OFFICE OF INSPECTOR GENERAL | UNITED STATES POSTAL SERVICE

After-Action Review of Unauthorized Access to USPS Employee Self-Service Portal

AUDIT REPORT

Report Number 23-134-R24 | June 6, 2024

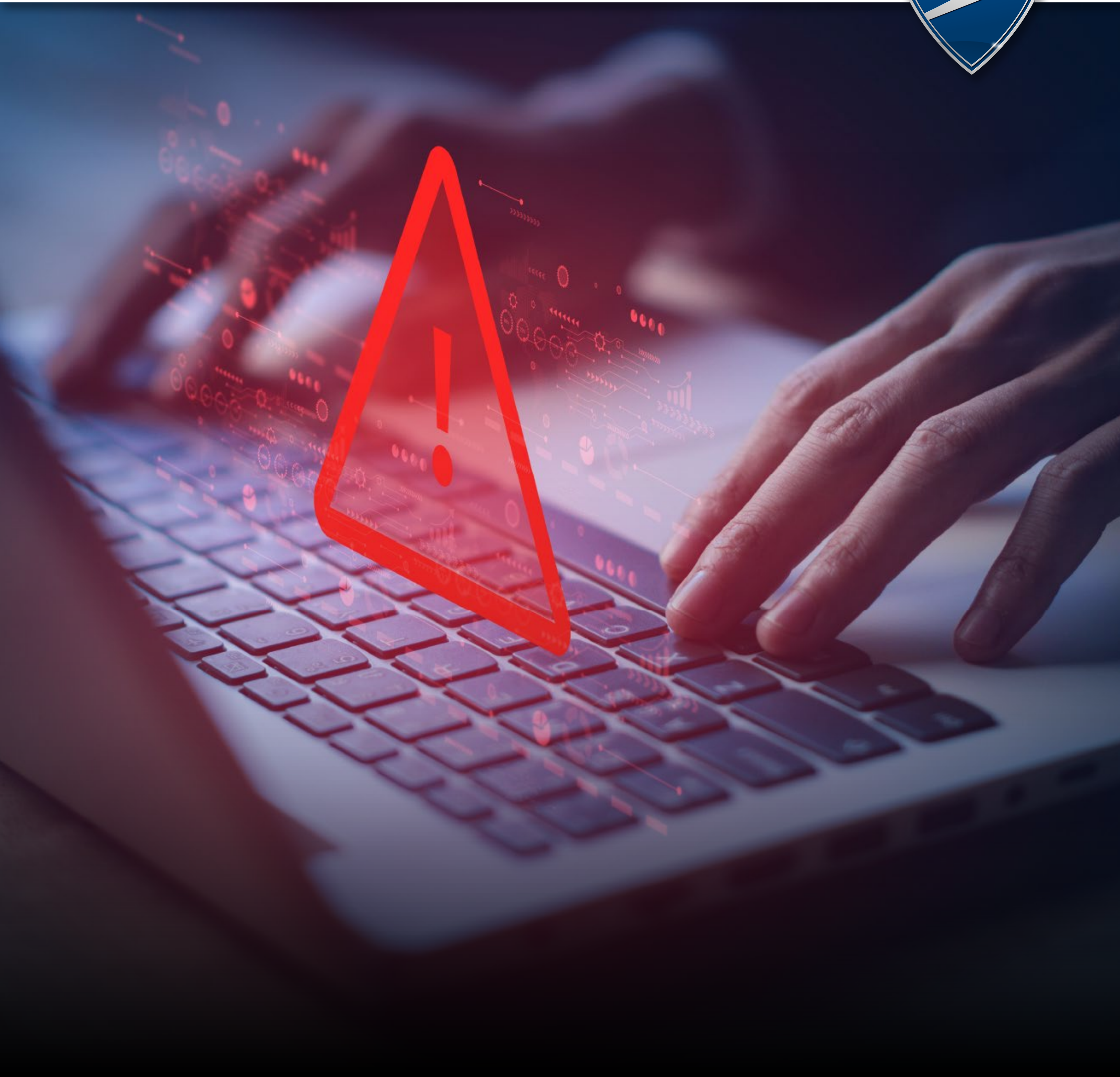


Table of Contents

Highlights

Background

The U.S. Postal Service is the second largest employer in the United States with 640,092 employees and $2.15 billion in bi-weekly salaries. To provide employees with convenient access to their payroll, benefits, and personnel data, the Postal Service uses the LiteBlue portal. This web-based portal contains several human resources (HR) applications, including PostalEASE, which allows employees to establish direct deposits, create or modify payroll allotments, and update retirement and health benefits information. In October 2022, some employees entered their login credentials into several fake LiteBlue websites, allowing bad actors to obtain their login credentials and fraudulently reroute employees' payroll direct deposits and create payroll allotments to bank accounts they controlled. As a result of this attack, [redacted] lost a collective total of at least [redacted].

What We Did

Our objective was to determine if the Chief Information Security Office (CISO) appropriately responded to and mitigated fraudulent access to the PostalEASE application. We also assessed the extent to which CISO could have prevented or mitigated this fraudulent access. For this audit, we reviewed CISO's response to the attack, evaluated cyber incident and event policies and procedures, and analyzed employee and payroll data.

