Office of Inspector General | United States Postal Service

Management Alert

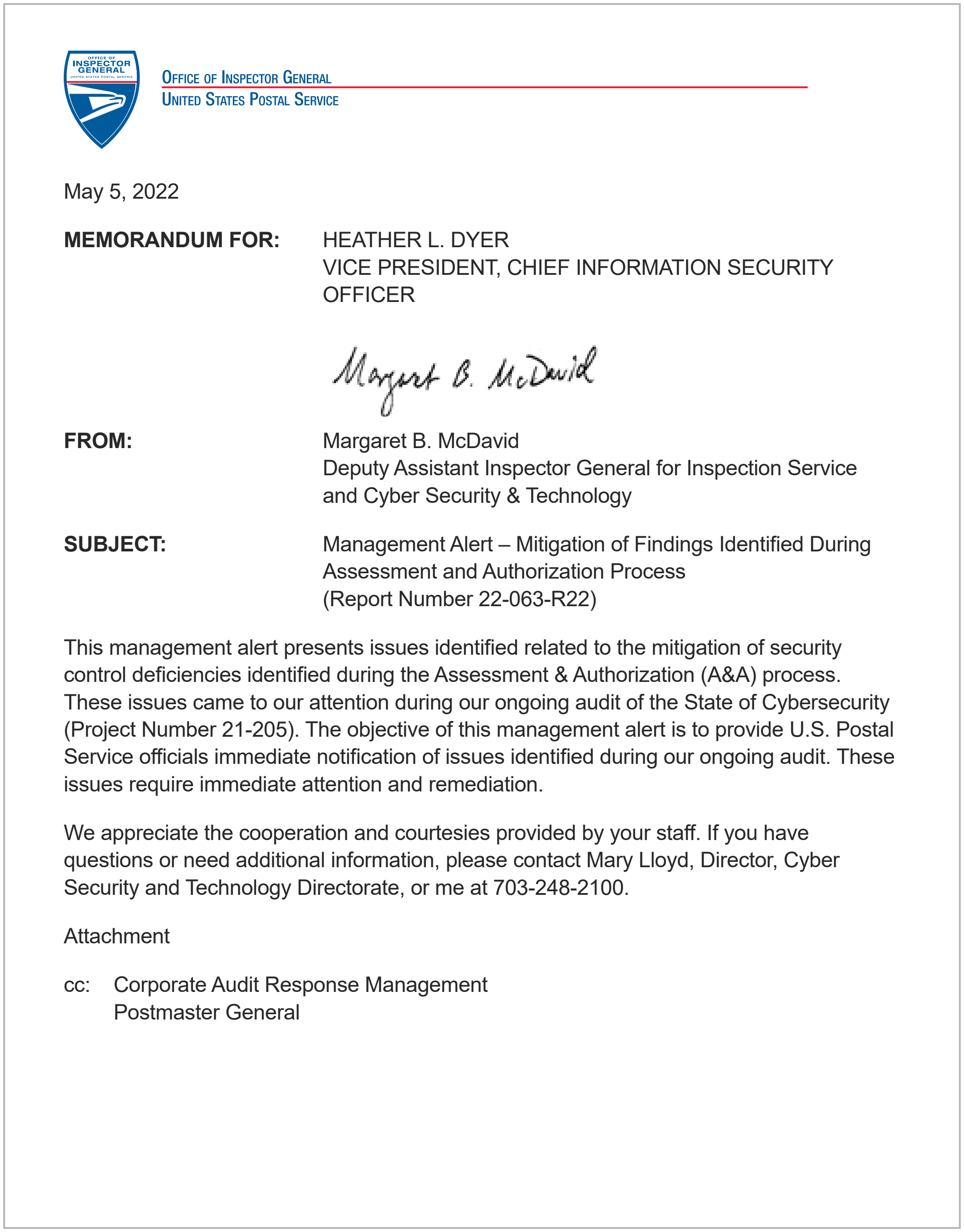
Mitigation of Findings Identified During Assessment and Authorization Process

