Highlights
Table of Contents
Findings
Recommendations
Appendices

OFFICE OF
INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Insider Threat Program

Audit Report

Report Number
IT-AR-17-007

September 18, 2017

Print

Highlights
Table of Contents
Findings
Recommendations
Appendices

Highlights

The Postal Service has not fully established and implemented an insider threat program in accordance with Postal Service policies and best practices.

Background

An insider threat program helps an organization prevent, detect, and respond to the threat of an employee, contractor, or business partner misusing their trusted access to computer systems and data. Threats to the U.S. Postal Service include the theft and disclosure of sensitive, proprietary, or national security information, and the sabotage of its computer systems or data.

Executive Order 13587 and the National Insider Threat Policy mandate that federal agencies with access to national security information have a formal insider threat program. The guidelines outlined within the National Insider Threat policy provide a framework of security principles and best practices that the Postal Service is required to follow.

Industry best practices recommend organizations create an insider threat program to protect an organization's sensitive, critical, and proprietary information. The program should include at minimum components such as, organization-wide participation, standard operating procedures, and insider threat training and awareness.

The Postal Service is not an originator of national security information. A limited number of employees have access to national security systems and are custodians of national security electronic and hard copy information for the purposes of continuity of [redacted].

With regard to sensitive information, the Postal Service stores and secures this type of information, [redacted]

The U.S. Postal Inspection Service (USPIS) is responsible for developing, coordinating, and implementing an insider threat program to protect national security information, while the Corporate Information Security Office (CISO) is responsible for cybersecurity, ensuring the organization's technologies, processes and digital assets are protected from improper access.

Our objective was to determine if the Postal Service has established and implemented an effective insider threat program in accordance with Postal Service policies and best practices.

What the OIG Found

The Postal Service has not fully established and implemented an insider threat program in accordance with Postal Service policies and best practices. Specifically, the USPIS has not implemented all of the minimum standards required by the National Insider Threat Policy for national security information. Also, the CISO has not fully established a program for protecting the Postal Service's [redacted].

This occurred because the USPIS did not dedicate full-time resources and the CISO focused their efforts on [redacted] prior to establishing and implementing an insider threat program.

Without an implemented insider threat program, [redacted] as well as negatively impact the Postal Service brand.

We also found several physical security and access deficiencies at some of the locations that hold national security information. The identified physical security deficiencies included non-functioning closed-circuit television cameras, a broken video intercom, and a [redacted] With the exception of one location, management corrected the deficiencies we identified. We also identified personnel who had access to these locations without the proper security clearance.

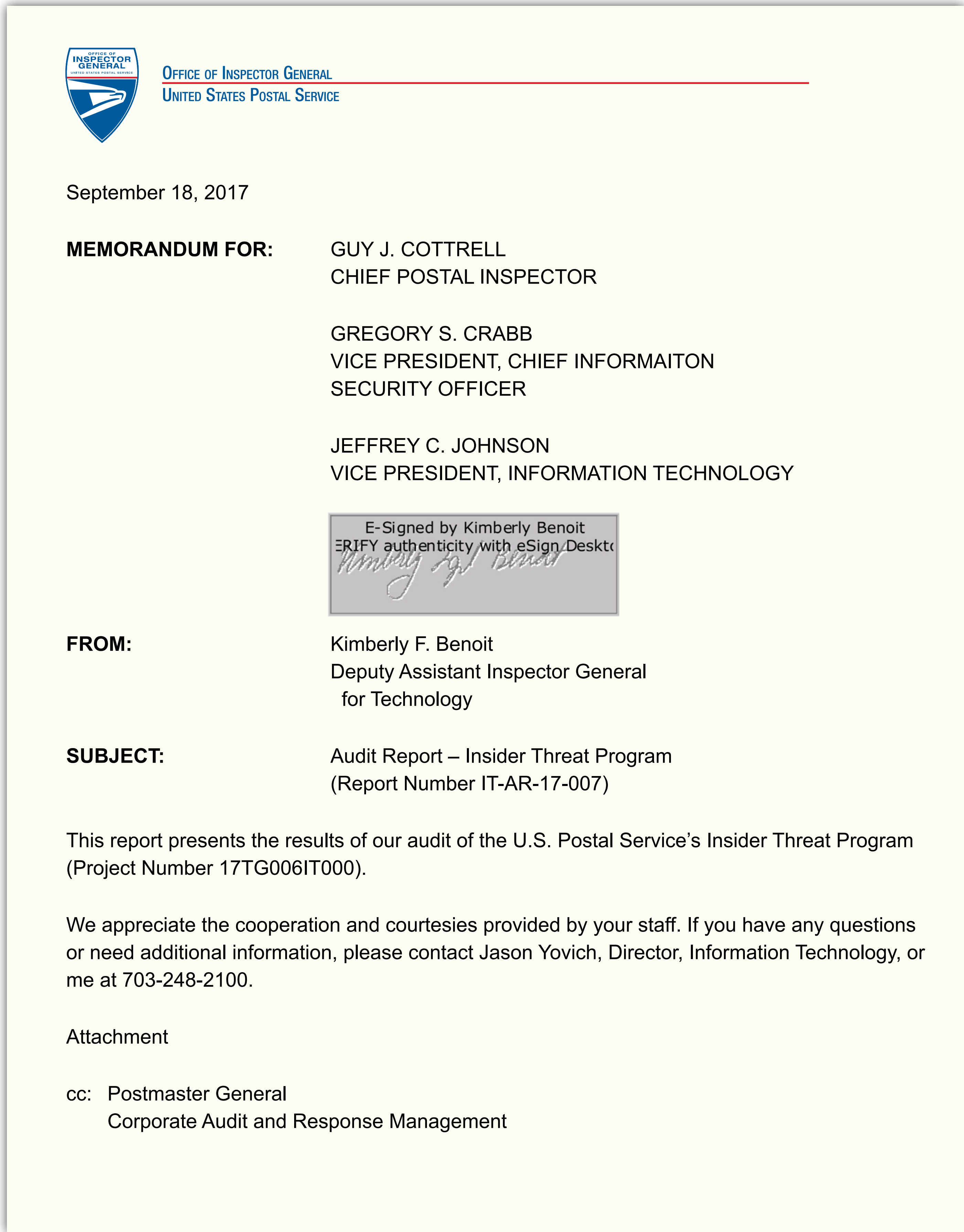
These deficiencies occurred due to a lack of coordination and communication between Information Technology, USPIS, and facilities management regarding physical security.

