Office of Audits
Office of Inspector General
U.S. General Services Administration

Audit of GSA's Insider Threat Program

Report Number A190016/I/T/F21002
February 17, 2021

Executive Summary

Audit of GSA's Insider Threat Program
Report Number A190016/I/T/F21002
February 17, 2021

Why We Performed This Audit

Insider threats involve employees using their authorized access, intentionally or unintentionally, to cause harm to an organization. Based on our assessment of the insider threat risks facing the General Services Administration (GSA), we included this audit in our *Fiscal Year 2018 Audit Plan*. Our objective was to assess whether GSA's Insider Threat Program (ITP) has controls in place to prevent, deter, detect, and mitigate actions by trusted insiders who represent a potential threat to Agency personnel, facilities, operations, and resources.

What We Found

We found that GSA's ITP does not consistently collaborate across the Agency to proactively prevent, detect, mitigate, and identify insider threats. For example, the ITP is unaware of and does not monitor insider threat risks from employees who receive termination proposals but retain access to GSA systems and facilities. Additionally, the ITP Senior Designated Official is failing to provide the annual insider threat report to the GSA Administrator as required.

We also found that the ITP does not effectively monitor insider threat risks related to separated and terminated employees. GSA faces heightened insider threat risks from these employees because it does not consistently deactivate their information technology accounts and recover and destroy Personal Identity Verification cards within required time frames.

Taken together, these deficiencies expose GSA information to theft or loss, facilities to damage, and personnel to actual or threatened harm; and create gaps that can be exploited in other ways to undermine GSA's ability to effectively carry out its operations.

What We Recommend

Based on our findings, we are making several recommendations to the GSA Deputy Administrator and the ITP Senior Designated Official. These recommendations include enhancing cross-organizational communication and collaboration with the ITP to improve information sharing and the ITP's access to insider-threat-related data. We also recommend that GSA improve oversight of the employee separation and termination process. A complete list of our recommendations is included in the ***Conclusion*** section of this report.

GSA agreed with our recommendations. GSA's comments are included in their entirety in ***Appendix B***.

Table of Contents

Introduction

We performed an audit of the General Services Administration's (GSA's) Insider Threat Program (ITP). The ITP is an Agency-wide program established to protect all GSA personnel, facilities, and automated systems from insider threats.

Purpose

We performed this audit as part of our *Fiscal Year 2018 Audit Plan*. GSA established an Agency-wide ITP within its Office of Mission Assurance (OMA) in 2014. Insider threats involve employees using their authorized access, intentionally or unintentionally, to cause harm to an organization. These threats can include espionage, terrorism, unauthorized disclosure of information, workplace violence, or the loss or degradation of Agency resources or capabilities.

Objective

Our objective was to assess whether GSA's ITP has controls in place to prevent, deter, detect, and mitigate actions by trusted insiders who represent a potential threat to Agency personnel, facilities, operations, and resources.

See ***Appendix A*** – Scope and Methodology for additional details.

Background

In October 2011, Executive Order 13587 required federal agencies to create insider threat programs and implement guidelines and standards developed by the Office of the Director of National Intelligence's National Insider Threat Task Force.[1] In November 2012, the National Insider Threat Task Force issued its *National Insider Threat Policy*, focused on strengthening and safeguarding federal agencies in order to counter insiders who may use their authorized access to compromise sensitive information. This policy incorporated requirements from Executive Order 13587 to develop insider threat detection and prevention programs to ensure responsible sharing and safeguarding of classified information on computer networks. GSA Order ADM 2400.1A, *Insider Threat Program*, also incorporates requirements from Executive Order 13556, which standardizes the way the executive branch handles and distributes unclassified information.[2]

The *National Insider Threat Policy* established 26 minimum standards for executive branch agencies' insider threat programs. Agencies are required to implement these minimum standards to receive a full operating capability designation. The National Insider Threat Task

[1] Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* (October 7, 2011).

[2] Executive Order 13556, *Controlled Unclassified Information* (November 4, 2010).

Force designates insider threat programs as having achieved full operating capability when programs, among other things:

- Operate in a proactive posture;
- Receive strong and active support from the agency head;
- Designate a senior official with direct access to the agency head on insider threat matters;
- Have access to multiple internal and external data sources to help with insider threat detection and prevention; and
- Create a culture of awareness about insider threats.

