



Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

Audit Report

Physical Security at Offices

042318 July 2025



Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: July 29, 2025

Refer to: 042318

To: Frank Bisignano
Commissioner

From: Michelle L. Anderson *Michelle L. Anderson*
Acting Inspector General

Subject: Physical Security at Offices

The attached final report presents the results of the Office of Audit's review. The objective was to determine whether the Social Security Administration monitored and resolved physical security issues identified during inspections of Agency offices.

If you wish to discuss the final report, please contact Jeffrey Brown, Deputy Assistant Inspector General for Audit.

Attachment

Physical Security at Offices

042318



July 2025

Office of Audit Report Summary

Objective

To determine whether the Social Security Administration (SSA) monitored and resolved physical security issues identified during inspections of SSA offices.

Background

SSA employees provide a broad range of services for the public through a nation-wide network of offices. While providing these services, employees may be exposed to physical security risks. To help protect employees and equipment, SSA offices are periodically inspected for physical security risks.

SSA's Office of Security and Emergency Preparedness (OSEP) is responsible for managing, implementing, and monitoring SSA's physical security program nationwide. OSEP uses the Federal Protective Service (FPS) to inspect all SSA offices to satisfy the Interagency Security Committee's (ISC) Federal standard for periodic inspections. OSEP conducts additional inspections on SSA's highest risk offices for unique Agency risks.

OSEP and FPS report physical security issues they find and recommend corrective actions to office management. Office managers must remediate the findings within 180 days or request extensions, when needed.

We obtained data for 1,517 offices open anytime between Fiscal Years 2018 and 2023. We reviewed a random sample of 100 offices.

Results

SSA did not always monitor and resolve physical security issues identified during inspections. OSEP did not ensure its offices received mandatory inspections, as required by the ISC's Federal standard. OSEP did not coordinate with FPS on inspection coverage or monitor FPS' inspection findings at SSA's offices. OSEP also did not have a complete list of all SSA offices that FPS should have inspected. As such, SSA could not monitor which offices FPS inspected and when those inspections occurred. In addition, without access to FPS' inspection findings, OSEP could not determine the effect those findings had on an office's physical security nor properly identify SSA's highest risk offices for its additional inspections. Although OSEP's stated responsibilities included managing, implementing, and monitoring SSA's physical security program, OSEP's policy did not require that it monitor FPS' inspections.

Despite having policy that required OSEP to monitor field office managers' actions to address OSEP's inspection findings, OSEP's procedures for implementing the policy should be strengthened. OSEP did not ensure field office managers took appropriate actions to resolve the security findings, nor did OSEP adequately monitor unresolved findings to ensure timely resolution in accordance with its policy. Of the 231 security findings we reviewed, office managers

- incorrectly marked 101 (44 percent) as resolved without properly implementing OSEP's corrective actions and
- did not resolve 125 (54 percent) within the required 180 days nor did they request extensions.

Some delays in resolving findings were unavoidable, including COVID-related closures. Other delays were not, such as when managers documented no action for several months or years despite receiving automated weekly reminders from OSEP. Unresolved findings can leave offices unnecessarily exposed to higher levels of security risk.

Recommendations

We made seven recommendations for SSA to strengthen its physical security program. SSA agreed to implement our recommendations.

TABLE OF CONTENTS

Objective	1
Background	1
Physical Security Assessments	1
Remediating Inspection Issues	2
Scope and Methodology	3
Results of Review	4
Access to Physical Security Inspections	4
Corrective Actions	5
Unresolved Security Findings	6
Conclusion	7
Recommendations	7
Agency Comments.....	7
Appendix A – Scope and Methodology.....	A-1
Appendix B – Agency Comments	B-1

ABBREVIATIONS

AIMS	Administrative Instructions Manual System
C.F.R.	Code of Federal Regulations
DHS	Department of Homeland Security
FPS	Federal Protective Service
FSL	Facility Security Level
GAO	Government Accountability Office
ISC	Interagency Security Committee
OSEP	Office of Security and Emergency Preparedness
SAFE	Security Automated Features and Enhancements
SSA	Social Security Administration
U.S.C.	United States Code

OBJECTIVE

To determine whether the Social Security Administration (SSA) monitored and resolved physical security issues identified during inspections of SSA offices.