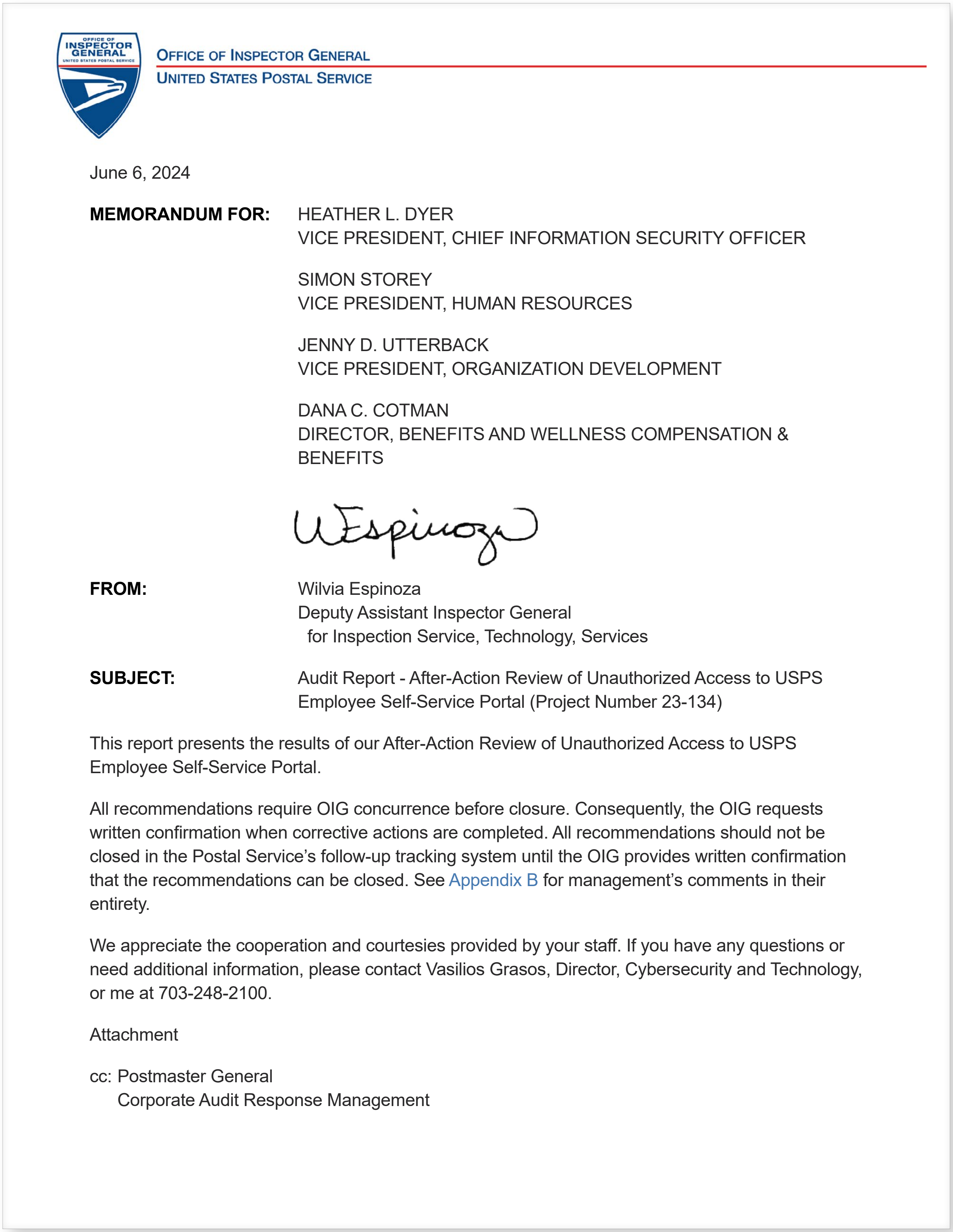
What We Found

CISO did not take all critical steps necessary to prevent fraudulent access to the PostalEASE application, such as implementing multifactor authentication (MFA) or providing security awareness training to all employees. These issues occurred because CISO prioritized securing the broader Postal Service network and did not make security awareness training mandatory. Additionally, CISO did not escalate the 2022 phishing attack from an "event" to an "incident," despite unauthorized system access, unlawful activity, and indication the attackers used employees' credentials to access multiple HR applications. CISO also did not notify employees to [redacted].

Recommendations and Managements Comments

We made six recommendations to address issues related to fraudulent account access, incident escalation, residual risk to MFA, and [redacted] [redacted] Postal Service management agreed with four recommendations and disagreed with two. Management's comments and our evaluation are at the end of each finding and recommendation. The U.S. Postal Service Office of Inspector (OIG) considers management's comments responsive to recommendations 1,3,4, and 6 and corrective actions should resolve the issues identified in the report. See Appendix C for management's comments in their entirety.

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

June 6, 2024

MEMORANDUM FOR: HEATHER L. DYER
VICE PRESIDENT, CHIEF INFORMATION SECURITY OFFICER

SIMON STOREY
VICE PRESIDENT, HUMAN RESOURCES

JENNY D. UTTERBACK
VICE PRESIDENT, ORGANIZATION DEVELOPMENT

DANA C. COTMAN
DIRECTOR, BENEFITS AND WELLNESS COMPENSATION & BENEFITS

WEspinoza

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

SUBJECT: Audit Report - After-Action Review of Unauthorized Access to USPS Employee Self-Service Portal (Project Number 23-134)

This report presents the results of our After-Action Review of Unauthorized Access to USPS Employee Self-Service Portal.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. All 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. See Appendix B for management's comments in their entirety.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Vasilios Grasos, Director, Cybersecurity and 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 After-Action Review of Unauthorized Access to USPS Employee Self-Service Portal (Project Number 23-134). Our objective was to determine if the U.S. Postal Service appropriately responded to and mitigated fraudulent access to the PostalEASE application. We also assessed the extent to which the Postal Service could have prevented or mitigated this fraudulent access. See Appendix A for additional information about this audit.

Background

Postal Service Human Resources Applications

The Postal Service is the second largest civilian employer in the United States, with a total of 640,092 employees earning over $2.15 billion in salaries bi-weekly.[1] A major portion of their workforce consists of craft employees — city and rural carriers, clerks, mail handlers, maintenance personnel, and motor vehicle operators — who do not routinely have access to the Postal Service network. The Postal Service uses LiteBlue, a web-based portal, to provide its employees with convenient access to their personnel data through [redacted] human resources (HR) applications. These applications include, but are not limited to:

- PostalEASE - allows employees to establish payroll direct deposits, create or modify pay allotments,[2] and update tax and health benefits information. This application also allows employees to transfer net pay to financial institutions of their choice, also known as "net to bank" changes.
- Electronic Official Personnel Folder (eOPF) - the official digitized record of a federal employee's employment records that includes personally identifiable information (PII) such as social security numbers, dates of birth, and current addresses.
- Self-Service Profile - allows employees to manage their passwords to other postal applications and personal identification numbers[3] for HR applications, such as PostalEASE.

> "Phishing attacks increased by 48 percent nationwide in the first half of 2022, with reports of 11,395 incidents costing businesses a total of $12.3 million."

In addition to these, there are several other HR applications that are accessible from the LiteBlue portal that allow employees to apply for jobs or plan for retirement.

Roles and Responsibilities

Several functional areas within the Postal Service work together to support and protect employees, applications, and data to support its mission. HR provides employees access to applications and information to meet their HR needs from benefits to retirement. The U.S. Postal Inspection Service's (USPIS's) cybercrime unit provides investigative, forensic, and analytical support to identify and prosecute individuals and organizations that use Postal Service's online tools to facilitate illegal activities.

The U.S. Postal Service Office of Inspector General's (OIG's) Computer Crimes Unit, similar to the USPIS cybercrimes unit, provides expert digital forensic support to the OIG's Office of Investigations. They conduct cyber investigations affecting the USPS network infrastructure, whether perpetrated by internal or external entities.

The Postal Service's Corporate Information Security Office (CISO) monitors its cyber environment to identify threats; provides cybersecurity awareness training, information, and resources to employees; and develops event management and incident

[1] Employee Master File from Mainframe, Pay Period 2, January 12, 2024.
[2] A recurring specified deduction from pay authorized by an employee to be disbursed on a pay period basis to an allottee.
[3] Memorized numerical passwords that are typically kept secret and are used to authenticate an individual's identity.

response plans that outline how they will contain, remediate, and mitigate events and incidents. Additionally, the CISO, Deputy CISO, and the Director of Cybersecurity Operations share responsibility for assessing a cybersecurity event to determine if it should be escalated to an incident.