In response to these requirements, GSA established its ITP in 2014 as an Agency-wide program to protect all GSA personnel, facilities, and automated systems with classified and controlled unclassified information from insider threats. GSA's ITP reports to the ITP Senior Designated Official, who is the Associate Administrator of OMA. The ITP is a two-person team comprised of a coordinator and one staff member. GSA's *Insider Threat Program* order requires all GSA employees to comply with the applicable federal laws and policies concerning the responsible sharing and safeguarding of classified, controlled unclassified, and proprietary information directly acquired through GSA employment.

In November 2017, the National Insider Threat Task Force granted GSA's ITP the full operating capability designation, certifying that the program had successfully implemented the 26 minimum standards. Since receiving that designation, the ITP has primarily focused on developing mandatory Agency-wide insider threat training and monitoring employee foreign travel and foreign visitors. However, the National Insider Threat Task Force also recommends that insider threat programs actively monitor for other risks, including but not limited to removing access to information technology (IT) systems and federal buildings for separated and terminated employees.[3]

[3] Separated employees are those who are voluntarily leaving GSA. Terminated employees are those who have been involuntarily separated for disciplinary or performance reasons. Both separated and terminated employees are departing employees and can pose an insider threat risk to the Agency.

Results

We found that GSA's ITP does not consistently collaborate across the Agency to proactively prevent, detect, mitigate, and identify insider threats. For example, the ITP is unaware of and does not monitor insider threats arising from employees who receive termination proposals but retain access to GSA systems and facilities. Additionally, the ITP Senior Designated Official is failing to provide the annual insider threat report to the GSA Administrator as required.

We also found that the ITP does not effectively monitor insider threat risks related to separated and terminated employees. GSA faces heightened insider threat risks from these employees because it does not consistently deactivate their IT accounts and recover and destroy Personal Identity Verification (PIV) cards within required time frames.

Taken together, these deficiencies expose GSA information to theft or loss, facilities to damage, and personnel to actual or threatened harm; and create gaps that can be exploited to undermine GSA's ability to effectively carry out its operations.

Finding 1 – GSA's Insider Threat Program does not consistently collaborate across the Agency to proactively gather insider threat information and communicate risks with GSA staff offices and senior officials.

The *National Insider Threat Policy* requires the ITP to gather information from staff offices for analysis and to share its annual insider threat report with the agency head. Consistent collaboration across the Agency would lead to better information sharing and increase the ITP's effectiveness in identifying insider threats. However, we found that GSA's ITP does not consistently collaborate with other GSA staff offices to gather key threat information proactively and does not communicate insider threat risks and program challenges to the GSA Administrator as required. Instead, the ITP Senior Designated Official has taken a reactive approach that leaves GSA susceptible to insider threats.

The ITP Does Not Consistently Collaborate with GSA Staff Offices to Gather Insider Threat Information

The National Insider Threat Task Force's *Insider Threat Program: Maturity Framework* recommends that insider threat programs collaborate with staff offices to identify potential insider threats and reinforce a sense of shared responsibility in fulfilling the insider threat mission. GSA policy requires that the ITP Senior Designated Official establish and lead an Insider Threat Working Group, consisting of the Office of Human Resources Management (OHRM), Office of GSA IT, Office of the Chief Financial Officer (OCFO), and OMA. According to GSA policy, the GSA Insider Threat Working Group is required to consult on all ITP-related issues, conduct program oversight and reviews, and identify and make program resource recommendations.

Notwithstanding the requirement, the GSA Insider Threat Working Group chose to disband after GSA received its full operating capability designation from the National Insider Threat Task Force in November 2017. ITP staff stated that the working group was no longer necessary after receiving this designation. The ITP staff communicates with OHRM, Office of GSA IT, OCFO, and OMA to request specific information on potential threats only on an as-needed basis.

The decision to disband the GSA Insider Threat Working Group violated GSA policy. It also eliminated the ITP's only established means of formal collaboration with GSA's staff offices. In so doing, the ITP eliminated a method to collect valuable information and consult on insider-threat-related issues necessary to prevent, detect, and mitigate insider threats. Among other things, the ITP currently has limited or no information on employee suspensions, proposed employee terminations, physical security incidents, employee arrests, IT system access, and PIV card collection data. Absent this information, the ITP is unable to monitor for threats proactively, and is instead in a constant reactionary state.