Without proper physical security controls in place, the Postal Service cannot deter and detect unauthorized entry and movement within locations. This could result in the theft of information.

What the OIG Recommended

We recommended USPIS to continue to develop and implement an insider threat program for national security information in accordance with the minimum standards outlined in the National Insider Threat Policy. We also recommended the CISO to formally establish and implement an organization-wide insider threat program for sensitive, critical, and proprietary information. Finally, management should coordinate to repair the security deficiencies we identified at the remaining location.

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

September 18, 2017

MEMORANDUM FOR: GUY J. COTTRELL
CHIEF POSTAL INSPECTOR

GREGORY S. CRABB
VICE PRESIDENT, CHIEF INFORMAITON
SECURITY OFFICER

JEFFREY C. JOHNSON
VICE PRESIDENT, INFORMATION TECHNOLOGY

E-Signed by Kimberly Benoit
ERIFY authenticity with eSign Deskt

FROM: Kimberly F. Benoit
Deputy Assistant Inspector General
for Technology

SUBJECT: Audit Report – Insider Threat Program
(Report Number IT-AR-17-007)

This report presents the results of our audit of the U.S. Postal Service's Insider Threat Program (Project Number 17TG006IT000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Jason Yovich, Director, Information Technology, or me at 703-248-2100.

Attachment

cc: Postmaster General
Corporate Audit and Response Management

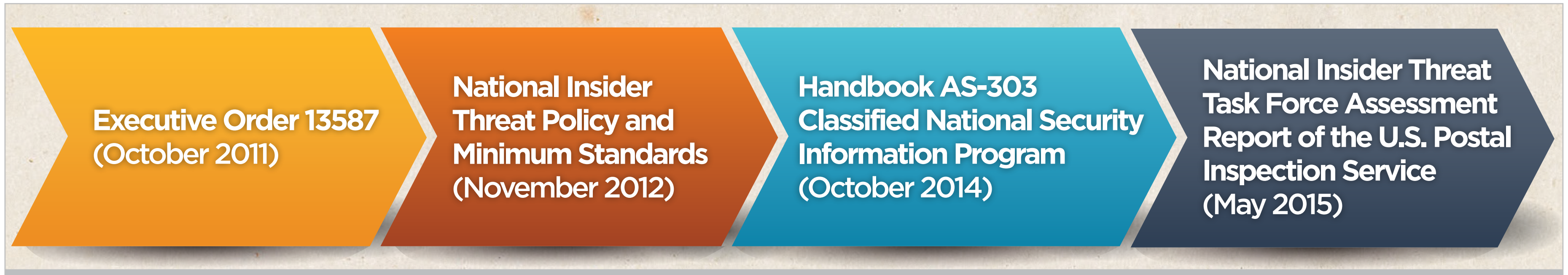
Table of Contents

Introduction

This report presents the results of our self-initiated audit of the U.S. Postal Service's insider threat program (Project Number 17TG006IT000). Our objective was to determine if the Postal Service has established and implemented an effective insider threat program in accordance with Postal Service policy and best practices.

An insider threat program helps an organization prevent, detect, and respond to the threat of an employee, contractor, or business partner from misusing their trusted access to computer systems and data. A threat to the Postal Service may include the theft and disclosure of sensitive,[1] proprietary, and national security information,[2] or the sabotage of its computer systems and data.

Figure 1: Insider Threat Policies and Assessment Applicable to the U.S. Postal Inspection Service


Executive Order 13587 (October 2011)
National Insider Threat Policy and Minimum Standards (November 2012)
Handbook AS-303 Classified National Security Information Program (October 2014)
National Insider Threat Task Force Assessment Report of the U.S. Postal Inspection Service (May 2015)

Executive Order 13587
This executive order mandates that all federal agencies with access to national security information have a formal insider threat program. EO 13587 provides structural reforms to improve the security of classified networks and the responsible sharing and safeguarding of national security information.