BACKGROUND

SSA employees provide a broad range of services for the public through a nation-wide network of offices.¹ While providing these services, employees may be exposed to physical security risks unique to the Agency. Federal statutes and regulations authorize legal actions such as fines, imprisonment,² and banning from offices³ to those who threaten SSA employees and their families. Nonetheless, employees are still vulnerable to acts of harassment and violence from visitors while carrying out their duties. To mitigate these risks, SSA offices undergo physical security assessments and office managers remediate safety issues.

Physical Security Assessments

SSA's Office of Security and Emergency Preparedness (OSEP) manages, implements, and monitors SSA's physical security program nationwide. OSEP and the Department of Homeland Security's (DHS) Federal Protective Service (FPS) periodically assess the security risks of all SSA offices.⁴ During these assessments, OSEP and FPS quantify an office's characteristics and vulnerabilities.⁵ This includes an assessment of the office's size and employee count as well as the area crime rate.⁶ The results of these assessments determine an office's Facility Security Level (FSL),⁷ which ranges from I to V.⁸ A smaller office with few employees in an area that has a low crime rate may be assessed a lower FSL of I or II, while a larger office with many employees in an area with a high crime rate may be assessed a higher FSL of III or IV.⁹ SSA does not have offices with an FSL of V.

¹ SSA, *Social Security Administration (SSA) Annual Data for Field Office Visitors (Daily Average)*, ssa.gov (April 14, 2025) and SSA, *Annual Statistical Supplement-2023*, Table 2.F1 (November 2023).

² 42 U.S.C. § 1320a (8b).

³ 20 C.F.R. chapter 3, § 422.901.

⁴ Interagency Security Committee (ISC), Executive Order No. 12,977, 60 Fed. Reg. 54,411 (October 24, 1995); SSA, *AIMS, General Administration Manual*, ch. 10.06, sec. 10.06.05 (February 28, 2025).

⁵ DHS, *The Risk Management Process: An Interagency Security Committee Standard*, sec. 8.1.2 (July 2024).

⁶ DHS, *The Risk Management Process: An Interagency Security Committee Standard*, sec. 8.1.3.3-8.1.3.5 (July 2024).

⁷ DHS, *The Risk Management Process: An Interagency Security Committee Standard*, sec. 8.1.2 (July 2024).

⁸ DHS, *The Risk Management Process: An Interagency Security Committee Standard*, sec. 8.1.1 (July 2024).

⁹ DHS, *The Risk Management Process: An Interagency Security Committee Standard*, sec. 8.1.3.3-8.1.3.5 (July 2024).

Per the ISC's Federal standard, OSEP and FPS use each office's FSL to establish the office's security requirements.¹⁰ The office's FSL determines how frequently OSEP and FPS inspect an office for physical security risks. An office with an FSL of I or II must be inspected every 5 years; offices with an FSL of III, IV, or V must be inspected every 3 years.¹¹ FPS periodically inspects all SSA offices as required by their FSL.¹² SSA uses FPS' inspections to satisfy the ISC's Federal standard for periodic inspections.¹³ FPS schedules and conducts its inspections independently from OSEP and does not provide forecasted inspection dates to OSEP.

OSEP conducts additional inspections on SSA's highest risk and most vulnerable offices¹⁴ to fulfill minimum security standards for Agency employees and property. In addition to reviewing Federal security requirements, OSEP reviews offices' vulnerability to unique Agency security issues.¹⁵ These issues include whether impact-resistant windows separate employees from visitors or items in the waiting room, such as flagpoles and chairs, are secured. These measures help protect employees from visitors who may attempt to damage or break the windows or make physical contact with employees.

