Recommendation [1]:
We recommend the **Executive Vice President, Chief Information Office**, direct **Corporate Information Security Office, Information Technology, and Engineering,** to complete the [redacted] project implementation as identified in Cybersecurity DAR III and implement the necessary [redacted]

Management Response/Action Plan:
Management agrees with this recommendation, however, the simulation did not demonstrate a business consequence to USPS assets, failing to impact USPS sensitive data or critical systems.

The Postal Service is committed to completing [redacted] The investment was approved by the Postal Service's Investment Review Committee (IRC) in December 2017, and funded by corporate finance in May 2018. This project was initiated during the second half of FY18 and continues across one of the world's largest, most complex networks. DAR III's completion was initially planned for FY20; however, intervening circumstances including the complexity of the environment extended the DAR performance period through 2021. The Chief Information Office has planned completion of the phase one [redacted] efforts for Q4 FY21.

The implementation of [redacted] remain in progress, as they have since DAR III was approved. These activities are supported in their entirety by the Executive Vice President, Chief Information Officer, and progress is tracked and reported as required by USPS financial policy.

[redacted] is one strategy to help mitigate the potential harm from a threat actor. It lays the groundwork for controls that can protect against activity by malicious actors or software, and helps safeguard against potential infection or compromise. [redacted] is foundational to our asset management and visibility strategy. However, it is not a substitute for monitoring and detection capabilities, or access management processes, as implied by this finding.

Target Implementation Date:
September 30, 2021

Responsible Official:
Executive Vice President, Chief Information Officer

Recommendation [2]:
We recommend the **Manager, Cybersecurity Operations**, determine which incident detection and response metrics are meaningful to the organization and establish a process to measure the effectiveness of the incident detection and response capability.

Management Response/Action Plan:
Management disagrees with this finding. Upon receipt of the draft report, management engaged the Software Engineering Institute (SEI) at Carnegie Mellon University, developer of the CERT-RMM framework, which was referenced by the OIG in this finding. SEI comprehensively reviewed the metrics provided to the OIG audit team and

interviewed key process stakeholders. SEI disagreed with the basis of the OIG finding, stating, "After a close examination of the audit results, the expert concurs with the USPS, and believe the metrics provided for review sufficiently meet the OIG audit requirements. The metrics defined for both the Incident Response capability as well as for the Incident Management and Control (IMC) Process Plan support this position."

Management also asserts the finding mischaracterizes statements made concerning process maturity, from which the OIG concluded management hadn't yet determined the "most meaningful" metrics to the organization. Management's remarks reflect the need for constant evaluation and improvement in the process area—including metrics. The "meaningfulness" of the metrics, or their relevance, efficacy, and sufficiency, will continue to reflect the evolution of management's capabilities in anticipation and response to the threat landscape.

Management concurs with the SEI assessment, which is incorporated in its entirety as part of management's response to this finding (Appendix A; see attached "*Response to Finding #2_Cybersecurity Incident Detection and Response Capability audit*").

Responsible Official:
Vice President, Chief Information Security Officer

Recommendation [3]:
We recommend the **Deputy, Corporate Information Security Office**, track one-to-one alignment of actual investments with Cybersecurity Decision Analysis Report III Enhancement and Maturity requests for each project.

Management Response/Action Plan:
Management disagrees with the recommendation. The capabilities described in DAR III were presented at a level of detail necessary to distill complex cybersecurity initiatives into discernable capabilities, in the context of a business case justification and in the interest of transparency. These capabilities were not intended to be tracked as individual "projects".

CISO complies with USPS' financial tracking and reporting requirements, supported by USPS standard accounting systems. Cybersecurity DAR III was assigned a single finance number by USPS Corporate Finance, to facilitate management's investment tracking and compliance reporting. The budget was maintained at the DAR level, which is the "project" level. In FY20, Corporate Finance provided additional finance numbers for DAR III, to track the budget at the business portfolio level, however, this does not extend to the capability level. CISO submits quarterly compliance reports, addressing performance relative to the project's cost, benefits, schedule, and risk, as well as other DAR-specified metrics. Reporting is accomplished via USPS' [redacted] These standardized corporate systems and processes hold

management accountable to ensure project expenditures are tracked, budgets are not overspent, and ensure projects are executed timely.

Responsible Official:
Vice President, Chief Information Security Officer

Recommendation [4]:
We recommend the **Manager, Cybersecurity Operations Center,** develop procedures for the safe handling of Cybersecurity Incident Response Ticket [redacted] or develop a risk acceptance letter.

Management Response/Action Plan:
Management agrees with this recommendation. On June 26, 2020, the CyberSecurity Operations (CSOC) team had updated and published its Standard Operating Procedure (SOP) titled: [redacted] *Cybersecurity Incident Response Ticket SOP.pdf*". Safe handling of [redacted] including encrypted zip files was included, and resources were fully trained by close of business (COB) July 12, 2020.

Target Implementation Date:
July 21, 2020

Responsible Official:
Vice President, Chief Information Security Officer

Recommendation [5]:
We recommend the **Manager, Cybersecurity Operations Center,** create a notification within the Cybersecurity Operations Center module in [redacted] notifying users of potential Cybersecurity Incident Response Ticket [redacted]

Management Response/Action Plan:
Management agrees with this recommendation. CSOC has confirmed CISO funding will be provided to support an update of the CSOC [redacted] banner. CSOC has worked with Information Technology to develop the banner with expectation this change will be in Customer Acceptance Testing (CAT) on July 16, 2020 and deployed to production July 23, 2020.

Target Implementation Date:
July 23, 2020

Responsible Official:
Vice President, Chief Information Security Officer

Recommendation [6]:
We recommend the **Manager, Cybersecurity Operations Center,** develop a process to regularly review, verify status, and ensure timely closure of unresolved tickets transferred to another office for resolution.

Management Response/Action Plan:
Management agrees with this recommendation. CSOC has communicated with multiple stakeholders and partially implemented processes and procedures for transfer of cases. Refinements to the processes and procedures were completed by July 21, 2020.

Target Implementation Date:
July 21, 2020

Responsible Official:
Vice President, Chief Information Security Officer

E-SIGNED by Kristin.A Seaver
on 2020-07-21 17:21:23 CDT

Kristin Seaver
Chief Information Officer and Executive Vice President

Gregory Crabb

Digitally signed by Gregory Crabb
DN: cn=Gregory Crabb, o=US Postal Service, ou=Corporate Information Security Office, email=GSCrabb@uspis.gov, c=US
Date: 2020.07.21 13:06:31 -04'00'

Gregory S. Crabb
Vice President, Chief Information Security Officer

E-SIGNED by Pritha Mehra
on 2020-07-21 14:44:37 CDT

Pritha Mehra
Vice President, Information Technology

E-SIGNED by SCOTT.R.BOMBAUGH
on 2020-07-21 16:13:21 CDT

Scott R. Bombaugh
Vice President, Engineering Systems

cc: *copy those that were copied on the OIG draft audit report, plus*
Manager, Corporate Audit Response 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, contact Agapi Doulaveris
Telephone: 703-248-2286
adoulaveris@uspsoig.gov