National Insider Threat Policy and Minimum Standards
This policy provides a framework of security principles and best practices that the Postal Service is required to follow. The minimum standards are (1) designation of senior official(s); (2) information integration, analysis, and response; (3) insider-threat program personnel; (4) access to information; (5) monitoring user activity on networks; and (6) employee training and awareness.

Handbook AS-303 Classified National Security Information Program
This handbook provides Postal Service instructions and procedures for the management, accountability, and protection of classified national security information, and these instructions and procedures apply to all Postal Service personnel who need access to classified national security information.

National Insider Threat Task Force (NITTF) Assessment Report
The National Insider Threat Policy requires the NITTF to conduct assessments to determine the level of organizational compliance with the Policy and Minimum Standards. The NITTF completed this assessment of the USPIS in May 2015.

[1] Handbook AS-805, *Information Security*, Section 3-2.3.3, defines sensitive information as hard copy or electronic information or material that requires protection.
[2] We used national security information instead of classified information for the purposes of our report.

The Postal Service is not the originator of national security information. A limited number of employees have access to national security systems and are custodians of national security electronic and hard copy information [redacted] Executive Order (EO) 13587[3] and the National Insider Threat Policy[4] mandate that the Postal Service have a formal insider threat program for national security information. The U.S. Postal Inspection Service (USPIS) is responsible for developing, coordinating, and implementing the insider threat program. The USPIS has approved [redacted] for the cybercrime investigative program, including an insider threat program, to continue the Postal Service on its path of compliance with EO 13587 and all identified cybercrime gaps.

The Postal Service stores and secures sensitive information, including private information about employees and contractors such as [redacted] The Corporate Information Security Office (CISO) is responsible for cybersecurity, ensuring the organization's technologies, processes and digital assets are protected from improper access. Industry best practices recommends organizations create an insider threat program to protect sensitive, critical, and proprietary information.

See Appendix A for additional information about this audit.

Summary

The Postal Service has not fully established and implemented a formal insider threat program in accordance with Postal Service policies and best practices. Specifically, the USPIS has not implemented all National Insider Threat Policy minimum standards required for [redacted]. In addition, the CISO has not establish an insider threat program for [redacted]. This occurred because the USPIS did not dedicate full-time resources and the CISO focused their efforts on [redacted] prior to establishing and implementing an insider threat program.

We also found several physical security deficiencies [redacted] due to a lack of coordination and communication between Information Technology (IT), USPIS, and facilities management. During the audit, management took corrective actions to remove five contractors who had access to secured spaces without the proper security clearance and to repair the closed-circuit televisions (CCTV) and a video intercom system.

Insider Threat Program Development

The USPIS has not implemented all of the minimum standards required by the National Insider Threat Policy for [redacted] Additionally, the CISO has not established a formal insider threat program to protect the Postal Service's [redacted].

The Postal Service has not fully established and implemented a formal effective insider threat program in accordance with Postal Service policy and best practices. Specifically, the USPIS has not implemented all of the minimum standards required by the National Insider Threat Policy for [redacted]. Additionally, the CISO has not established a formal insider threat program to protect the Postal Service's [redacted]

[3] EO 13587, dated October 7, 2011, directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. This executive order mandates that all federal agencies with access to national security information have a formal insider threat program.

[4] *The National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, dated November 21, 2012, provides direction and guidance for promoting the development of effective insider threat programs.

[5] Secured spaces are areas within the main location that are co-use or multiple use locations that perform functions other than just national security.

Highlights
Table of Contents
Findings
Recommendations
Appendices

EO 13587 and the National Insider Threat Policy state that federal agencies with access to national security information must have a formal insider threat program. This policy contains six minimum standards[6] with 26 tasks that agencies must follow.

We determined that management started implementing the six minimum standards outlined in the National Insider Threat Policy. However, we found deficiencies in:

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

We found several physical security deficiencies at [redacted] [redacted]

See Appendix B for details about the status of the six minimum standards and their related tasks.

According to industry best practices,[7] organizations should create an enterprise-wide insider threat program to protect sensitive, critical, and proprietary information. An insider threat program includes at minimum components such as, organization-wide participation, an insider threat team, standard operating procedures, insider threat training to everyone, and specialized awareness training to all individuals participating in the program. Additionally, organizations should monitor employees to detect insider threats.

This occurred because the USPIS did not dedicate full-time resources to fully develop and implement an insider threat program to protect [redacted] CISO focused their efforts and resources on remediating [redacted] prior to establishing and implementing an insider threat program to protect [redacted].

Without an established and implemented insider threat program, the Postal Service cannot effectively prevent, detect, and respond to employee and contractor insider threats. [redacted] as well as negatively impact the Postal Service brand.[8]

Physical Security Controls

We found several physical security deficiencies at [redacted]. Specifically, we found:

- Five contractors had access to two of the secure spaces without proper security clearances. According to each of the secured space's Standard Operating Procedures (SOP), access to the secured spaces is limited to personnel with a need[9] and a top-secret security clearance and the access must be authorized by the security manager.

[6] The minimum standards are (1) designation of senior official(s); (2) information integration, analysis, and response; (3) insider threat program personnel; (4) access to information; (5) monitoring user activity on networks; and (6) employee training and awareness.

[7] Gartner, *Best Practices for Managing Insider Security, Threats*, August 2016 udpate and Carnegie Mellon University, Software Engineering Institute, *Common Sense Guide to Mitigating Insider Threats*, Fifth Edition, December 2016.