Remediating Inspection Issues

OSEP and FPS report any physical security issues they find and recommend corrective actions to office management for remediation. OSEP or FPS then monitors how the office remediates their findings. After OSEP inspects an office, it discusses its findings with the office's management.¹⁶ OSEP then records the findings in its security application¹⁷ and prepares a formal report. Office management must address each finding and update the application. If management does not update their progress for 30 days, the application sends offices automated reminders weekly. Office managers must remediate the findings within 180 days or request extensions, when needed.¹⁸ After an office manager remediates a finding, they change its status to "Resolved," and applicable users are notified via email.¹⁹ If office management cannot timely remediate a finding, they may request extensions within the application. If office management disagrees with OSEP's suggested corrective actions, they must discuss alternatives with OSEP before they resolve the finding.²⁰ If office management cannot

¹⁰ DHS, *The Risk Management Process: An Interagency Security Committee Standard*, sec. 8.1.8 (July 2024).

¹¹ DHS, *The Risk Management Process: An Interagency Security Committee Standard*, sec. 8.1.1 (July 2024).

¹² SSA, *AIMS, General Administration Manual*, ch. 10.06, sec. 10.06.05 (B) (February 28, 2025).

¹³ SSA, *AIMS, General Administration Manual*, ch. 10.06, sec. 10.06.05 (E.1) (February 28, 2025).

¹⁴ SSA's highest risk and most vulnerable offices include those with a higher risk FSL or offices whose area crime rate has increased since their last OSEP or FPS inspection. SSA, *AIMS, General Administration Manual*, ch. 10.06, sec. 10.06.05 (E.1) (February 28, 2025).

¹⁵ SSA, *AIMS, General Administration Manual*, ch. 10.06, sec. 10.06.05 (A) (February 28, 2025).

¹⁶ SSA, *AIMS, General Administration Manual*, ch. 10.06, sec. 10.06.05 (E.1) (February 28, 2025).

¹⁷ SSA, *Remediation User Guide, Security Automated Features and Enhancements (SAFE)*, (January 9, 2025).

¹⁸ SSA, *AIMS, General Administration Manual*, ch. 10.06, sec. 10.06.05 (E.1) (February 28, 2025).

¹⁹ SSA, *Remediation User Guide, Security Automated Features and Enhancements (SAFE)*, pp. 26 and 27 (January 9, 2025).

²⁰ SSA, *AIMS, General Administration Manual*, ch. 10.06, sec. 10.06.05 (E.1) (February 28, 2025).

remediate a finding and must accept the underlying security risk as is, OSEP should maintain documentation of the office's risk acceptance.²¹ OSEP's guidance informs managers that, if a manager resolves a finding without implementing corrective actions, that manager assumes the security risk posed by the unaddressed finding on the Agency's behalf.²²

Office managers can request funds from OSEP to help remediate security findings.²³ In some cases, remediation of a physical security issue may not be possible because of such factors as funding. In these cases, the ISC suggests implementing interim security measures²⁴ given the real threat to Federal offices and serious consequences to employees.²⁵

The Government Accountability Office (GAO) reported that FPS recorded 70 percent of approved recommendations closed and not implemented. The interviewed representatives identified several factors, including cost and available funding or budgetary considerations, that contributed to Federal agencies not implementing recommendations.²⁶

SCOPE AND METHODOLOGY

To accomplish our objective, we obtained data for 1,517 offices open for business anytime between Fiscal Years 2018 and 2023 (see Table 1). We separated the offices into two populations based on their FSL. We reviewed a random sample of 50 offices with an FSL of I or II and 50 offices with an FSL of III or IV to determine whether SSA monitored and resolved the 231 physical security issues identified during office inspections. We also interviewed managers from 10 different offices. We judgmentally selected five offices from each of our two populations whose inspection reports contained multiple security findings. See Appendix A for more information on our audit scope and methodology.

Table 1: Office Populations and Sample Sizes

FSL	Population Size	Sample Size
I or II	1,374	50
III or IV	143	50
Total Offices	1,517	100

²¹ DHS, *The Risk Management Process: An Interagency Security Committee Standard*, sec. 5.3 (July 2024).