For example, the ITP does not receive notice when GSA's services and staff offices initiate action to terminate an employee. GSA issues a Notice of Proposed Removal to these employees, after which the Agency cannot officially remove the employee for a period of at least 30 days to allow for due process.[4] During this interim period, these employees present a serious insider threat risk because they can exploit their knowledge of GSA and their continued access to systems and facilities to cause significant damage or harm.

The risks posed by these employees make it imperative to take appropriate measures to protect GSA interests. Carnegie Mellon University's *Common Sense Guide to Mitigating Insider Threats, Sixth Edition,* recommends proactively monitoring high-risk insiders by reviewing their IT system access activity for the 30 days prior to their last day of employment.

However, we found that the ITP was unaware of employees facing termination, and therefore took no action to coordinate proactive measures to monitor these employees for potential malicious IT account activity. For example, the ITP was unaware of termination proposals for employees whose misconduct posed significant insider threat risks. These employees faced termination for:

- Sexually harassing employees;
- Threatening to kill their supervisor and harm co-workers;
- Making false claims about their past criminal record to gain employment; and
- Altering official purchase documents.

In each instance, the IT account activity of these employees was not subject to additional monitoring after they received their Notices of Proposed Removal. The ITP's lack of awareness of these high-risk employees prevented the implementation of proactive measures to mitigate

[4] GSA can issue Notice of Proposed Removal letters to employees as a penalty for repeated violations or offenses or for one or more offenses involving serious misconduct or delinquency.

any potential damage to GSA. This demonstrates the need to reconstitute the GSA Insider Threat Working Group as required by GSA policy in order to provide the ITP with timely and reliable information for use in proactively addressing insider threats.

The ITP Does Not Communicate with the GSA Administrator as Required

The ITP does not communicate insider threat risks and program challenges to the GSA Administrator as required by the *National Insider Threat Policy*. The *National Insider Threat Policy* requires that insider threat programs issue an annual report to the agency head. Annual reports should include annual accomplishments, resources allocated, insider threat risks to the agency, recommendations and goals for program improvement, and major challenges. Additionally, GSA's *Insider Threat Program* order requires the reporting of all ITP issues to the GSA Administrator.

However, we found that the ITP has not submitted an annual report to the GSA Administrator since Fiscal Year 2016. While the ITP prepares an annual report and submits it to the ITP Senior Designated Official, the ITP Senior Designated Official told us that he does not submit the annual reports to the GSA Administrator as required. Instead, he discusses insider threat topics with the GSA Deputy Administrator, such as when cases involving GSA are referred to the Federal Bureau of Investigation. Further, the ITP Senior Designated Official stated that he does not share the annual reports outside the ITP due to the sensitive nature of the program.

The ITP's failure to provide the annual report deprives the GSA Administrator of information necessary to provide effective oversight of the Agency's ITP. For example, the 2017, 2018, and 2019 annual reports highlighted significant program challenges, including the need for the ITP to more proactively monitor for insider threats. The reports also cited challenges to proactive monitoring arising from budget and staffing constraints, and the ITP's limited ability to view an employee's IT account activity without involving "several sections within GSA IT."

Additionally, both the 2018 and 2019 annual reports conclude that it is critical for GSA to strengthen its insider threat capability. For instance, the 2019 annual report provides that:

> Without a robust insider threat capability, GSA could be exposing itself to potential foreign intelligence collection, trusted insider exploitation and other evolving threats to personnel, programs and infrastructure that are critical to the GSA and our national security.

As shown above, the annual reports contain vital information that could be used by the GSA Administrator to address challenges facing the ITP and strengthen GSA's insider threat posture. In sum, improving collaboration with Agency staff offices will allow the ITP to proactively obtain insider-threat-related data and improve its ability to prevent, detect, monitor, and identify insider threats. Additionally, addressing and submitting ITP annual reports to the GSA Administrator will ensure that leadership is aware of program accomplishments, challenges, and limitations. To address these deficiencies, GSA should establish group collaboration and individual communication with GSA staff offices and submit its annual report to the GSA Administrator.

Finding 2 – GSA's Insider Threat Program does not effectively monitor insider threat risks relating to separated and terminated employees.

The National Insider Threat Task Force's government best practices notes that it is critical to monitor and mitigate insider threat risks related to separated and terminated employees because "an insider can do just as much damage in the 30 to 90 days after leaving as in the time prior to departure."[5] However, we found that the ITP's process to monitor insider threat risks related to separated and terminated employees is ineffective and is compounded by GSA's failure to consistently deactivate IT accounts for these employees and to recover and destroy their PIV cards. Taken together, these deficiencies hinder the ITP's ability to protect GSA from insider threat risks.