Report Number 22-063-R22 | May 5, 2022

BACK to COVER

Table of Contents

Transmittal Letter



Office of Inspector General
United States Postal Service

May 5, 2022

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

Margaret B. McDavid

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

SUBJECT: Management Alert – Mitigation of Findings Identified During Assessment and Authorization Process
(Report Number 22-063-R22)

This management alert presents issues identified related to the mitigation of security control deficiencies identified during the Assessment & Authorization (A&A) process. These issues came to our attention during our ongoing audit of the State of Cybersecurity (Project Number 21-205). The objective of this management alert is to provide U.S. Postal Service officials immediate notification of issues identified during our ongoing audit. These issues require immediate attention and remediation.

We appreciate the cooperation and courtesies provided by your staff. If you have questions or need additional information, please contact Mary Lloyd, Director, Cyber Security and Technology Directorate, or me at 703-248-2100.

Attachment

cc: Corporate Audit Response Management
Postmaster General

Results

Introduction

This management alert presents issues the U.S. Postal Service Office of Inspector General (OIG) identified during the *State of Cybersecurity* audit (Project Number 21-205). Our objective is to notify Postal Service management of risks associated with security control deficiencies identified during the Assessment & Authorization (A&A) process that have not been mitigated. See Appendix A for additional information about this alert.

Background

The U.S. Postal Service uses approximately 545 business applications[1] that provide services to both postal employees and its customers and has one of the federal government's most frequently visited websites (usps.com).[2] Given its large cyber presence, the Postal Service faces ongoing threats and challenges that have the potential to hinder its ability to carry out its core function of providing secure and reliable delivery of mail to homes and businesses.[3]

> *"As cyberattacks on the government continue to increase and become more sophisticated, the need for a well-defined A&A process is critical and helps an organization to be proactive rather than reactive to cybersecurity threats."*

As cyberattacks on the government continue to increase and become more sophisticated, the need for a well-defined A&A process is critical and helps an organization to be proactive rather than reactive to cybersecurity threats.[4] The A&A process is a comprehensive process of determining sensitivity and criticality defining security requirements and assessing risk. This process establishes the extent to which the design and implementation of an application meet security requirements defined by federal guidelines, mandates, and the organization. Once these requirements are assessed, the Corporate Information Security Office (CISO) may grant one of these three approval statuses: [5]

- *Full Authorization*, which allows an application to operate on the network because it meets all necessary security controls.
- *Conditional Authorization*, which allows an application to operate on the network under specific terms and conditions.
- *Deny Authorization*, which indicates that the application does not meet security controls requirements.

