



Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

Audit Summary

Firewall Administration

142315 August 2025



Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: August 6, 2025

Refer to: 142315

To: Frank Bisignano
Commissioner

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

Subject: Firewall Administration

The attached report summarizes the results of the Office of Audit's review. The objective was to determine whether the Social Security Administration managed and maintained Agency firewalls in accordance with Federal standards and guidelines.

Our full audit report contains information that, if not protected, could result in adverse effects to the Agency's information systems. In accordance with government auditing standards, we have separately transmitted to SSA management our audit's detailed findings and recommendations and excluded from this summary certain sensitive information because of the potential damage if the information is misused. We determined the omitted information neither distorts the audit results described in this report nor conceals improper or illegal practices.

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

Attachment

Firewall Administration 142315



August 2025

Office of Audit Report Summary

Objective

To determine whether the Social Security Administration (SSA) managed and maintained Agency firewalls in accordance with Federal standards and guidelines.

Background

Firewalls are devices or systems that control the flow of traffic between networks that have different security measures in place. A firewall acts as a barrier between the network and trusted and untrusted portions of the internet. Effective firewall administration is crucial for preventing unwanted and unapproved traffic from infiltrating the internal network.

The National Institute of Standards and Technology (NIST) provides organizations “. . . practical guidance on developing firewall policies and selecting, configuring, testing, deploying, and managing firewalls.”

SSA’s security infrastructure incorporates hundreds of firewalls to support and secure the Agency’s network and data, including customers’ personally identifiable information. Firewalls must be monitored, maintained, and replaced as appropriate to provide a high level of network security.

Results

SSA did not administer its firewalls in accordance with Federal standards and guidelines. Although SSA had some policies, procedures, and practices to secure its firewalls and networks against threats, we identified gaps that increased the risk of unauthorized access to the Agency’s sensitive and critical infrastructure.

Conclusion

If SSA implements our recommendations, it can better administer and secure its network and would be better positioned to defend and secure its resources and assets from cyber-attacks and inappropriate access that could compromise critical Agency data.

Recommendations

We made 13 recommendations to secure SSA’s networks and resources. SSA agreed to implement our recommendations.

TABLE OF CONTENTS

Objective	1
Background	1
Scope and Methodology	2
Results of Review	2
Firewall Inventory	2
Patching and Updating Firewalls.....	2
Firewall Annual Review and Rules Configuration	3
Firewall Configuration Change Management.....	4
Privileged Access to Firewalls and Logs.....	4
Firewall Configuration Backup	5
Advanced Firewall Features.....	6
Firewall Account and Password Controls.....	6
Physical Firewall Security	7
Conclusion	7
Recommendations	7
Agency Comments.....	7
Appendix A – Scope and Methodology.....	A-1
Appendix B – Agency Comments	B-1

ABBREVIATIONS

GAO	Government Accountability Office
IP	Internet Protocol
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
SSA	Social Security Administration

OBJECTIVE

Our objective was to determine whether the Social Security Administration (SSA) managed and maintained Agency firewalls in accordance with Federal standards and guidelines.

BACKGROUND

Firewalls are devices or systems that control the flow of traffic between networks that have different security measures in place.¹ A firewall acts as a barrier between the network and trusted and untrusted portions of the Internet. Effective firewall administration is crucial for preventing unwanted and unapproved traffic from infiltrating the internal network.

The National Institute of Standards and Technology (NIST) provides organizations “. . . practical guidance on developing firewall policies and selecting, configuring, testing, deploying, and managing firewalls.”² According to NIST, organizations should implement the following recommendations to improve the effectiveness and security of their firewalls.

- Create a policy that specifies how firewalls should handle in- and outbound network traffic.
- Identify all requirements that should be considered when determining which firewall to implement.³
- Create rulesets that implement the agency’s firewall policy while supporting firewall performance. Firewall rulesets should be as specific as possible about the network traffic they control.
- Manage firewall architectures, policies, software, and other components throughout the firewall solutions’ life.⁴

SSA’s security infrastructure comprises hundreds of firewalls to support and secure the Agency’s network and data, including its customers’ personally identifiable information. Firewalls must be monitored, maintained, and replaced as appropriate to provide a high level of network security. The Division of Network Engineering within SSA’s Office of Systems Operations and Hardware Engineering manages, administers, and maintains the Agency’s firewalls.