²² SSA, *Remediation User Guide, Security Automated Features and Enhancements (SAFE)*, p. 26 (January 9, 2025); DHS, *The Risk Management Process: An Interagency Security Committee Standard*, sec. 8.4.2-8.4.3 (July 2024).

²³ SSA, *AIMS, General Administration Manual*, ch. 10.06, sec. 10.06.06 (February 28, 2025).

²⁴ DHS, *The Risk Management Process: An Interagency Security Committee Standard*, sec. 8.4.4 (July 2024).

²⁵ DHS, *The Risk Management Process: An Interagency Security Committee Standard*, sec. 8.4.1 (July 2024).

²⁶ GAO, *Federal Facilities: Improved Oversight Needed for Security Recommendations*, GAO-23-105649, pp. 8 through 11 (May 2023).

RESULTS OF REVIEW

SSA did not always monitor and resolve physical security issues identified during inspections. OSEP did not ensure its offices received mandatory inspections, as required by the ISC's Federal standard. OSEP did not coordinate with FPS on inspection coverage or monitor FPS' inspection findings at SSA's offices. OSEP also did not have a complete list of all SSA offices that FPS should have inspected. As such, SSA could not monitor which offices FPS inspected and when inspections occurred. In addition, without access to FPS' inspection findings, OSEP could not determine the effect findings had on an office's physical security nor properly identify SSA's highest risk offices for its additional inspections. Although OSEP's stated responsibilities included managing, implementing, and monitoring SSA's physical security program, OSEP's policy did not require it to monitor FPS' inspections.

Despite having policy requiring OSEP to monitor field office managers' actions to address OSEP's inspection findings, OSEP's procedures for implementing the policy should be strengthened. OSEP did not ensure field office managers took appropriate actions to resolve the security findings, nor did OSEP adequately monitor unresolved findings to ensure timely resolution in accordance with its policy. Of the 231 security findings we reviewed, office managers

- incorrectly marked 101 (44 percent)²⁷ as resolved without properly implementing OSEP's corrective actions and
- did not resolve 125 (54 percent)²⁸ within the required 180 days nor did they request extensions.

Some delays in resolving findings were unavoidable, including COVID-related closures.²⁹ Other delays were not, such as when managers documented no action for several months or years despite receiving automated weekly reminders from OSEP. Unresolved findings can leave offices unnecessarily exposed to higher levels of security risk.

Access to Physical Security Inspections

OSEP did not have full oversight of SSA physical security inspections. OSEP's policy states SSA meets the Federal standard for inspections by using FPS to inspect all its offices.³⁰ OSEP's *Physical Security Handbook* also states it should coordinate with FPS while directing its physical security program.³¹ However, neither the *Handbook* nor OSEP's policy require that OSEP monitor FPS' inspections. At the time of our audit, OSEP did not have access to FPS' inspections and therefore OSEP could not ensure its offices were inspected to the Federal

²⁷ We did not identify improperly resolved findings in the remaining 130 findings we reviewed.

²⁸ We did not identify improperly resolved findings in the remaining 106 findings we reviewed.

²⁹ On March 18, 2020, SSA responded to the COVID-19 pandemic by limiting in-person services. By April 2020, SSA had assigned more than 90 percent of its employees to full-time remote work. Most employees did not return to the office before March 30, 2022, and SSA did not resume in-person services until April 7, 2022.

³⁰ SSA, *AIMS, General Administration Manual*, ch. 10.06, sec. 10.06.05 (E.1) (February 28, 2025); DHS, *The Risk Management Process: An Interagency Security Committee Standard*, sec. 8.1.1 (July 2024).

³¹ SSA, *Physical Security Handbook*, sec. 3.B.1 (November 11, 2023).

standard nor whether actions were taken to address FPS' findings.³² OSEP also could not provide us a list that (1) included all SSA offices that should have been inspected by FPS and (2) had been reconciled to the official list of SSA's offices.^{33,34}

Without oversight of FPS' inspection findings and a complete list of offices, OSEP could not ensure it could identify and inspect SSA's highest risk and most vulnerable offices. OSEP's policy also requires on-site inspections of 10 percent of offices inspected by FPS in the prior fiscal year.³⁵ OSEP could not meet this requirement since it did not know which offices FPS had inspected.