[8] The U.S. Postal Service Office of Inspector General (OIG) assessed Postal Service IT security's risk for not having a fully developed and implemented insider threat program by using our Risk Impact Assessment tool. We calculated a [redacted] of an insider event occurring. Using the 2016 Ponemon industry standard average cost for a cybercrime of $6.9 million, we calculated IT security at risk totaling about [redacted]

[9] A prospective recipient's need for access to specific classified information required to perform or assist in a lawful and authorized government function as determined by an authorized custodian of that classified information.

- At one location, the CCTV cameras used to monitor access to secured spaces were not functioning. Postal Service policy[10] requires functioning CCTV systems for access-controlled entrances.

- One location did not have an [redacted] or a fire extinguisher in the secured space to protect its national security information. According to this location's SOP, an [redacted] and fire extinguisher are required for the secured space within the location.

- Another location did not have a working video intercom system[12] for its secure space as required by its SOP.

These deficiencies occurred due to a lack of coordination and communication between facilities management, USPIS, and IT regarding physical security at the secured spaces. Without physical security controls, the Postal Service cannot deter and detect unauthorized entry and movement at each secured space. Additionally, personnel may not be adequately protected from environmental hazards. This could result in national security information being stolen, which could be used to damage U.S. national security and negatively impact the Postal Service brand.

During our audit, management took corrective action to remove the improper secured space's access for the five contractors and repaired the security cameras and video intercom system at another location.

[10] Administrative Support Manual (ASM) 273.172-173.
[11] [redacted].
[12] A unit that has a camera, speaker, a push button that is installed at an entrance door, and an internal monitor unit that can communicate with the entrance unit.

Recommendations

We recommend management establish and implement a formal organization-wide insider threat program for [redacted]

We recommend the chief postal inspector:

1. Continue to develop and fully implement an insider threat program for national security information in accordance with National Insider Threat Policy minimum standards.

We recommend the vice president, chief information security officer to:

2. Establish and implement a formal organization-wide insider threat program for [redacted]

We recommend the Chief Postal Inspector and Vice President, Information Technology, direct managers to:

3. [redacted] and a fire extinguisher at the secured space currently not in compliance.

Management's Comments

Management generally agreed with all of the findings and recommendations in the report. See Appendix C for management's comments in their entirety.

Regarding recommendation 1, management agreed to achieve Full Operating Capability for the twenty-six minimum standards as defined by the National Insider Threat Task Force for its National Security Insider Threat Program. The target implementation date is October 1, 2019.

Regarding recommendation 2, management agreed to ensure the effective implementation of an insider threat program through executive sponsorship, develop an insider threat policy, request funding in a future cybersecurity related decision analysis report and finalize an organizational-wide general insider threat module. The target implementation date is September 30, 2018.

Regarding recommendation 3, management agreed to coordinate and install an [redacted] and fire extinguisher at the secured space. The target implementation date is October 1, 2018.

Evaluation of Management's Comments

The OIG considers management comments responsive for recommendations 1, 2, and 3 and corrective actions should resolve the issues identified.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective action(s) 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.

Appendices

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

Appendix A: Additional Information

Background

An insider threat is the potential for a current or former employee, contractor, or business partner to accidentally or maliciously misuse their trusted access to harm an organization's employees, customers, assets, or reputation. The threat may include theft of classified and unclassified information that is sensitive, critical, or proprietary. This threat can also include damage to the U.S. through espionage, terrorism, or unauthorized disclosure of national security information.[13]

Organizations can significantly reduce their exposure to insider threats and prevent attacks by establishing an effective insider threat program. An insider threat program helps organizations prevent, detect, and respond to insider threats. Such programs develop and implement policies and procedures so that all insider threat activities are conducted in accordance with federal guidance, laws, regulations, and an organization's policy.

A mature insider threat program fosters coordination among different organizational groups that would be involved with an insider threat incident and includes an insider threat team responsible for responding to insider threats. In addition, employee education and awareness are necessary to ensure that an insider threat program is effective. Management alerting employees to the possibility of an insider threat and its consequences may make them more aware and more likely to report it to management.

EO 13587 and the National Insider Threat Policy mandate that federal agencies with access to national security information have a formal insider threat program. While the Postal Service is not the originator of national security information, a limited number of its employees have access to national security systems and are custodians of national security electronic and hard copy information for the purposes of [redacted]. The USPIS is responsible for developing, coordinating, and implementing an insider threat program for national security information, while the CISO is responsible for cybersecurity, ensuring the organization's technologies, processes and digital assets are protected from improper access.

The USPIS created a program to enhance its cybercrime investigative response, detect organizational cyber threats, and develop an Insider Threat program. The USPIS has approved [redacted] for the cybercrime investigative program to continue the Postal Service on its path to compliance with EO 13587 and all identified cybercrime gaps. This program is in the [redacted] and will expand the existing USPIS insider threat program in coordination with CISO to protect sensitive, critical, proprietary information.

Objective, Scope, and Methodology

Our objective was to determine if the Postal Service has established and implemented an effective insider threat program in accordance with Postal Service policy and best practices. Our scope was the detection, prevention and response functions of the Postal Service's insider threat program. We did not perform an analysis of potential insider threat activities. Also, we did not assess the CISO information security functions.