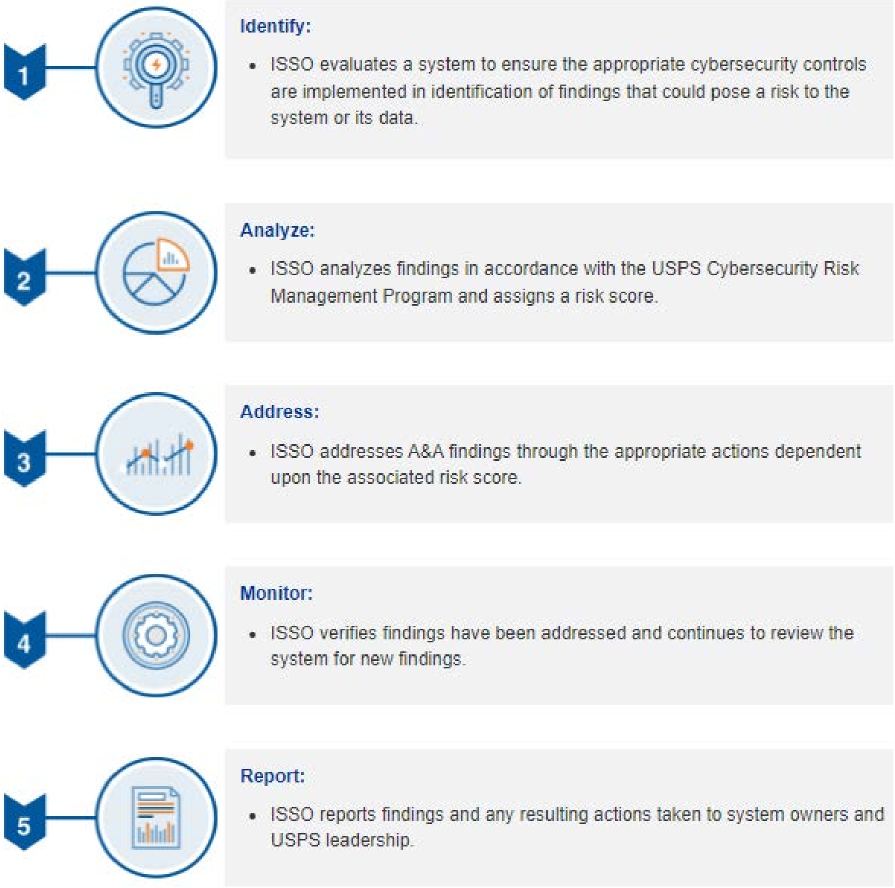
> *"Although the Postal Service has made strides in continuously monitoring and scanning systems on its network, we found issues with the process for mitigating security control deficiencies identified during A&A."*

In October 2020, the Postal Service transitioned from the annual certification[6] and accreditation[7] process to a [redacted] A&A process[8] to support the need for ongoing monitoring

[1] [redacted]
[2] About the United States Postal Service.
[3] USPS Delivers the Facts.
[4] U.S. Department Of Homeland Security Cybersecurity Strategy, dated May 2018.
[5] NIST Special Publication 800-100, dated October 2006.
[6] Certification involves the testing and evaluation of the technical and nontechnical security features of an IT system to determine its compliance with a set of specified security requirements. Certification and Accreditation (C&A) – Glossary | CSRC (nist.gov).
[7] Accreditation is a process whereby a Designated Approval Authority or other authorizing management official authorizes an IT system to operate for a specific purpose using a defined set of safeguards at an acceptable level of risk. Certification and Accreditation (C&A) – Glossary | CSRC (nist.gov).
[8] [redacted]

of security controls. Although the Postal Service has made strides in continuously monitoring and scanning systems on its network, we found issues with the process for mitigating security control deficiencies identified during A&A. Based on the critical nature of postal applications, the Postal Service should ensure that it has adequate security controls in place to prevent risk of exposure of postal systems and data. Figure 1 illustrates the A&A process.

Figure 1. A&A Process



Identify:

- ISSO evaluates a system to ensure the appropriate cybersecurity controls are implemented in identification of findings that could pose a risk to the system or its data.

Analyze:

- ISSO analyzes findings in accordance with the USPS Cybersecurity Risk Management Program and assigns a risk score.

Address:

- ISSO addresses A&A findings through the appropriate actions dependent upon the associated risk score.

Monitor:

- ISSO verifies findings have been addressed and continues to review the system for new findings.

Report:

- ISSO reports findings and any resulting actions taken to system owners and USPS leadership.

Source: Assessment and Authorization (usps.gov).

Findings Summary

We identified deficiencies in the A&A process that limit the ability of the Postal Service to appropriately manage risk within the organization. Specifically, we found applications with security control deficiencies that management was aware of as early as October 2020 that continue to operate under a *Conditional Authorization* with no consequences for unaddressed findings. Applications with known security weaknesses that go unremedied have a higher risk of being exploited. Open exploits could lead to potential disclosure of sensitive customer and employee information and impact postal business operations, which could be costly to remediate.