The ITP's procedures for monitoring separated and terminated employees consist of a limited review of monthly lists of employees who have left the Agency. ITP personnel stated that their reviews are limited to those employees with a security clearance because the ITP does not have sufficient staffing to perform more comprehensive assessments. They also told us that threats from separated and terminated employees are minimal because these employees have already left the Agency.

However, separated and terminated employees can exploit their knowledge of the Agency to cause significant damage or harm, making it important for the ITP to have robust procedures in place to monitor and mitigate these insider threats. As described below, the ITP's need for effective monitoring procedures is made more critical because GSA is not consistently deactivating separated and terminated employees' IT account access and collecting and destroying their PIV cards.

Deactivation of IT Account Access

When an employee leaves an agency, it is critically important to deactivate their IT accounts to protect systems and data from unauthorized access. Accordingly, federal IT security standards, including those established by the National Institute of Standards and Technology, require agencies to deactivate IT account access for separated and terminated employees in a timely manner. In accordance with this requirement, the GSA IT Security Procedural Guide, *Termination and Transfer*, CIO-IT Security-03-23, Revision 4, requires that the Office of GSA IT deactivate IT account access within 24 hours after it receives a help desk ticket indicating the employee's last day.

However, GSA is not deactivating IT account access within the required time frames. We sampled 89 GSA employees who were separated or terminated between October 1, 2018, and

[5] *Protect your Organization from the Inside Out: Government Best Practices* (2016).

September 30, 2019. For 59 of the 89 employees in our sample, the employee's IT account was deactivated an average of 14 days after the last day of employment. In one instance, an employee's IT account was not deactivated for 136 days after their last day of employment. Our analysis showed that the majority of accounts were not deactivated as required because supervisors failed to submit help desk tickets to deactivate the employees' IT accounts in a timely manner.

When IT accounts for separated and terminated employees are not deactivated in a timely manner, GSA operations and resources are at risk from insider threats. A separated or terminated employee could misuse GSA vendor information, pricing strategies, proprietary formulas and processes, and critical infrastructure and facilities information. Without visibility into IT account deactivation for separated and terminated employees, the ITP cannot detect and prevent potential insider threats. While the ITP is not responsible for IT account deactivation, GSA must ensure that IT account access is deactivated within required time frames and that the ITP is positioned to monitor IT account deactivation to proactively mitigate potential threats.

Recovery and Destruction of PIV Cards

GSA uses PIV cards as the primary means of identification to access physically secured federal areas and IT systems. The proper control and disposal of these cards is critical to properly protect GSA buildings and IT systems from unauthorized access that could place employees, data, and facilities at risk. Federal Information Processing Standards Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, requires federal agencies to recover and destroy PIV cards for separated and terminated employees.

Within GSA, OMA is responsible for destroying PIV cards that are no longer required, including PIV cards belonging to separated and terminated employees. However, we found that OMA did not receive or destroy PIV cards by the last day of employment for 76 of the 89 employees in our sample. While OMA eventually received and destroyed PIV cards for 55 of these employees, it did not receive or destroy PIV cards for the remaining 21 employees. In the majority of these 21 instances, OMA informed us that "the employee never turned in the card or someone did not provide the card to us," but did not provide evidence that it took any additional actions to recover the card.

Separated and terminated employees can potentially use unrecovered PIV cards to access GSA facilities and information. While the ITP is not responsible for PIV card collection and destruction, it is critical for the ITP to monitor and mitigate risks arising from this process. The ITP's involvement is especially important when employees have been terminated for misconduct or lapses in judgement that make them more likely to cause intentional or unintentional harm to GSA and its employees. For example, we found that OMA did not recover a PIV card from a terminated employee who sexually harassed federal employees and mixed medications and alcohol while working on site. In another example, a GSA building manager, who worked at a federal courthouse and was terminated for falsifying information to obtain employment, refused to return their PIV card to OMA. In both instances, the ITP was unaware of the individual or the insider threat risk they posed to GSA personnel, facilities, operations, and resources.