Cybersecurity Attacks on PostalEASE

PostalEASE is a business-critical application containing sensitive PII that, prior to September 2021, was accessible as a standalone application for all employees.

On September 20, 2021, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA)[4] informed CISO of suspicious [redacted] According to the CISA, these [redacted] were also involved in compromises to other federal agencies' networks. CISO traced the activity and identified [redacted] A joint investigation by CISO and the OIG found that these [redacted] In response to this incident, CISO removed [redacted] However, CISO continued to allow [redacted]

More than a year after the first attack, between October 12 and October 19, 2022, employees submitted complaints to CISO, USPIS, and the OIG regarding missing payroll deposits. On October 19, 2022, the USPIS became aware of multiple fraudulent allotments and net to bank changes, which they learned resulted from a phishing attack[7] during which employees accessed multiple fake LiteBlue websites that closely resembled the LiteBlue portal and entered their login credentials.[8] On October 12, 2022, CISO, USPIS, and the OIG's Computer Crimes Unit began a joint investigation into bad actors capturing employee login credentials and gaining unauthorized access to PostalEASE. The bad actors used these credentials to fraudulently reroute employees' bi-weekly wages to different bank accounts they controlled. In addition, these actors created allotments that transferred portions of employees' wages to unknown bank accounts. As a result, [redacted] lost a collective total of at least [redacted]

According to the Cyber Incident Reporting for Critical Infrastructure Act of 2022, federal organizations are required to report cyber incidents to CISA within 72 hours from the time the organization believes the incident occurred. However, no federal laws bind the Postal Service to any reporting or notification requirements.

Incident Response Plan

Cybersecurity-related attacks have increased and become more diverse, damaging, and disruptive, with certain types emerging more frequently. For example, phishing attacks increased by 48 percent nationwide in the first half of 2022, with reports of 11,395 incidents costing businesses a total of $12.3 million.[9] As these attacks increase, it is critical for organizations to rapidly detect incidents, minimize loss, mitigate the weaknesses exploited, and restore information technology services. These actions should be included in an incident response plan.

The National Institute of Standards and Technology (NIST)[10] states that an incident response plan defines the procedures for prioritizing and handling cybersecurity attacks, which are classified as either events or incidents; implementing effective methods to collect, analyze, and report data; and establishing

[4] This organization coordinates and collaborates across government agencies, conducts vulnerability assessments to help critical infrastructure owners, and provides information on emerging threats so that appropriate actions can be taken to protect government networks.

[5] [redacted]

[6] [redacted]

[7] A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person.

[8] Login credentials include an employee's username and password.

[9] *CompTIA Top 50 Cybersecurity Statistics, Figures, and Facts.* January 27, 2023, Top 50 Cyber Security Statistics and Facts | CompTIA.

[10] NIST developed a Cybersecurity Framework that is widely considered the gold standard for building cybersecurity programs and is a scalable and customizable approach that can work in organizations of any size across various industries.

Examples *of* Multifactor Authentication

Things you know
A password and the answers to security questions.

Things you have
An identification badge with an embedded chip or a digital code generator.

Things you are
Biometric elements, such as fingerprints or voice.

communication with internal and external groups (e.g., HR and law enforcement).[11]

The CISO's Cybersecurity Incident Response Plan describes how to respond to information-security incidents and high-level events impacting the Postal Service's network. At a high level, it lists roles and responsibilities, methodology for discovery and remediation, and the process to manage events and incidents.

The plan defines an "event" as one or more occurrences, possibly minor, which affect organizational assets and has the potential to disrupt operations.[12] Examples of events include system crashes, unauthorized use of system privileges, or execution of malware that destroys data.[13] The plan defines an "incident" as a violation or imminent threat to an organization's security policies and procedures. Different types of incidents include attempts to gain unauthorized access to applications or modifying users' information without their knowledge, instruction, or consent.[14]

Security Controls

As security breaches, stolen data, and identity theft become more prevalent, applications such as PostalEASE require additional layers of security to protect employees' PII. An example of these security controls includes multifactor authentication (MFA), which requires a user to present a combination of two or more credentials for verification and authentication. Example credentials include:

- **Things you know** – a password and the answers to security questions.
- **Things you have** – an identification badge with an embedded chip or a digital code generator.
- **Things you are** – biometric elements, such as fingerprints or voice.

MFA increases access security because even if one credential is compromised, unauthorized users will need to know the second authentication requirement. While implementing MFA will not prevent every cybersecurity attack, it makes it more difficult for hackers to gain unauthorized access to user accounts.[15]

Findings Summary

Although CISO took action to contain damages to known employees affected by the 2022 phishing attack, we identified opportunities for improvement in their response. Specifically, CISO did not implement security controls timely to prevent unauthorized access to employees' PII, prioritize and escalate the 2022 phishing attack according to their internal policy and industry standards, and mitigate all threats and vulnerabilities that posed a security risk to the PostalEASE application.

[11] NIST Special Publication (SP) 800-61R2, *Computer Security Incident Handling Guide, Executive Summary*, August 2012.
[12] USPS CISO Cybersecurity Incident Response Plan, Version 5.2, Section 2 Key Terms and Definitions, February 23, 2023.
[13] NIST SP 800-61R2, *Computer Security Incident Handling Guide*, Section 2.1 Events and Incidents, August 2012.
[14] USPS CISO Cybersecurity Incident Response Plan, Version 5.2, Section 2 Key Terms and Definitions, February 23, 2023.
[15] National Institute for Standards and Technology (NIST), Multifactor Authentication, updated March 12, 2024, Back to basics: Multi-factor authentication (MFA) | NIST.

Finding #1: Preventing Fraudulent Access

In response to the initial 2021 cybersecurity incident, CISO coordinated with [redacted] However, we found that these actions were not sufficient to prevent bad actors from gaining unauthorized access to accounts or data and protect Postal Service employees.

Additionally, we found that employees that did not have [redacted] were ill-prepared to protect themselves from identifying spoofed[16] or fraudulent websites. According to CISO, 469,963 of the Postal Service's 640,092 employees (73.4 percent) did not have [redacted] because access was limited to the [redacted]

The NIST states that organizations must exercise due diligence in managing information security and privacy risk by establishing safeguards or countermeasures in a system to protect the confidentiality, integrity, and availability of the system and its information. These safeguards or controls include identification and authentication of users. In addition, the CISA states that organizations must prepare for major incidents before they occur to mitigate any impacts. This can include documenting and understanding policies and educating users on cyber threats and notification procedures.

Unauthorized access to PostalEASE occurred because CISO did not implement MFA timely and the Postal Service's craft employees were not required to take security awareness training. Specifically, while CISO had the ability to implement MFA, it did not. According to the 2021 PostalEASE cybersecurity attack after-action report (dated January 26, 2022), CISO cited the lack of MFA as one of the root causes of the attack. CISO stated that it did not prioritize MFA for HR applications because their priority and focus was on securing the broader Postal Service network, to include identity and access management initiatives. As such, CISO did not implement MFA for PostalEASE until January 18, 2023, and did not fully implement MFA for the other [redacted] Postal HR applications until May 2023. However, CISO has a plan to implement MFA for [redacted] USPS applications with sensitive or business critical information by [redacted].