> *"Specifically, we found applications with security control deficiencies that management was aware of as early as October 2020 that continue to operate under a Conditional Authorization with no consequences for unaddressed findings."*

Finding #1: Mitigation of Security Control Deficiencies

The CISO does not always ensure that security control deficiencies found during the A&A process are properly mitigated within established timelines. When a security control deficiency is found during the A&A process, CISO works with system owners to develop a Risk Mitigation Plan that establishes a planned date to remediate or mitigate the finding. However, the system accreditor does not always ensure remediation of the identified issues by this date. We reviewed a sample of 115 applications, including 37 business critical and 78 non-business critical applications and identified security control deficiencies that were rated a heat score[9] of 5 or higher and had been open for at [redacted] (see Table 1). The heat score is based on the deficiencies' impact level and possibility of occurrence specified in the Cyber Risk Heat Score matrix (see Table 2). Based on our review, we identified security control deficiencies were placed on a Risk

[9] [redacted]

Mitigation Plan and had planned [redacted]. Specifically, we found:

- [redacted] business critical applications with open findings.
- [redacted] non-business critical applications with open findings.

Table 1. Applications with Open Security Control Deficiencies for [redacted]

Application Name	Enterprise Information Repository (EIR) Number
Business Critical Applications	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
Non-Business Critical Applications	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Source: [redacted] as of January 2022.

Additionally, we found [redacted] Industry applications for which we could not validate risk acceptance in the [redacted] System, the A&A system of record, because they follow a separate process for risk acceptance. These applications are granted Security Exception Letters from the Technology Management Office and maintained in a separate repository. The [redacted] does not formally indicate that these exceptions are granted; therefore, limiting the ability for one to understand and appropriately manage the cybersecurity risk for the organization.

High-risk security issues should be mitigated or deployment of the application should be deferred.[10] If security control weaknesses with an associated application are not remediated within the Risk Mitigation Plan timeframe, the

[10] Handbook AS-805-A, *Information Resource Certification and Accreditation (C&A) Process*, Section 2-12, Accreditor, dated March 2021.

application should be placed in *Deny Authorization* status.[11] Handbook AS-805 states that CISO is responsible for ensuring compliance with information security policies and standards.[12] Vulnerabilities are left unmitigated because CISO is not enforcing security policy compliance and allowing applications to remain on the network after a failure to comply.

Table 2. Cyber Risk Heat Score Matrix

Heat Score						
IMPACT	**Catastrophic**	5	6	7	8	9
	Major	4	5	6	7	8
	Moderate	3	4	5	6	7
	Minor	2	3	4	5	6
	Insignificant	1	2	3	4	5
		Rare	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
		LIKELIHOOD				

Source: Cyber Risk Management Program.

As the Postal Service continues to evolve and mature its A&A process, implementing a process that ensures applications are operating with an acceptable level of risk to the organization is crucial. By not addressing security control deficiencies, the Postal Service leaves itself susceptible to operating in a reactive state when a security incident does occur, rather than proactively working to reduce the risk of these security incidents happening. For example, in [redacted] the Postal Service was made aware of suspicious internet activity involving a [redacted]. This occurred, due to a lack of security [redacted]. The Postal Service was aware of these [redacted] since at least as early as 2011 and continued to track the [redacted] in an [redacted] The Postal Service missed the remediation date of [redacted]. Once the suspicious login activity occurred, the system was placed in a [redacted]. Due to this incident, the Postal Service was required to notify over [redacted] of a potential data breach and forced password resets on [redacted] accounts.[13] [redacted] this could lead to further exposure of the [redacted] and [redacted]

Recommendation #1

We recommend the **Vice President, Chief Information Security Officer**, implement a process that ensures security control deficiencies are remediated timely and in accordance with established remediation plans

[11] Handbook AS-805-A, Section 2-12, Accreditor, dated March 2021.

[12] Handbook AS-805, *Information Security*, Section 2-2.5, Chief Information Security Officer, dated June 2021.