The OIG's Office of Investigations would normally participate in a response to an insider threat or attack if notified. However, to maintain its independence, it does not have direct responsibility for designing or implementing the Postal Service's insider threat program. Therefore, it was not included in the scope of this audit.

[13] Handbook AS-303, *Classified National Security Information Program*, October 2014. Chapter 11, This handbook provides Postal Service instructions and procedures for the management, accountability, and protection of classified national security information, and these instructions and procedures apply to all Postal Service personnel who need access to classified national security information. The CERT Insider Threat Center, *Common Sense Guide to Mitigating Insider Threats,* Fifth Edition, December 2016.

To accomplish our objective we:

- Interviewed Postal Service personnel responsible for the insider threat program and its activities. Also, we identified and interviewed all groups involved in the insider threat program, such as USPIS, Human Resources, CISO, and Office of Independent Counsel.

- Determined if there is a formal documented insider threat program and compared it to Postal Service policies, federal guidance, best practices, and the National Insider Threat Task Force assessment[14] and identified any gaps.

- Identified locations that contain national security information and conducted a limited physical security review in accordance with criteria for national security areas.

- Determined if management has developed insider threat awareness training for all employees.

We conducted this performance audit from March through September 2017, 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 August 2, 2017, and included their comments where appropriate.

We assessed the reliability of the insider threat program data by reviewing related documentation, interviewing knowledgeable Postal Service officials, reviewing related internal controls, and analyzing the data. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

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

[14] The National Insider Threat Policy requires NITTF to conduct assessments to determine the level of organizational compliance with the Policy and Minimum Standards. The NITTF completed this assessment of the USPIS in May 2015.

This chart contains our analysis of the Postal Service's current status of compliance with the National Insider Threat Policy and its minimum standards applicable to national security information.

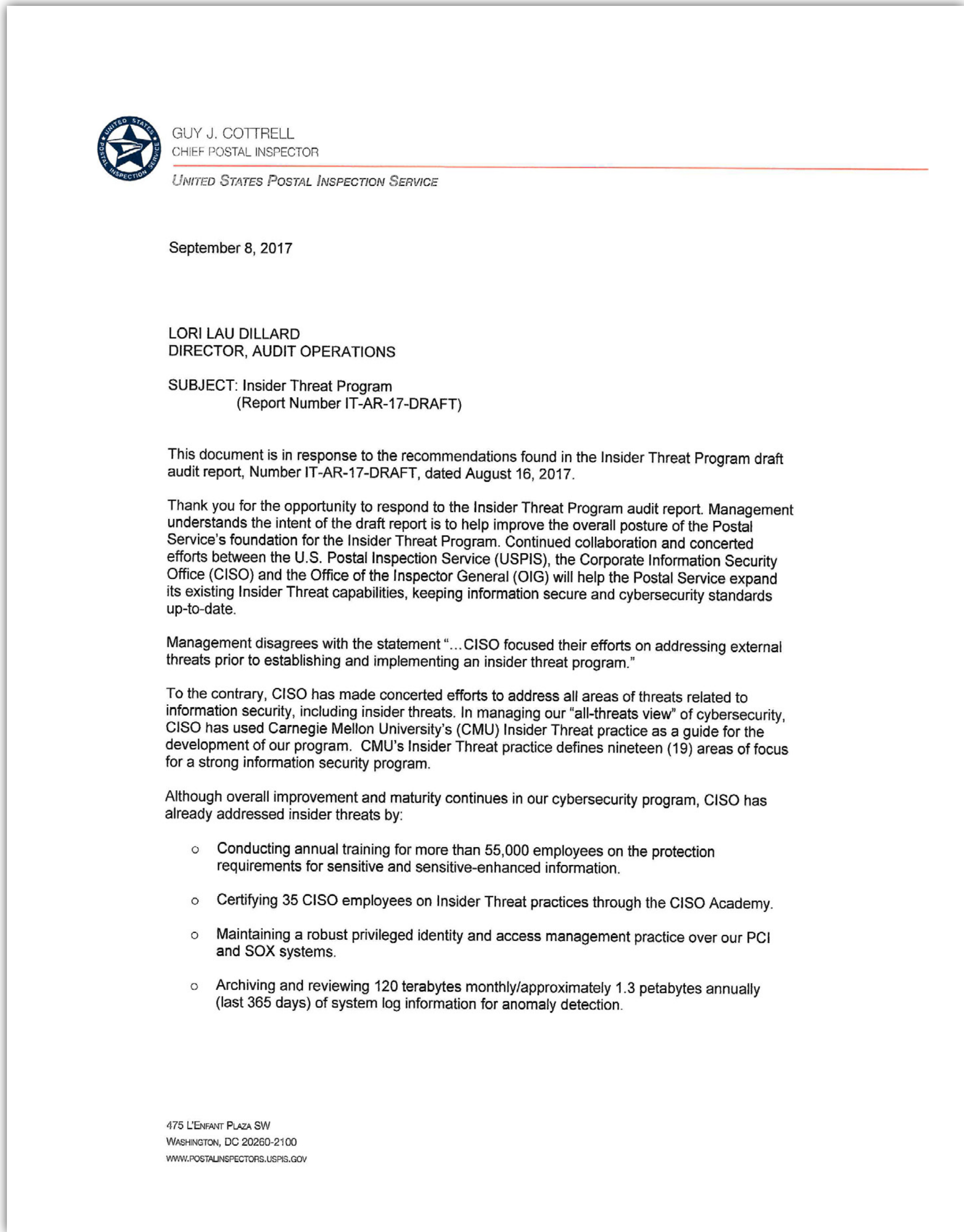
	Minimum Standards	OIG Determined Status	Maturity Level**
Designation of Senior Official			
1	Designate a Senior Official	[redacted]	[redacted]
2	Create an Insider Threat Policy	[redacted]	[redacted]
3	Establish Implementation Plan and	[redacted]	[redacted]
	Produce an Annual Report	[redacted]	[redacted]
4	Coordinate program activities with proper authorities	[redacted]	[redacted]
5	Create records handling and use procedures	[redacted]	[redacted]
6	Develop records retention guidelines	[redacted]	[redacted]
7	Conduct oversight reviews for policy & legal compliance	[redacted]	[redacted]
Information Integration, Analysis and Response			
8	Build and maintain an insider threat analytic and response capability - to ingest, review, centrally analyze, and respond to internal relevant information	[redacted]	[redacted]
9	Procedures for insider threat response actions - centrally managed by Insider Threat Program*	[redacted]	[redacted]
10	Procedures for documenting each matter reported and response action taken	[redacted]	[redacted]
Insider Threat Program Personnel			
11	Program personnel trained in CI & security fundamentals	[redacted]	[redacted]
12	Program personnel trained in conducting response actions	[redacted]	[redacted]
13	Program personnel trained in retaining, safeguarding and use of records/data	[redacted]	[redacted]
14	Program personnel trained in applicable civil liberty and privacy laws	[redacted]	[redacted]
15	Program personnel trained in applicable laws, regulations and policies and requirements - investigative referral requirements of Section 811	[redacted]	[redacted]
Access to Information			
16	Program receives timely relevant component information - CI & security IA and HR	[redacted]	[redacted]
17	Procedures to establish access to sensitive or protected information	[redacted]	[redacted]
18	Reporting guidelines for component departments to report relevant insider information	[redacted]	[redacted]
19	Timely Access to CI reporting and analytical products pertaining to adversarial threats	[redacted]	[redacted]
Monitor User Activity on Networks			
20	Monitor use activity on all classified networks; either via internal or external agreements	[redacted]	[redacted]
	Conduct monitoring on at least one classified network	[redacted]	[redacted]
21	Create policies for protecting, interpreting, storing and limiting access to user activity monitoring methods and results	[redacted]	[redacted]