OMA officials stated that there are challenges to recovering and destroying PIV cards in a timely manner. For example, they stated that supervisors are not submitting PIV cards for destruction. They also stated that OMA cannot force separated employees to return their PIV cards. Nonetheless, the insider threat risk posed by unrecovered PIV cards makes it critical that GSA and OMA work in concert with the ITP to ensure PIV cards are recovered in a timely manner. The ITP also needs to monitor and mitigate insider threat risks arising from unrecovered PIV cards.

As demonstrated above, the ITP is not effectively monitoring insider threat risks posed by separated and terminated employees. The ITP's lack of awareness, coupled with GSA's poor management of IT systems access and PIV card collection and destruction for separated and terminated employees, exposes the Agency to significant insider threat risks. Accordingly, GSA should improve its processes for separated and terminated employees to ensure that it deactivates IT accounts and recovers and destroys PIV cards in a timely manner.

The ITP should establish a comprehensive approach to monitor and protect GSA from insider threat risks arising from separated and terminated employees. In doing so, GSA should ensure that the ITP is aware of risks associated with contract employees, as identified in our recent audit of contractor PIV cards. In November 2020, we reported that GSA is mismanaging PIV cards issued to contract employees.[6] As a result, GSA could not account for thousands of PIV cards issued to these employees, including cards issued to contract employees who failed background checks. Increasing the ITP's awareness of threats arising from both employees and contractors will enable GSA to more effectively protect the Agency and its resources.

[6] *GSA's Mismanagement of Contract Employee Access Cards Places GSA Personnel, Federal Property, and Data at Risk* (Report Number A190085/A/6/F21001, November 4, 2020).

Conclusion

We found that GSA's ITP does not consistently collaborate across the Agency to proactively prevent, detect, mitigate, and identify insider threats. For example, the ITP is unaware of and does not monitor insider threat risks from employees who receive termination proposals but retain access to GSA systems and facilities. Additionally, the ITP Senior Designated Official is failing to provide the annual insider threat report to the GSA Administrator as required.

We also found that the ITP does not effectively monitor insider threat risks relating to separated and terminated employees. GSA faces heightened insider threat risks from these employees because it does not consistently deactivate their IT accounts and recover and destroy PIV cards within required time frames.

Taken together, these deficiencies expose GSA information to theft or loss, facilities to damage, and personnel to actual or threatened harm; and create gaps that can be exploited in other ways to undermine GSA's ability to effectively carry out its operations. Accordingly, the ITP should improve coordination across the Agency and fulfill its annual reporting requirements. The ITP should also establish controls to effectively monitor the separation and termination process.

Recommendations

We recommend the GSA Deputy Administrator and the ITP Senior Designated Official establish effective controls to:

1. Enhance cross-organizational communication and collaboration with the ITP by:

    a. Re-establishing consistent group collaboration with OHRM, Office of GSA IT, OCFO, OMA, and other relevant offices to consult on broader, non-case-specific, insider-threat-related issues.

    b. Identifying insider threat information, including but not limited to employee suspensions, proposed employee terminations, IT system access, and PIV card collection data maintained by OHRM, Office of GSA IT, OCFO, OMA, and other relevant offices. Reassess this information on an ongoing basis.

    c. Establishing a method for the ITP to proactively and consistently receive insider threat information from OHRM, Office of GSA IT, OCFO, OMA, and other relevant offices.

    d. Submitting ITP annual reports to the GSA Administrator in accordance with the *National Insider Threat Policy*.

2. Enhance oversight of the employee separation and termination processes by:

    a. Establishing procedures that ensure the ITP is informed and aware of insider threat risks posed by separated and terminated employees. Among other things, the ITP must be notified when GSA employees' and contractors' IT accounts have not been deactivated within 24 hours of their last day of employment and their PIV cards have not been recovered and destroyed in accordance with Federal Information Processing Standards Publication 201-2.
    b. Enhancing procedures to monitor separated and terminated employees' IT account activity prior to and after the last day of employment. Consult with the Office of General Counsel as needed.
    c. Establishing roles and responsibilities to ensure oversight of the employee separation and termination process.
    d. Establishing a policy for supervisors to collect and submit separated and terminated employees' PIV cards to OMA for destruction within a required time frame.
    e. Establishing procedures that account for the collection of separated and terminated employees' PIV cards, including the date GSA collects the PIV card.
    f. Exhausting efforts to collect and destroy the 21 PIV cards from our sample that OMA did not destroy. Additionally, OMA should identify, collect, and destroy the PIV cards of other separated and terminated employees whose cards were not collected.