[13] [redacted]

Management's Comments

Management agreed with the finding and recommendation.

Regarding the recommendation, management agreed and stated that they plan to introduce additional requirements for an A&A compliance failure, shift from accreditation to Authorization to Operate (ATO) and have the Executive Cyber Risk Committee review all delinquent compliance failures beyond the [redacted] The target implementation date is September 30, 2022.

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

Evaluation of Management's Comments

The U.S. Postal Service Office of Inspector General (OIG) considers management's comments responsive to the recommendation in the report.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective action is complete. The recommendation should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendation can be closed.

Appendices

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

Appendix A: Additional Information

Scope and Methodology

The audit scope for this management alert includes controls over the A&A process.

Our fieldwork methodology for the alert included:

- Reviewing a sample of 115 applications for A&A findings in [redacted] from November 2021 and January 2022 with heat scores of 5 or higher and evaluating open findings for compliance with established Postal Service policy and procedures.
- Evaluating the Postal Service's cybersecurity policies for alignment with accepted A&A frameworks and best practices.
- Reviewing the [redacted] for effect of suspicious logins on the [redacted] applications and the Postal Service's response.
- Interviewing and reviewing postal documents to determine the root cause(s) of ineffective controls over the A&A process.

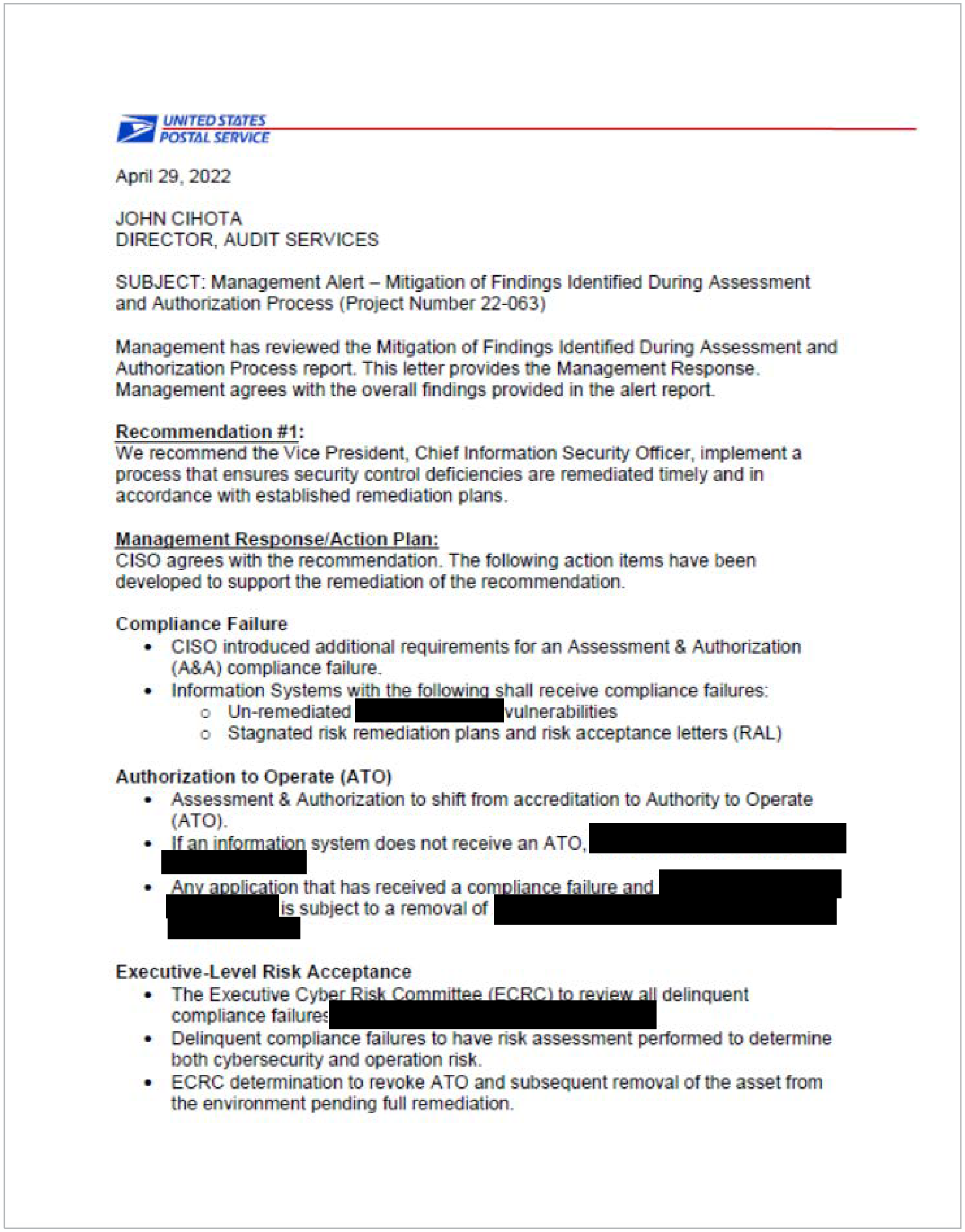
We conducted this performance audit from February through May 2022, in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions. We discussed our observations and conclusions with management on April 14, 2022, and included their comments where appropriate.