Highlights
Table of Contents
Findings
Recommendations
Appendices

	Minimum Standards	OIG Determined Status	Maturity Level**
22	Obtain signed agreements by all cleared employees	[redacted]	[redacted]
23	Ensure that there are classified and unclassified network banners informing users that networks are monitored	[redacted]	[redacted]
Employee Training and Awareness			
24	Create procedures for initial & recurring training for employees to include documentation	[redacted]	[redacted]
25	Verify all cleared employees have completed required insider threat awareness training	[redacted]	[redacted]
26	Provide an Internal network site to provide Insider Threat Information and to receive referrals	[redacted]	[redacted]

Source: OIG analysis and National Insider Threat Policy as of April 12, 2017.
* For these tasks, we relied on the National Insider Threat Assessment conducted May 27, 2015.
** Each maturity level (program establishment, initial operating capability, and full operating capability) provides a layer in the foundation for continuous program improvement.

Appendix C: Management's Comments



GUY J. COTTRELL
CHIEF POSTAL INSPECTOR

UNITED STATES POSTAL INSPECTION SERVICE

September 8, 2017

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Insider Threat Program
(Report Number IT-AR-17-DRAFT)

This document is in response to the recommendations found in the Insider Threat Program draft audit report, Number IT-AR-17-DRAFT, dated August 16, 2017.

Thank you for the opportunity to respond to the Insider Threat Program audit report. Management understands the intent of the draft report is to help improve the overall posture of the Postal Service's foundation for the Insider Threat Program. Continued collaboration and concerted efforts between the U.S. Postal Inspection Service (USPIS), the Corporate Information Security Office (CISO) and the Office of the Inspector General (OIG) will help the Postal Service expand its existing Insider Threat capabilities, keeping information secure and cybersecurity standards up-to-date.