¹ NIST, *Guidelines on Firewalls and Firewall Policy*, 800-41 Rev. 1, sec. Executive Summary, p. ES-1 (September 2009).

² NIST, *Guidelines on Firewalls and Firewall Policy*, 800-41 Rev. 1, sec. 1.2, p. 1-1 (September 2009).

³ Organizations should determine which network areas they need to protect, and which types of firewall technologies will be most effective for the traffic that requires protection.

⁴ NIST, *Guidelines on Firewalls and Firewall Policy*, 800-41 Rev. 1, sec. Executive Summary, pp. ES-1 to ES-2 (September 2009). A formal change management control process should manage firewall rulesets and policies because of potential impacts to security and business operations and should include periodic ruleset reviews or tests to ensure continued compliance with the organization’s policies.

SCOPE AND METHODOLOGY

We evaluated SSA's processes for managing and maintaining Agency firewalls. We also interviewed Agency staff and reviewed Agency firewall configurations, SSA policies and procedures, and other industry and Federal guidance. We used NIST's *Guidelines on Firewalls and Firewall Policy* as the primary criteria for our audit. See Appendix A for additional information about our scope and methodology.

RESULTS OF REVIEW

SSA did not administer its firewalls in accordance with Federal standards and guidelines.⁵

Firewall Inventory

Firewall inventories allow agencies to identify and track their devices. A complete and accurate inventory allows an agency to identify and ensure firewalls are properly configured, adequately patched and updated, and retired once they are no longer supported. In addition, once firewalls are retired or no longer necessary, an accurate inventory ensures devices that contain critical and sensitive network architecture details are sanitized before SSA disposes of them as part of the device life-cycle management process.⁶

The Office of Management and Budget (OMB) requires that Federal agencies “[continually] facilitate adoption of new and emerging technologies, and regularly assess the . . . physical and software assets associated with the system.”⁷ Additionally, OMB states “Agencies shall ensure that physical devices, software applications, hardware platforms, and systems within the organization are inventoried initially when obtained and updated on an ongoing basis.”⁸ We reviewed SSA's firewall inventory process and found deficiencies.

Patching and Updating Firewalls

Patching is the act of changing installed software—such as firmware, operating systems, or applications—to correct security or functionality problems or add new capabilities. Patching and updating operating systems are crucial to network security.⁹

⁵ Our audit report contains information that, if not protected, could result in adverse effects to the Agency's information systems. In accordance with government auditing standards, we have separately transmitted to SSA management our audit report, which details our findings and recommendations. We excluded from this summary certain sensitive information because of the potential damage if the information is misused. We have determined the omitted information neither distorts the audit results described in this report nor conceals improper or illegal practices. GAO, *Government Auditing Standards*, GAO-18-568G, pars. 9.61 through 9.67, pp. 208 through 210 (July 2018).

⁶ Device life-cycle management is the process of managing devices from the moment they are purchased to when they are retired. This includes decommissioning and disposal.

⁷ OMB, *Managing Information as a Strategic Resource*, Circular A-130, sec. 5.a.1.b.i, p. 5 (July 28, 2016).

⁸ OMB, *Managing Information as a Strategic Resource*, Circular A-130, sec. 5.a.1.b.i, footnote 6, p. 5 (July 28, 2016).

⁹ NIST, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*, 800-40 Rev. 4, sec. Executive Summary, p. iv (April 2022).

Firewalls are the first line of cyber-security defense. Administrators should patch and update firewalls as soon as possible when vendors release patches and updates to address known security vulnerabilities that individuals can exploit to gain unauthorized access and perform inappropriate activities.

Organizations should install security-relevant software and firmware updates within an organization-defined timeline from the updates' release.¹⁰ Each organization defines the number of days allowed from the release of each update until the organization installs it to allow for a testing period. Additionally, organizations should consider patching a standard cost of doing business and rigorously follow and track the process.¹¹ We reviewed SSA's firewall patching and updating process and found deficiencies.