We assessed the reliability of [redacted] data by interviewing personnel knowledgeable about the data, obtaining screenshots of how the [redacted] data was pulled, and performing manual reconciliations to supporting documents or systems. We determined that the data were sufficiently reliable for the purposes of this alert.

Prior Audit Coverage

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

Appendix B: Management's Comments



UNITED STATES POSTAL SERVICE

April 29, 2022

JOHN CIHOTA
DIRECTOR, AUDIT SERVICES

SUBJECT: Management Alert – Mitigation of Findings Identified During Assessment and Authorization Process (Project Number 22-063)

Management has reviewed the Mitigation of Findings Identified During Assessment and Authorization Process report. This letter provides the Management Response. Management agrees with the overall findings provided in the alert report.

Recommendation #1:
We recommend the Vice President, Chief Information Security Officer, implement a process that ensures security control deficiencies are remediated timely and in accordance with established remediation plans.

Management Response/Action Plan:
CISO agrees with the recommendation. The following action items have been developed to support the remediation of the recommendation.

Compliance Failure

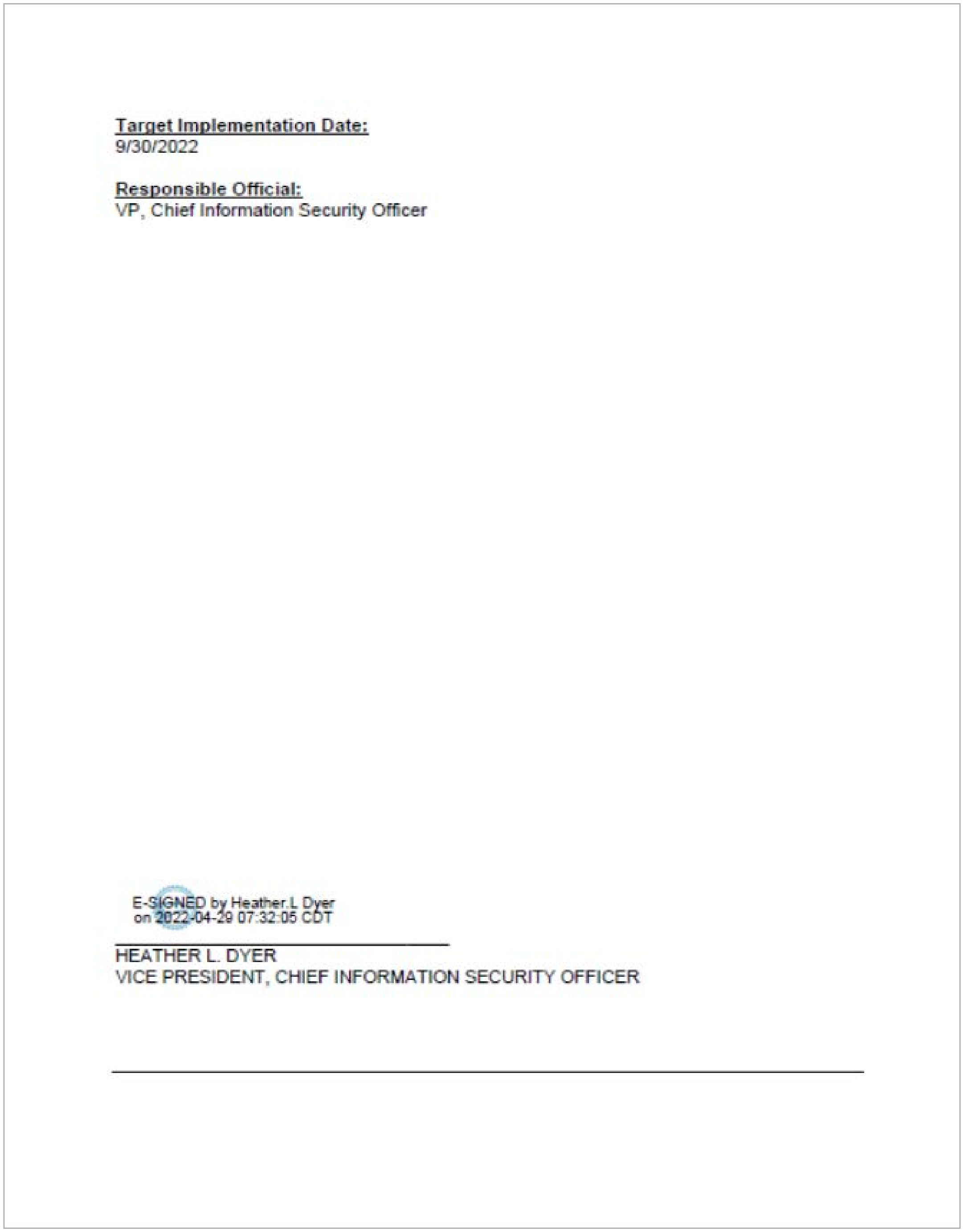
- CISO introduced additional requirements for an Assessment & Authorization (A&A) compliance failure.