During our review, OSEP obtained access to FPS' inspection information. OSEP can use these inspections to ensure Agency compliance with ISC Federal requirements and its own policy. OSEP is also upgrading its physical security applications to include FPS' inspection information so it may oversee FPS' inspections and findings. SSA stated this system upgrade should further strengthen OSEP's oversight of offices' physical security needs.

Corrective Actions

Office managers marked as resolved 101 (44 percent) of the 231 sampled security findings without implementing OSEP's corrective actions.³⁶ This occurred because OSEP did not ensure office managers took appropriate actions to resolve these security findings. Office managers can mark findings as resolved in OSEP's security application without implementing any corrective actions. OSEP's policy instructs office managers to remediate each finding and discuss any disagreements or alternative corrective actions with OSEP,³⁷ but the policy does not require that office managers document or support their corrective actions when marking findings as resolved. As such, office managers did not always document their actions, which made it more challenging for OSEP to ensure office managers properly resolved findings. However, according to policy, OSEP should monitor whether corrective actions were implemented and, if not, the reason they were not implemented.³⁸ Despite having policy requiring that OSEP monitor field office managers' actions to address OSEP's inspection findings, OSEP's procedures for implementing the policy could be strengthened.

³² GAO found Federal agencies were not implementing approved recommendations identified by FPS inspections. GAO, *Federal Facilities: Improved Oversight Needed for Security Recommendations*, GAO-23-105649, pp. 7 and 8 (May 2023).

³³ SSA, *Detailed Office/Organization Resource System Web Application User Guide*, version 1.13, ch. 2.1 (June 13, 2024).

³⁴ A sampled OSEP physical security inspection identified an additional SSA-occupied office space that was not recorded in its list of offices. SSA's official list of its offices included this office space. OSEP did not identify or schedule this office for a physical security inspection. Had OSEP reconciled its list to SSA's official list of offices, OSEP could have placed this office space on its list of offices requiring inspections beforehand.

³⁵ SSA, *AIMS, General Administration Manual*, ch. 10.06, sec. 10.06.05 (E.1) (February 28, 2025).

³⁶ We focused our review on the resolution of OSEP's security findings because SSA was not tracking the resolution of FPS security findings at the time of our review.

³⁷ SSA, *AIMS, General Administration Manual*, ch. 10.06, sec. 10.06.05 (E.1) (February 28, 2025).

³⁸ DHS, *The Risk Management Process: An Interagency Security Committee Standard*, sec. 5.3 (July 2024).

For example, an office manager resolved a finding but did not install the recommended duress alarm at their guard's desk. The manager stated they would consider installing the alarm in the future. In another example, an office manager supported they resolved a finding by stating they would discuss it with their landlord. However, the manager did not document any corrective actions. OSEP did not follow up with managers on either unimplemented corrective action.

Based on our interviews with office managers and OSEP staff, some office managers assumed OSEP reviewed their remediation actions and therefore office managers assumed OSEP implicitly approved their remediation. According to OSEP staff, the Agency lacked the resources for them to review all resolved findings to ensure they agreed with the actions. As a result, some managers unknowingly assumed responsibility for the unimplemented corrective actions, thus leaving potential security risks at their offices unaddressed.

OSEP could do more to help office managers remediate findings. Office managers we interviewed indicated OSEP's inspectors ensured they understood the security findings identified during their inspections. However, when finding information is not shared, newly assigned managers can inherit security findings developed before they were assigned without fully understanding them. For example, one newly assigned manager felt they did not have sufficient information, including graphical aids, to remediate their existing findings. Enhancing the security findings with more information would help managers not present during the inspections understand the prior findings and take appropriate action.