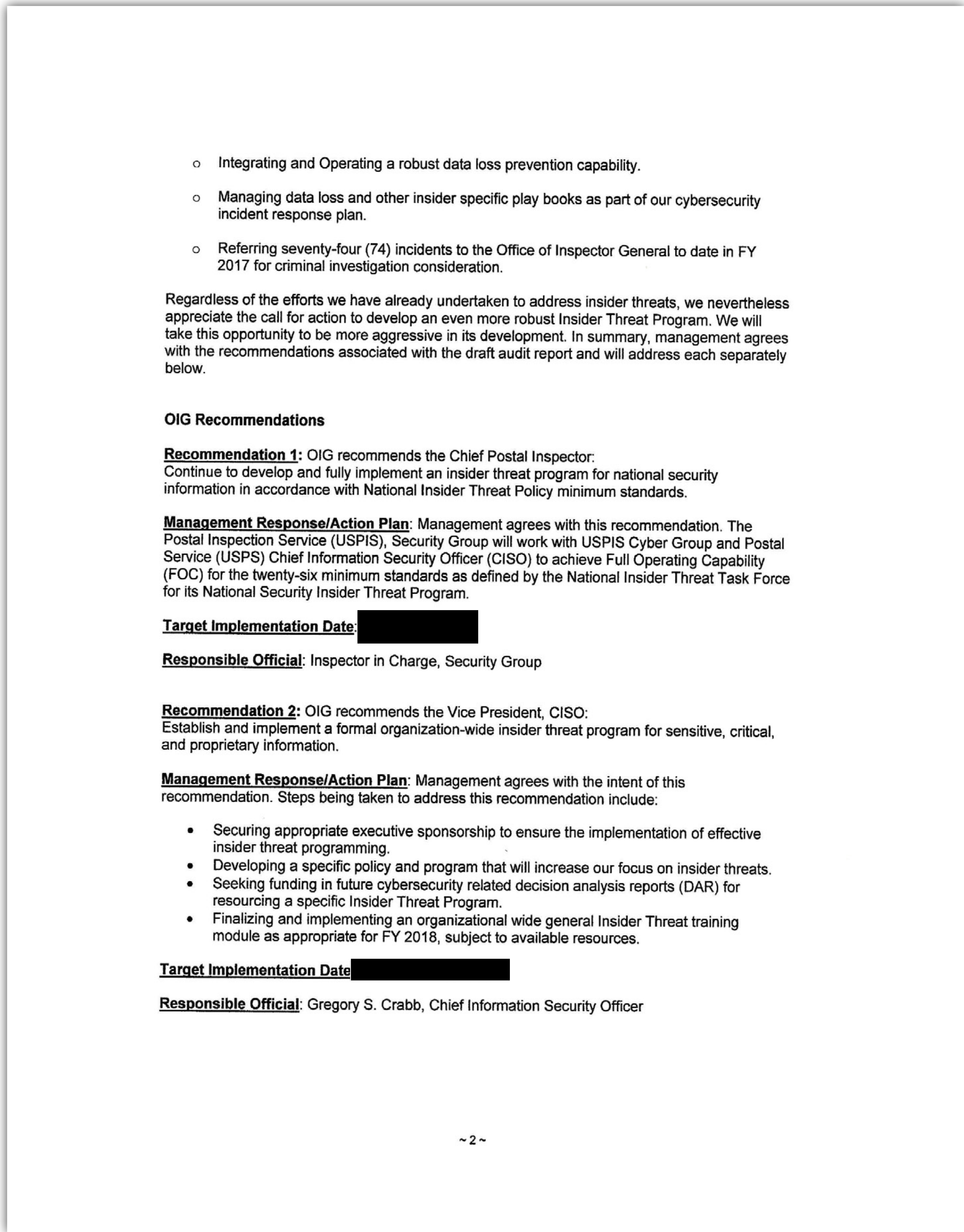
Management disagrees with the statement "…CISO focused their efforts on addressing external threats prior to establishing and implementing an insider threat program."

To the contrary, CISO has made concerted efforts to address all areas of threats related to information security, including insider threats. In managing our "all-threats view" of cybersecurity, CISO has used Carnegie Mellon University's (CMU) Insider Threat practice as a guide for the development of our program. CMU's Insider Threat practice defines nineteen (19) areas of focus for a strong information security program.

Although overall improvement and maturity continues in our cybersecurity program, CISO has already addressed insider threats by:

- Conducting annual training for more than 55,000 employees on the protection requirements for sensitive and sensitive-enhanced information.
- Certifying 35 CISO employees on Insider Threat practices through the CISO Academy.
- Maintaining a robust privileged identity and access management practice over our PCI and SOX systems.
- Archiving and reviewing 120 terabytes monthly/approximately 1.3 petabytes annually (last 365 days) of system log information for anomaly detection.

475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260-2100
WWW.POSTALINSPECTORS.USPIS.GOV



- Integrating and Operating a robust data loss prevention capability.
- Managing data loss and other insider specific play books as part of our cybersecurity incident response plan.
- Referring seventy-four (74) incidents to the Office of Inspector General to date in FY 2017 for criminal investigation consideration.

Regardless of the efforts we have already undertaken to address insider threats, we nevertheless appreciate the call for action to develop an even more robust Insider Threat Program. We will take this opportunity to be more aggressive in its development. In summary, management agrees with the recommendations associated with the draft audit report and will address each separately below.

OIG Recommendations

Recommendation 1: OIG recommends the Chief Postal Inspector:
Continue to develop and fully implement an insider threat program for national security information in accordance with National Insider Threat Policy minimum standards.

Management Response/Action Plan: Management agrees with this recommendation. The Postal Inspection Service (USPIS), Security Group will work with USPIS Cyber Group and Postal Service (USPS) Chief Information Security Officer (CISO) to achieve Full Operating Capability (FOC) for the twenty-six minimum standards as defined by the National Insider Threat Task Force for its National Security Insider Threat Program.

Target Implementation Date: [redacted]

Responsible Official: Inspector in Charge, Security Group

Recommendation 2: OIG recommends the Vice President, CISO:
Establish and implement a formal organization-wide insider threat program for sensitive, critical, and proprietary information.