GSA Comments

GSA agreed with our recommendations. GSA's comments are included in their entirety in ***Appendix B***.

Audit Team

This audit was managed out of the Acquisition and Information Technology Audit Office and conducted by the individuals listed below:

Sonya D. Panzo	Associate Deputy Assistant Inspector General for Auditing
Kyle D. Plum	Audit Manager
Victor R. Pimentel	Auditor-In-Charge
James W. Dean	Management Analyst

Appendix A – Scope and Methodology

Our audit assessed the effectiveness of GSA's ITP. We examined the ITP's coordination across GSA and its involvement in the employee separation and termination process. We also tested when separated and terminated employees' PIV cards were collected and when their IT account access was removed. For purposes of this audit, we focused on GSA's controls related to unclassified information due to the audit team's security access limitations.

To accomplish our objective, we:

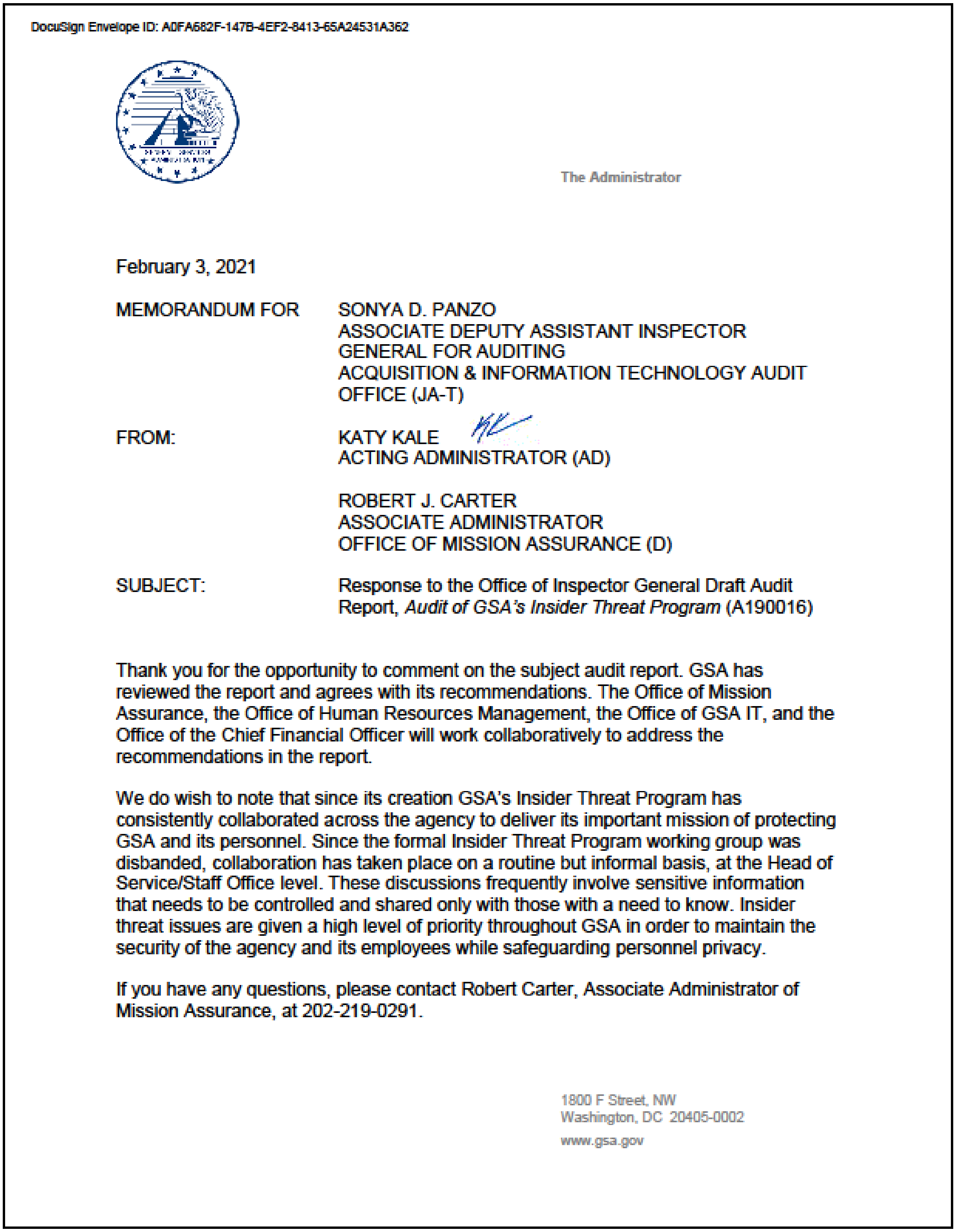
- Reviewed insider threat policies, standards, and best practices developed by the National Insider Threat Task Force, GSA, and other applicable sources;
- Reviewed GSA orders, instructional letters, and guidance; Executive Orders, National Institute of Standards and Technology special publications; and Carnegie Mellon University's *Common Sense Guide to Mitigating Insider Threats, Sixth Edition*;
- Reviewed GSA procedural guidance related to the employee separation and termination process;
- Requested and reviewed employee separation and termination data, including termination letters, PIV card collection data, and GSA IT account deactivation data for the employees in our sample;
- Tested GSA's timeliness in deactivating IT account access and collecting PIV cards for our sample of 89 employees departing GSA between October 2018 and September 2019. Specifically, we analyzed:
    - The entire population of 29 involuntarily separated employees during Fiscal Year 2019. We reduced our testing population to 20 individuals due to anomalies with the termination process. Removal of these anomalies did not affect the audit team's ability to form conclusions.
    - A statistical sample of 35 of 798 voluntarily separated employees. The sampling plan provided a 95 percent confidence level. We reduced our testing sample size to 34 individuals due to an anomaly with the separation process. Removal of this anomaly did not affect the audit team's ability to form conclusions.
    - The entire population of 41 voluntarily separated employees due to expiration of appointment in Fiscal Year 2019. We reduced our testing population to 35 individuals due to anomalies with the separation process. Removal of this anomaly did not affect the audit team's ability to form conclusions.
- Interviewed personnel from ITP, Office of GSA IT, OHRM, and OMA, including individuals from the Office of Personnel Security and Office of Physical Security.