Unresolved Security Findings

Office managers did not resolve 125 (54 percent) of the 231 security findings within 180 days nor did they request extensions. Though OSEP's physical security application sends weekly reminders to managers with unresolved findings,³⁹ OSEP did not adequately monitor these findings to ensure they were resolved timely. OSEP should monitor each finding's progress to determine whether offices implemented all corrective actions within 180 days or requested extensions.⁴⁰ Findings that are of no cost to the office should be remediated as soon as possible.⁴¹ The reasons for some delays were not documented in the application. In one instance, the office manager took no action on security findings for over 6 years but did not document the reason for the delay. OSEP did not follow up with managers on the unresolved findings outside of automated reminders.

Managers did provide valid reasons for some delays. Some managers did not timely resolve findings because their office was scheduled to relocate or have a security system upgrade that would address the finding in the near future. These managers, along with upper management, determined costly remediations were not fiscally responsible. For example, one office's findings were unaddressed for over 1 year as the findings required significant funding and the office's future was uncertain. Additionally, some corrective actions took longer

³⁹ OSEP's physical security application sends automated weekly reminders to managers when they have not taken action to resolve findings for at least 30 days.

⁴⁰ SSA, *AIMS, General Administration Manual*, ch. 10.06, sec. 10.06.05 (E.1) (February 28, 2025).

⁴¹ SSA, *AIMS, General Administration Manual*, ch. 10.06, sec. 10.06.06 (D) (February 28, 2025).

to implement because of significant office improvements, COVID-related closures, and funding or contractor delays.

Regardless of the reasons for delays, OSEP should have better monitored actions to address findings pending longer than 180 days. To address delays in resolving findings, OSEP could have suggested interim corrective actions, as suggested by the ISC,⁴² to help mitigate the risk until a permanent solution became available.

CONCLUSION

SSA's OSEP plays a critical role in the safety of offices and their employees, including conducting inspections that assess employees' protection from unique Agency risks. When SSA does not mitigate security risks and vulnerabilities through corrective actions, Agency employees and offices can remain unnecessarily exposed to higher levels of security risk. However, opportunities exist to strengthen OSEP's oversight of security inspections and how office managers remediate security findings.

RECOMMENDATIONS

We recommend SSA's OSEP:

1. Update its policy to include monitoring FPS' physical security inspections of Agency offices.
2. Regularly reconcile its list of offices to the Agency's official list of offices to ensure all applicable offices are periodically inspected.
3. Work with office management to properly resolve the 101 security findings that were improperly remediated.
4. Revise policy to require that managers document corrective actions.
5. Review findings when they are resolved in its security application to ensure it agrees with actions taken.
6. Provide office managers with information to aid their remediations of security findings, such as diagrams or pictures, and information on requesting remediation extensions.
7. Review security findings not remediated within 180 days or the agreed upon timeframe and when appropriate, suggest interim corrective actions to office managers when permanent actions will not be timely implemented.

AGENCY COMMENTS

SSA agreed to implement our recommendations; see Appendix B.

⁴² DHS, *The Risk Management Process: An Interagency Security Committee Standard*, sec. 8.4.4 (July 2024).

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

To accomplish our objective, we:

- Reviewed applicable sections of the Interagency Security Committee's *The Risk Management Process: An Interagency Security Committee Standard*.
- Reviewed applicable sections of the Social Security Administration's (SSA) *Administrative Instructions Manual System* and *Physical Security Handbook*.
- Reviewed applicable sections of SSA's manuals for applications within its Security Automated Features and Enhancements web portal.
- Obtained physical security inspection information of SSA's offices that were open for business anytime between Fiscal Years 2018 and 2023 (see Table A–1).
 - Used information for 1,517 offices to identify
 - 1,374 offices for review whose facility security level (FSL) was assessed as I or II and
 - 143 offices for review whose FSL was assessed as III or IV.
 - We used these 2 populations of offices to establish 2 sampling frames of 50 offices from each population for a total of 100 sampled offices.