Further, employees were ill-prepared because only those employees [redacted] were required to take mandatory security awareness training, so those [redacted] (about 73 percent of Postal Service employees) were not afforded opportunities to learn how to protect themselves from cyber threats. In response to the second PostalEASE event, CISO provided four memos to Corporate Communications to reinforce cyber safety practices and MFA requirements. This information was disseminated to employees during four separate stand-up talks[17] between December 23, 2022, and April 21, 2023. These stand-up talks were designated as mandatory by CISO and intended to communicate the fraudulent sites that employees must avoid. However, only the employees who were present at the facilities during these talks received the message.

Applications available via the internet are at increased risk of a cyberattack, especially those that contain high-value information such as personnel and payroll information. The likelihood of a successful cyberattack further increases when needed security controls are not implemented. Because CISO did not properly secure PostalEASE with MFA before the 2022 phishing attack, [redacted] in wages, with only [redacted] recovered to date. As such, we consider the [redacted] to be questioned cost.[18]

[16] Faking the sending address of a transmission to gain illegal entry into a secure system.
[17] The organization's main communication method to inform employees on a wide range of issues. These talks are held in person at local facilities.
[18] A cost the OIG believes is unnecessary, unreasonable, or an alleged violation of law, regulation, or contract.

Recommendation #1

We recommend the **Vice President, Chief Information Security Officer**, continue to complete the implementation of multi-factor authentication for applications that hold sensitive or business critical information.

Recommendation #2

We recommend the **Vice President, Organization Development**, and **Vice President, Human Resources**, in coordination with the **Vice President, Chief Information Security Officer**, provide mandatory annual security awareness training to craft employees and maintain documentation that these employees completed the training.

Postal Service Response

The Postal Service disagreed with the finding and stated the cited steps would not have prevented the incident from occurring. Management further stated they provided evidence on several occasions that showed, despite having taken training, employees still fell victim.

Management agreed with recommendation 1 and provided a target implementation date of [redacted]. Management disagreed with recommendation 2 and stated the OIG did not sufficiently provide evidence to support a guarantee that training would be a solution that would mitigate the issue. Additionally, management stated the cost to develop and conduct mandatory training to craft employees would be significantly high for an endeavor that has no clear benefit.

Subsequent to their comments, management disagreed with the monetary impact and stated they recognized there were some employees who lost funds, however, the OIG overstated the scope as they failed to factor in the amount net of what the Postal Service was able to recover.

OIG Evaluation

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

Regarding management's disagreement with the finding and recommendation 2, there is no control that can guarantee all future phishing attacks will be prevented. However, providing all employees with security awareness training could reduce the number of potential future victims of phishing attacks. Although management provided training documentation for employees who fell victim, it demonstrated that [redacted] of the [redacted] took the security awareness training in FY 2023, but the dcocumentation did not include completion dates. We view the disagreement with recommendation 2 as unresolved and will work with management through the formal audit resolution process.

Regarding the monetary impact, OIG reported the total amount of employee wages lost as a result of not implementing MFA timely to prevent the attack.

Finding #2: Response to the PostalEASE Attack

Once notified in October 2022 of the phishing attack, CISO took immediate action to assist impacted employees, to include working with employees to reset passwords, implementing [redacted] and preventing employee access to eOPF and Interactive Voice Response (IVR)[20] indefinitely. Further, they conducted a joint investigation with the OIG and USPIS and recovered [redacted] in stolen funds on behalf of employees as of January 2024. See Appendix C for the investigation, mitigation, and communication efforts taken by the Postal Service in response to this attack.

However, CISO did not escalate this attack from an event to an incident, remediate a residual threat to MFA, or verify [redacted]

Incident Escalation

CISO misclassified the attack as an event. According to their incident declaration criteria, the actions taken by the bad actors met CISO's definition of an incident. Specifically, CISO confirmed unauthorized system access, unlawful activity, and lateral movement,[21] to include:

[redacted]

[redacted]

[redacted]

According to CISO's policy, a cybersecurity incident includes unauthorized access to an information system or unlawful activity. Also, this policy states that a cybersecurity event must be escalated to an incident if there is indication of lateral movement. In addition, CISA states that industries should follow an incident response playbook,[24] especially when malicious cyber activity occurs, including evidence of lateral movement or credential access.

CISO classified this phishing attack as an event instead of an incident because:

- The criteria CISO used for classifying an incident did not align with their policy. Specifically, the criteria were limited to assessing only four actions,[25] none of which included an assessment of whether there was unauthorized access to an information system or unlawful activity.
- Their incident response policies contained a limited definition of lateral movement; therefore, they did not [redacted] Specifically, CISO stated this did not constitute lateral movement because the bad actors [redacted]
- Their event management plan was outdated. While their policy states the plan should be updated yearly, the December 2023 version was unchanged from the original version released in May 2020. It is unclear if a valid event management plan exists.

By not classifying this attack as an incident, CISO was not required to complete all incident response steps, and thus, did not complete steps to prevent incidents, eradicate and mitigate vulnerabilities, recover

[19] [redacted]
[20] IVR is a phone system that prompts callers through a step-by-step question and response process that enables employees to access benefits, payroll, and retirement information, verify employment, and reset personal identification numbers.
[21] A technique adversaries use to enter and control systems by taking advantage of misconfigurations, vulnerabilities, or other weaknesses.
[22] [redacted]
[23] [redacted]
[24] *Cybersecurity and Infrastructure Security Agency, Federal Government Cybersecurity Incident & Vulnerability Response Playbooks*, dated November 2021.
[25] The four actions include the presence of advanced, persistent threat or active techniques, tactics, and procedures; indication of lateral movement; external notification from a trusted source; or successful exploitation of a Postal Service Officer.

systems to an operationally ready state, or conduct post incident reporting or lessons learned activities. See Table 1 for CISO's incident lifecycle steps and what they did and did not complete.

Table 1. Analysis of CISO's Response to 2022 Phishing Attack

CISO Incident Lifecycle Steps	Steps Completed by CISO
Alert and Scope	✓
Investigate	✓
Contain	✓
Eradicate and Mitigate	X
Recover	X
Report	X
Lessons Learned	X

Source: OIG analysis of CISO's Incident Response Plan dated February 2023. ✓ indicates CISO completed this step. X indicates CISO did not complete this step.

If CISO had completed these steps during their response and investigation from October 2022 to January 2023, they could have identified and mitigated vulnerabilities in their system and security controls sooner, such as the ability to [redacted] (discussed below). Additionally, [redacted]

In addition, while not legally required to report incidents, by not classifying this attack as an incident, they missed an opportunity to report it to CISA, which would have allowed the Postal Service to receive assistance, analyze activity to identify trends, and share this information with other federal agencies.