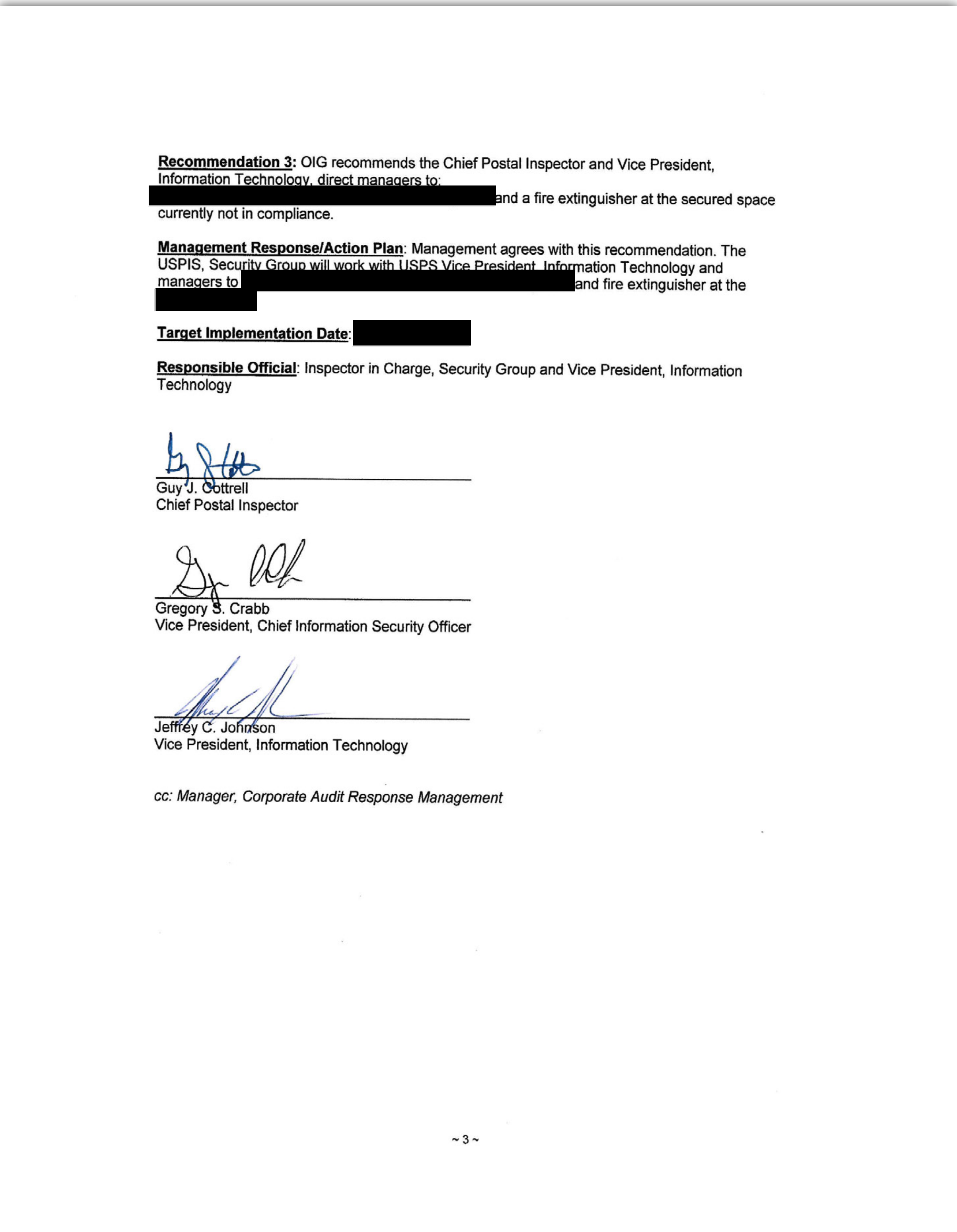
Management Response/Action Plan: Management agrees with the intent of this recommendation. Steps being taken to address this recommendation include:

- Securing appropriate executive sponsorship to ensure the implementation of effective insider threat programming.
- Developing a specific policy and program that will increase our focus on insider threats.
- Seeking funding in future cybersecurity related decision analysis reports (DAR) for resourcing a specific Insider Threat Program.
- Finalizing and implementing an organizational wide general Insider Threat training module as appropriate for FY 2018, subject to available resources.

Target Implementation Date [redacted]

Responsible Official: Gregory S. Crabb, Chief Information Security Officer

~ 2 ~



Recommendation 3: OIG recommends the Chief Postal Inspector and Vice President, Information Technology, direct managers to: [redacted] and a fire extinguisher at the secured space currently not in compliance.

Management Response/Action Plan: Management agrees with this recommendation. The USPIS, Security Group will work with USPS Vice President, Information Technology and managers to [redacted] and fire extinguisher at the [redacted]

Target Implementation Date: [redacted]

Responsible Official: Inspector in Charge, Security Group and Vice President, Information Technology

Guy J. Cottrell
Chief Postal Inspector

Gregory S. Crabb
Vice President, Chief Information Security Officer

Jeffrey C. Johnson
Vice President, Information Technology

cc: 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