We conducted the audit between October 2018 and August 2020 in accordance with generally accepted government auditing standards. 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 objective.

Internal Controls

Our assessment of internal controls was limited to those necessary to address the objective of the audit.

Appendix B – GSA Comments



DocuSign Envelope ID: A0FA682F-147B-4EF2-8413-65A24531A362

The Administrator

February 3, 2021

MEMORANDUM FOR SONYA D. PANZO
ASSOCIATE DEPUTY ASSISTANT INSPECTOR
GENERAL FOR AUDITING
ACQUISITION & INFORMATION TECHNOLOGY AUDIT
OFFICE (JA-T)

FROM: KATY KALE
ACTING ADMINISTRATOR (AD)

ROBERT J. CARTER
ASSOCIATE ADMINISTRATOR
OFFICE OF MISSION ASSURANCE (D)

SUBJECT: Response to the Office of Inspector General Draft Audit Report, *Audit of GSA's Insider Threat Program* (A190016)

Thank you for the opportunity to comment on the subject audit report. GSA has reviewed the report and agrees with its recommendations. The Office of Mission Assurance, the Office of Human Resources Management, the Office of GSA IT, and the Office of the Chief Financial Officer will work collaboratively to address the recommendations in the report.

We do wish to note that since its creation GSA's Insider Threat Program has consistently collaborated across the agency to deliver its important mission of protecting GSA and its personnel. Since the formal Insider Threat Program working group was disbanded, collaboration has taken place on a routine but informal basis, at the Head of Service/Staff Office level. These discussions frequently involve sensitive information that needs to be controlled and shared only with those with a need to know. Insider threat issues are given a high level of priority throughout GSA in order to maintain the security of the agency and its employees while safeguarding personnel privacy.

If you have any questions, please contact Robert Carter, Associate Administrator of Mission Assurance, at 202-219-0291.

1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov

Appendix C – Report Distribution

Acting GSA Administrator (A)

GSA Chief of Staff (AC)

GSA Deputy Administrator (AD)

Associate Administrator for Mission Assurance (D)

Deputy Associate Administrator for Mission Assurance (D1)

Chief of Staff for Mission Assurance (D2)

Personnel Security Division Director (DBA)

Personnel Security Division Deputy Director, Security Programs Branch (DBAC)

Chief Financial Officer (B)

Office of Audit Management and Accountability (BA)

Assistant Inspector General for Auditing (JA)

Director, Audit Planning, Policy, and Operations Staff (JAO)