Finally, they missed an opportunity to conduct post incident reporting, such as an after-action report or lessons learned activity. If CISO had completed these activities, they could have better leveraged the lessons learned from this attack to prevent or mitigate future cybersecurity incidents.

Residual Risk to MFA

Prior to MFA being implemented, the bad actors changed some employees' personal identification numbers unbeknownst to the employees. [redacted]

These issues occurred because CISO did not identify vulnerabilities in their system and security controls prior to implementing MFA, which resulted in bad actors circumventing security controls.

According to Postal Service policy,[26] the incident response team is required to locate, neutralize, and remove artifacts of the cybersecurity event or incident to prevent future compromise. Additionally, industry best practices[27] recommend that organizations continue with detection and analysis activities to monitor for any signs of adversary re-entry or use of new access methods.

Without identifying vulnerabilities prior to implementing security controls, management cannot fully eradicate or mitigate vulnerabilities. Specifically, they may miss opportunities to identify and plan for residual risks, vulnerabilities, and unexpected events. In addition, without taking proactive steps to secure applications, these systems and employees are at continuous risk of being targeted.

To remediate the residual risk to MFA, CISO [redacted] Because of these actions, we will not be making a recommendation related to eradicating vulnerabilities.

[26] USPS CISO Cybersecurity Incident Response Plan, Version 5.2, February 23, 2023.

[27] *Cybersecurity and Infrastructure Security Agency, Federal Government Cybersecurity Incident & Vulnerability Response Playbooks*, dated November 2021.

[redacted]

CISO and Postal Service management did not ensure that all [redacted] resulting from this attack were removed. In October 2022, CISO became aware of the compromise to [redacted] During USPIS's investigation in October 2022, they [redacted] that were created before MFA was in place but had not been [redacted] This activity could result in [redacted]. For example, if a [redacted] This action would only be processed once the [redacted] Due to this risk, it is important for the Postal Service to identify other possible [redacted]

We analyzed [redacted] Based on this analysis, [redacted]

According to CISO policy,[28] incident response teams and resources must eradicate and mitigate remaining artifacts of the cybersecurity attack to prevent similar incidents moving forward. Additionally, industry best practices[29] state that after an incident is contained, eradication is necessary to eliminate components of the incident, including mitigating all vulnerabilities that were exploited.

Although CISO worked with other components, including Human Resources and payroll teams, to identify additional employees impacted by this event, CISO did not proactively inform all [redacted] Specifically, these issues occurred because CISO did not [redacted]

[redacted]

Without fully mitigating all vulnerabilities, there is an increased risk that [redacted] Additionally, a majority, if not all, of an [redacted]

Recommendation #3

We recommend the **Vice President, Chief Information Security Officer**, update incident response escalation criteria to align with the Postal Service's definition of an incident.

Recommendation #4

We recommend the **Vice President, Chief Information Security Officer**, update the definition of lateral movement to align with industry standards.

[28] USPS CISO Cybersecurity Incident Response Plan, Version 5.2, February 23, 2023.

[29] National Institute of Standards and Technology, Special Publication 800-61r2 and *Cybersecurity and Infrastructure Security Agency, Federal Government Cybersecurity Incident and Vulnerability Response Playbooks*, dated November 2021.

Recommendation #5

We recommend the **Vice President, Chief Information Security Officer**, update the event management plan to align with the incident response plan and develop a process to review annually.

Recommendation #6

We recommend the **Director, Benefits and Wellness Compensation & Benefits**, in coordination with the **Vice President, Chief Information Security Officer**, notify all [redacted]

Postal Service Response

The Postal Service stated they disagreed with the finding because there was no lateral movement. Specifically, management stated the activity in the PostalEase/LiteBlue attempt was a fraudulent actor harvesting credentials and then logging into the system with those credentials. Management also stated there was no attempt by the fraudster to access additional USPS information resources or traverse the USPS network.

Management agreed with recommendations 3, 4, and 6 and provided a target implementation date of June 15, 2024, for recommendations 3 and 4 and June 30, 2024, for recommendation 6. Management disagreed with recommendation 5 and stated the event management plan is no longer in practice and has been replaced with the incident management process.

OIG Evaluation

Regarding management's disagreement with the finding, management stated prior to the phishing attack, each application within LiteBlue required a separate login, which means the attackers had to traverse and authenticate to each system that was compromised. As such, moving between these applications is lateral movement.

Management's comments were responsive to recommendations 3, 4, and 6 and corrective actions should resolve the issues identified in the report. Regarding management's disagreement with recommendation 5, management provided a copy of their new incident response plan in May 2024. While the plan states that it would be reviewed bi-annually, the plan does not clearly explain how events and incidents should be determined, which may impact how the Postal Service responds to future cyber attacks. We view the disagreement with recommendation 5 as unresolved and will work with management through the formal audit resolution process.

Appendices

Appendix A: Additional Information

Scope and Methodology

Our audit scope consisted of an after-action review of the Postal Service's response to the 2022 PostalEASE phishing attack from October 2022 to July 2023. Specifically, we reviewed the Postal Service's actions to respond to, mitigate, and prevent the fraudulent access to PostalEASE.

To accomplish our objective, we:

- Reviewed CISO's timeline of responses to the fraudulent access to determine timeliness of notification to affected employees.
- Evaluated internal policies for event and incident response to understand how CISO classified and responded to the 2022 phishing attack.
- Assessed CISO's preventive measures, including monitoring tools and the timely implementation of MFA, to determine if this event could have been prevented or appropriately mitigated.
- Determined if CISO discovered and eradicated vulnerabilities in the PostalEASE application, [redacted] to ensure CISO fully secured LiteBlue to protect its employees from further monetary loss and exposure of PII.
- Analyzed [redacted] including identifying high-risk [redacted] of the phishing attack.

We conducted this performance audit from August 2023 through June 2024 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We discussed our observations and conclusions with management on May 1, 2024, and included their comments where appropriate.

In planning and conducting the audit, we obtained an understanding of the PostalEASE internal control structure to help determine the nature, timing, and extent of our audit procedures. We reviewed the management controls for overseeing the program and mitigating associated risks. Additionally, we assessed the internal control components and underlying principles, and we determined that the following three components were significant to our audit objective:

- Risk assessment.
- Control activities.
- Information and communication.

We developed audit work to ensure that we assessed these controls. Based on the work performed, we identified internal control deficiencies related to control activities, risk assessment, and information and communication that were significant within the context of our objectives. Our recommendations, if implemented, should correct the weaknesses we identified.