- Information Systems with the following shall receive compliance failures:
  - Un-remediated [redacted] vulnerabilities
  - Stagnated risk remediation plans and risk acceptance letters (RAL)

Authorization to Operate (ATO)

- Assessment & Authorization to shift from accreditation to Authority to Operate (ATO).
- If an information system does not receive an ATO, [redacted]
- Any application that has received a compliance failure and [redacted] is subject to a removal of [redacted]

Executive-Level Risk Acceptance

- The Executive Cyber Risk Committee (ECRC) to review all delinquent compliance failures [redacted]
- Delinquent compliance failures to have risk assessment performed to determine both cybersecurity and operation risk.
- ECRC determination to revoke ATO and subsequent removal of the asset from the environment pending full remediation.



Target Implementation Date:
9/30/2022

Responsible Official:
VP, Chief Information Security Officer

E-SIGNED by Heather.L Dyer
on 2022-04-29 07:32:05 CDT

HEATHER L. DYER
VICE PRESIDENT, CHIEF INFORMATION SECURITY OFFICER

OFFICE OF
INSPECTOR
GENERAL
UNITED STATES POSTAL SERVICE

Contact us via our Hotline and FOIA forms.
Follow us on social networks.
Stay informed.

1735 North Lynn Street
Arlington, VA 22209-2020
(703) 248-2100

For media inquiries, please email
press@uspsoig.gov or call 703-248-2100