Table A–1: Office Populations and Sample Sizes

Sample Descriptions	Population Size	Sample Size
Offices with an FSL of I or II	1,374	50
Offices with an FSL of III or IV	143	50
Total Offices	1,517	100

- We used a simple random sample statistical approach to review both populations. This is a standard statistical approach used to create a sample from a population completely at random. As a result, each sample item had an equal chance of being selected throughout the sampling process, and the selection of one item had no impact on the selection of other items.
- We chose a sample that represented the population, absent human biases, and ensured statistically valid conclusions of the entire population under review.
- We noted SSA's systems grouped co-located offices under a parent office code in their security inspection database. In these cases, a parent office code included multiple offices.
- For each sampled office, we reviewed physical security inspection information from SSA's Office of Security and Emergency Preparedness (OSEP). We determined whether:
 - OSEP documented security findings and corrective actions to remediate findings in the Remediation application within the Security Automated Features and Enhancements portal.
 - Office managers incorrectly marked security findings as resolved without properly implementing OSEP's corrective actions.

- Office managers resolved their findings within 180 days or requested extensions not to exceed an additional 180 days.
- OSEP sent reminders to offices when findings were not timely resolved.
- For physical security inspection information obtained from Federal Protective Service (FPS), we reviewed whether OSEP properly monitored whether:
 - FPS conducted physical security inspections of SSA offices in our sample.
 - OSEP used FPS' inspection information of SSA offices to determine which SSA offices OSEP should inspect.¹
- Interviewed local and regional managers in our sampled offices to obtain their input on physical security inspections and remediation of inspection issues. We judgmentally selected five offices from each of our two populations of offices whose inspection reports contained multiple security findings. We interviewed five offices from our population of offices with a FSL of I or II and another five offices from our population of offices with an FSL of III or IV.

We assessed the reliability of SSA's physical security inspection information by (1) conducting electronic testing, (2) reviewing existing information about the data and the system that produced them, and (3) interviewing Agency officials knowledgeable about the data and determined the data were sufficiently reliable for the purposes of responding to our objective.

We assessed the significance of internal controls necessary to satisfy the audit objective. This included an assessment of the five internal control components, including control environment, risk assessment, control activities, information and communicating, and monitoring. In addition, we reviewed the principles of internal controls associated with the audit objective. We identified the following components and principles as significant to our objective to whether the SSA monitored and resolved identified physical security inspection issues at its offices.

- Component: Risk Assessment
 - Principle 7: Identify, analyze, and respond to risks
- Component: Control Activities
 - Principle 10: Design control activities
- Component: Information and Communication
 - Principle 14: Communicate internally
 - Principle 15: Communicate externally
- Component: Monitoring
 - Principle 17: Evaluate issues and remediate deficiencies

¹ SSA, *Administrative Instructions Manual System, General Administration Manual*, ch. 10.06, sec. 10.06.05 (February 28, 2025).

The SSA entity audited was the Office of Mission Support. We conducted our review between May 2024 and March 2025. We conducted this performance audit 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 objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix B – AGENCY COMMENTS




MEMORANDUM

Date: July 8, 2025

Refer To: TQA-1

To: Michelle L. Anderson
Acting Inspector General

From: Chad Poist 
Chief of Staff

Subject: Office of the Inspector General Draft Report, “Physical Security at Offices” (042318) --
INFORMATION

Thank you for the opportunity to review the draft report. We agree with the recommendations and appreciate your team’s work on this important issue. Security of our employees is one of our top priorities and we will work diligently to address the seven recommendations contained within the report.

Please let me know if I can be of further assistance. You may direct staff inquiries to Amy Gao at (410) 966-1711.

**Mission:**

The Social Security Office of the Inspector General (OIG) serves the public through independent oversight of SSA's programs and operations.

Report:

Social Security-related scams and Social Security fraud, waste, abuse, and mismanagement, at oig.ssa.gov/report.

Connect:

[OIG.SSA.GOV](https://oig.ssa.gov)

Visit our website to read about our audits, investigations, fraud alerts, news releases, whistleblower protection information, and more.

Follow us on social media via these external links:



@TheSSAOIG



OIGSSA



TheSSAOIG



Subscribe to email updates on our website.