We assessed the reliability of the letters of indemnity and employee master file data by performing tests to confirm the completeness, reasonableness, accuracy, and validity of the data. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

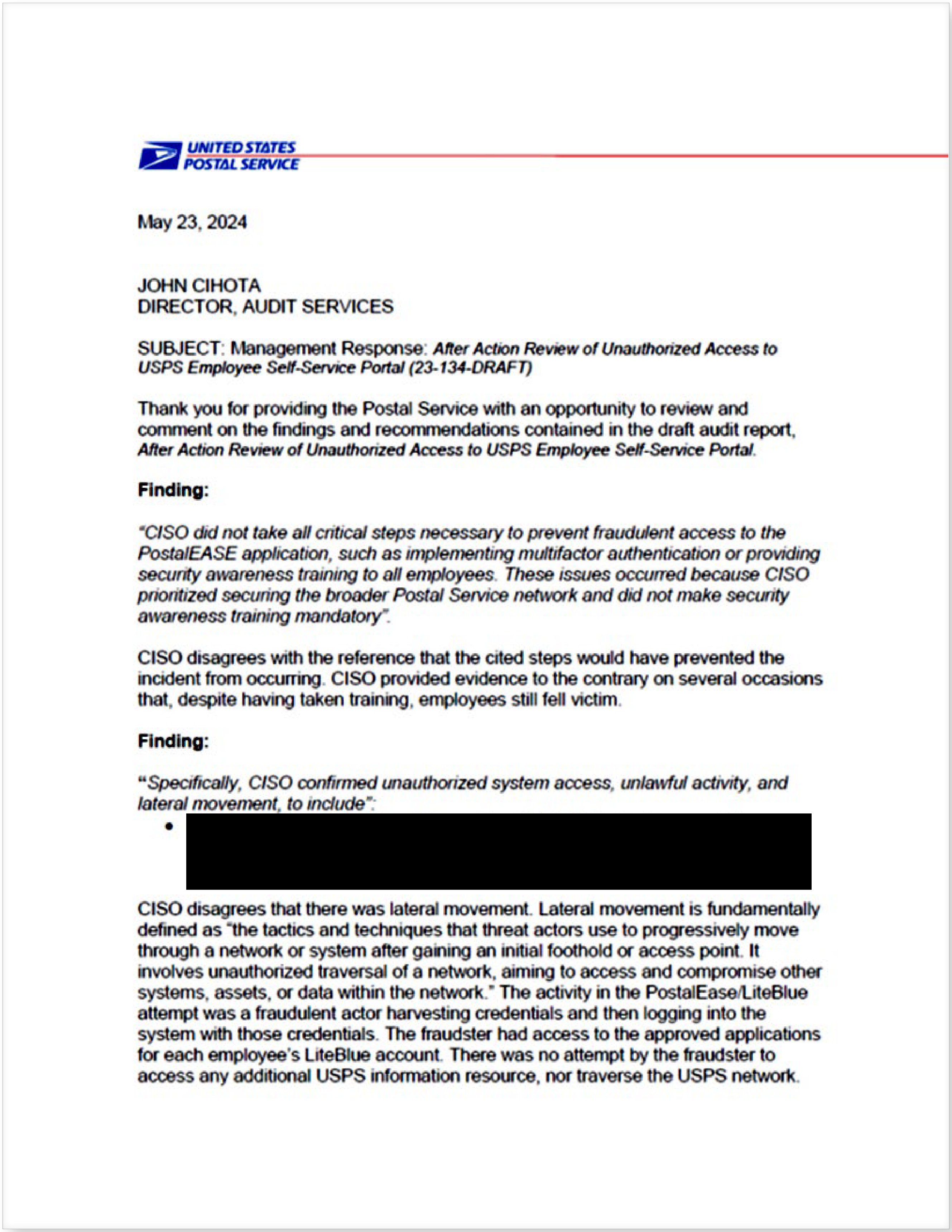
Report Title	Objective	Report Number	Final Report Date	Monetary Impact
Postal Service's Response [redacted]	[redacted]	IT-AR-19-005	09-06-2019	N/A

Appendix B: Postal Service's Investigation, Mitigation, and Communication Efforts

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

USPS Investigation, Mitigation, and Communications Timeline.

Appendix C: Management's Comments



UNITED STATES POSTAL SERVICE

May 23, 2024

JOHN CIHOTA
DIRECTOR, AUDIT SERVICES

SUBJECT: Management Response: *After Action Review of Unauthorized Access to USPS Employee Self-Service Portal (23-134-DRAFT)*

Thank you for providing the Postal Service with an opportunity to review and comment on the findings and recommendations contained in the draft audit report, *After Action Review of Unauthorized Access to USPS Employee Self-Service Portal.*

Finding:

"CISO did not take all critical steps necessary to prevent fraudulent access to the PostalEASE application, such as implementing multifactor authentication or providing security awareness training to all employees. These issues occurred because CISO prioritized securing the broader Postal Service network and did not make security awareness training mandatory".

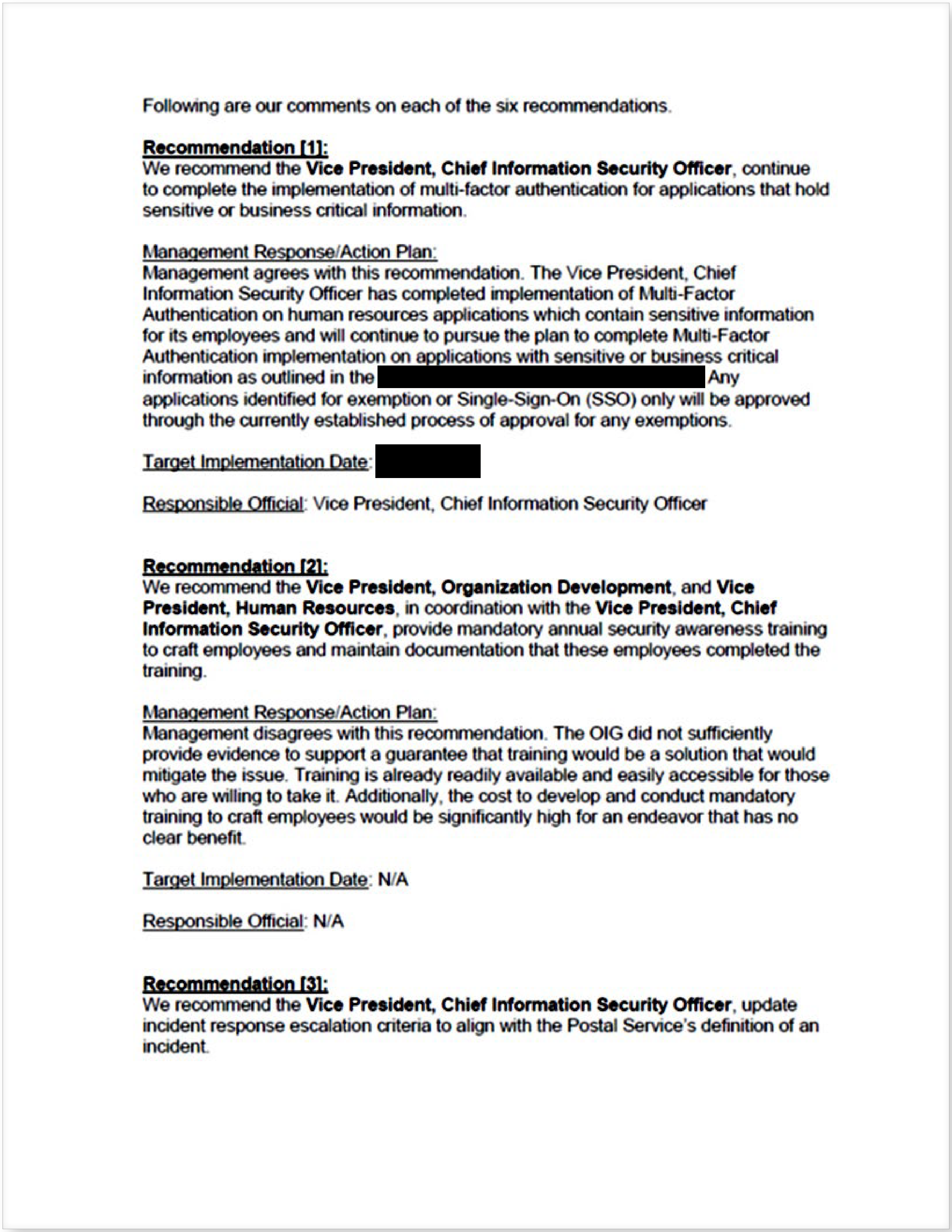
CISO disagrees with the reference that the cited steps would have prevented the incident from occurring. CISO provided evidence to the contrary on several occasions that, despite having taken training, employees still fell victim.

Finding:

"Specifically, CISO confirmed unauthorized system access, unlawful activity, and lateral movement, to include":

- [redacted]

CISO disagrees that there was lateral movement. Lateral movement is fundamentally defined as "the tactics and techniques that threat actors use to progressively move through a network or system after gaining an initial foothold or access point. It involves unauthorized traversal of a network, aiming to access and compromise other systems, assets, or data within the network." The activity in the PostalEase/LiteBlue attempt was a fraudulent actor harvesting credentials and then logging into the system with those credentials. The fraudster had access to the approved applications for each employee's LiteBlue account. There was no attempt by the fraudster to access any additional USPS information resource, nor traverse the USPS network.



Following are our comments on each of the six recommendations.

Recommendation [1]:
We recommend the **Vice President, Chief Information Security Officer**, continue to complete the implementation of multi-factor authentication for applications that hold sensitive or business critical information.

Management Response/Action Plan:
Management agrees with this recommendation. The Vice President, Chief Information Security Officer has completed implementation of Multi-Factor Authentication on human resources applications which contain sensitive information for its employees and will continue to pursue the plan to complete Multi-Factor Authentication implementation on applications with sensitive or business critical information as outlined in the [redacted] Any applications identified for exemption or Single-Sign-On (SSO) only will be approved through the currently established process of approval for any exemptions.

Target Implementation Date: [redacted]

Responsible Official: Vice President, Chief Information Security Officer

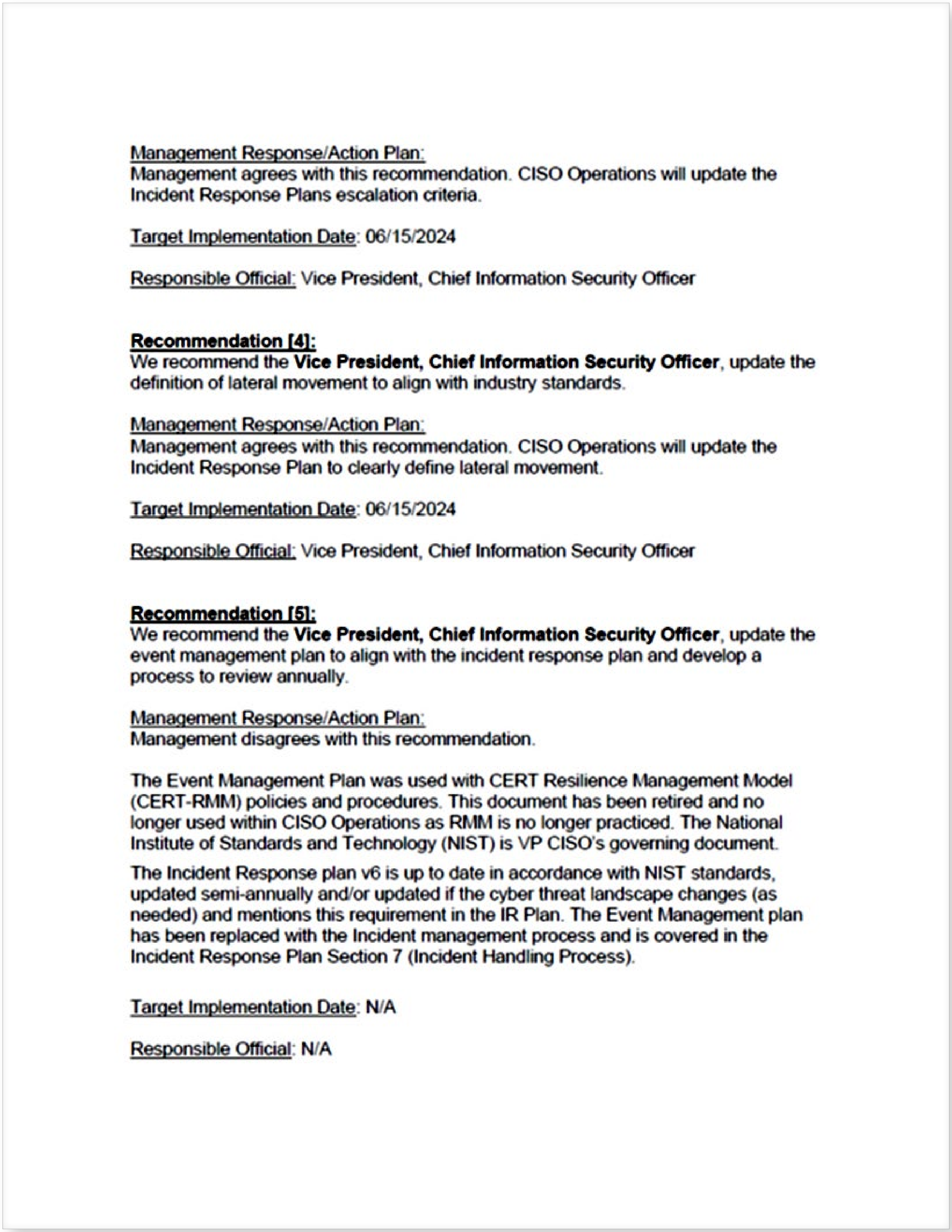
Recommendation [2]:
We recommend the **Vice President, Organization Development**, and **Vice President, Human Resources**, in coordination with the **Vice President, Chief Information Security Officer**, provide mandatory annual security awareness training to craft employees and maintain documentation that these employees completed the training.

Management Response/Action Plan:
Management disagrees with this recommendation. The OIG did not sufficiently provide evidence to support a guarantee that training would be a solution that would mitigate the issue. Training is already readily available and easily accessible for those who are willing to take it. Additionally, the cost to develop and conduct mandatory training to craft employees would be significantly high for an endeavor that has no clear benefit.

Target Implementation Date: N/A

Responsible Official: N/A

Recommendation [3]:
We recommend the **Vice President, Chief Information Security Officer**, update incident response escalation criteria to align with the Postal Service's definition of an incident.



Management Response/Action Plan:
Management agrees with this recommendation. CISO Operations will update the Incident Response Plans escalation criteria.

Target Implementation Date: 06/15/2024

Responsible Official: Vice President, Chief Information Security Officer

Recommendation [4]:
We recommend the **Vice President, Chief Information Security Officer**, update the definition of lateral movement to align with industry standards.

Management Response/Action Plan:
Management agrees with this recommendation. CISO Operations will update the Incident Response Plan to clearly define lateral movement.

Target Implementation Date: 06/15/2024

Responsible Official: Vice President, Chief Information Security Officer

Recommendation [5]:
We recommend the **Vice President, Chief Information Security Officer**, update the event management plan to align with the incident response plan and develop a process to review annually.

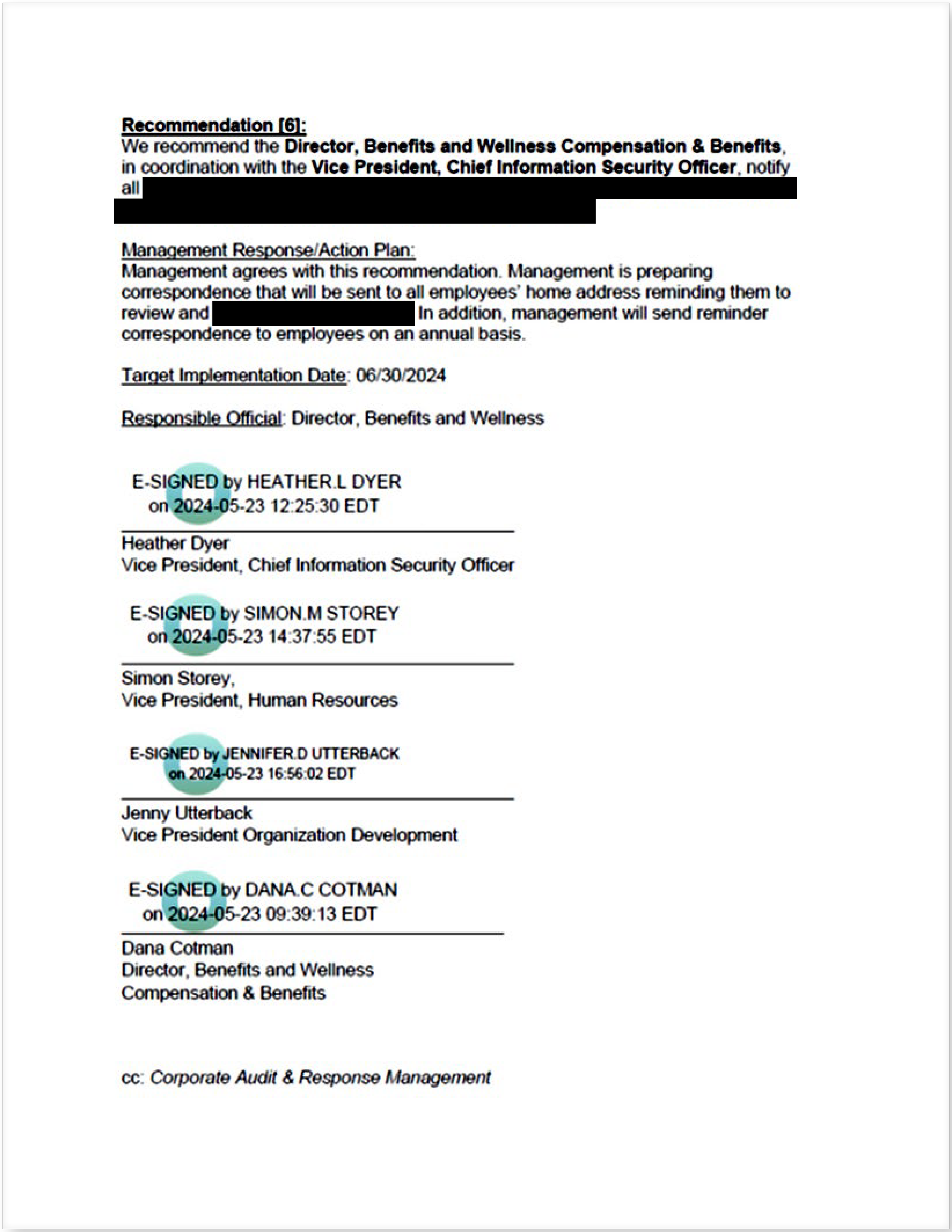
Management Response/Action Plan:
Management disagrees with this recommendation.

The Event Management Plan was used with CERT Resilience Management Model (CERT-RMM) policies and procedures. This document has been retired and no longer used within CISO Operations as RMM is no longer practiced. The National Institute of Standards and Technology (NIST) is VP CISO's governing document.

The Incident Response plan v6 is up to date in accordance with NIST standards, updated semi-annually and/or updated if the cyber threat landscape changes (as needed) and mentions this requirement in the IR Plan. The Event Management plan has been replaced with the Incident management process and is covered in the Incident Response Plan Section 7 (Incident Handling Process).

Target Implementation Date: N/A

Responsible Official: N/A



Recommendation [6]:
We recommend the **Director, Benefits and Wellness Compensation & Benefits**, in coordination with the **Vice President, Chief Information Security Officer**, notify all [redacted]

Management Response/Action Plan:
Management agrees with this recommendation. Management is preparing correspondence that will be sent to all employees' home address reminding them to review and [redacted] In addition, management will send reminder correspondence to employees on an annual basis.

Target Implementation Date: 06/30/2024

Responsible Official: Director, Benefits and Wellness

E-SIGNED by HEATHER.L DYER
on 2024-05-23 12:25:30 EDT

Heather Dyer
Vice President, Chief Information Security Officer

E-SIGNED by SIMON.M STOREY
on 2024-05-23 14:37:55 EDT

Simon Storey,
Vice President, Human Resources

E-SIGNED by JENNIFER.D UTTERBACK
on 2024-05-23 16:56:02 EDT

Jenny Utterback
Vice President Organization Development

E-SIGNED by DANA.C COTMAN
on 2024-05-23 09:39:13 EDT

Dana Cotman
Director, Benefits and Wellness
Compensation & Benefits

cc: *Corporate Audit & Response Management*

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