Firewall Annual Review and Rules Configuration

A firewall acts as the gatekeeper for an agency's resources and a barrier between the agency's internal and external networks that connect to SSA. Agencies use access lists—sets of rules that determine whether network traffic is allowed or denied based on predefined conditions, including source and destination Internet Protocol (IP) addresses, port numbers, and protocols—to prevent unauthorized access to its networks. Agencies configure these access lists to allow traffic the Agency has approved to access its network. Agencies' firewall policies should

- allow only necessary protocols through the firewall to enter the network;¹²
- permit only appropriate source and destination IP addresses to be used;¹³ and
- block all in- and outbound traffic the firewall policy has not expressly permitted.¹⁴

NIST notes it is important to review the firewall policy often. Such a review can uncover rules that are no longer needed as well as new policy requirements that need to be added to the firewall. It is best to review the firewall policy at regular intervals so that such reviews do not only happen during policy or security audits (or, worse, only during emergencies).¹⁵ We reviewed SSA's firewall annual review and rules configuration process and found deficiencies.

¹⁰ NIST, *Security and Privacy Controls for Information Systems and Organizations*, 800-53 Rev. 5, sec. SI-2, p. 333 (September 2020).

¹¹ NIST, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*, 800-40 Rev. 4, sec. Executive Summary, p. iv (April 2022).

¹² NIST, *Guidelines on Firewalls and Firewall Policy*, 800-41 Rev. 1, sec 4.1, p. 4-1 (September 2009).

¹³ NIST, *Guidelines on Firewalls and Firewall Policy*, 800-41 Rev. 1, sec 4.1.1, p. 4-1 (September 2009).

¹⁴ NIST, *Guidelines on Firewalls and Firewall Policy*, 800-41 Rev. 1, app. A, p. A-1 (September 2009).

¹⁵ NIST, *Guidelines on Firewalls and Firewall Policy*, 800-41 Rev. 1, sec. 5.5, p. 5-8 (September 2009).

Firewall Configuration Change Management

The firewall configuration's change management process ensures Agency employees make only approved changes to its devices, including firewalls. The process should include (1) a change request, (2) the change approval, (3) the change performed, and (4) a review to ensure only the approved change was made. In addition, the process should include separation of duties to ensure device administrators do not approve their own change requests. SSA must complete emergency, or unscheduled, changes quickly, outside of the normal change-management process. The Agency should monitor and review such changes to ensure they are appropriate, necessary, and approved.

According to NIST guidance, agencies should “[monitor] and review activities associated with configuration-controlled changes to the system; and [coordinate] and provide oversight for configuration change control activities.”¹⁶ In addition, NIST notes “. . . [it] is best to review the firewall policy at regular intervals so that such reviews do not only happen during policy and security audits (or, worse, only during emergencies).”¹⁷ Each review should include a detailed examination of all changes made since the last regular review, who made the changes, and under what circumstances the changes were made.¹⁸ We reviewed SSA's firewall configuration change-management process and found deficiencies.

Privileged Access to Firewalls and Logs

Privileged access allows users to change and modify systems, applications, or information technology resources. A user with a privileged account can perform security-relevant functions that ordinary users cannot.¹⁹ Agencies should employ the principle of least privilege—allowing users only the minimum level of access necessary to perform their duties—when determining whether to grant privileged access, while also ensuring they maintain appropriate separation of duties. Additionally, agencies should revoke access when the user no longer needs it.²⁰

¹⁶ NIST, *Security and Privacy Controls for Information Systems and Organizations*, 800-53 Rev. 5, sec. CM-3, p. 99 (September 2020).

¹⁷ NIST, *Guidelines on Firewalls and Firewall Policy*, 800-41 Rev. 1, sec. 5.5, p. 5-8 (September 2009).

¹⁸ See footnote 17.

¹⁹ NIST, *Security and Privacy Controls for Information Systems and Organizations*, 800-53 Rev. 5, sec. app. A, p. 412 (September 2020).

²⁰ NIST, *Security and Privacy Controls for Information Systems and Organizations*, 800-53 Rev. 5, secs. AC-5 and AC-6, p. 36 (September 2020).

Firewall administrators have privileged user accounts to perform administrative tasks, including firewall modifications and updates. Firewall-generated logs play a critical role in preventing and recovering from system failures and ensuring proper security configurations are set on the firewall.²¹ Proper logging can provide vital information for responding to security incidents. Security teams should continuously monitor logs to identify threats to the firewall itself.²²

Agencies should not grant users access to log files unless they need access as part of their duties. If agencies grant users access to log files, the users should not be able to read, modify, rename, or delete the logs. Instead, they should only be able to add to the existing logs.²³

Storing audit records—such as logs—in a repository separate from the audited system or system component helps ensure a compromise of the system being audited does not also result in a compromise of the audit records. Storing audit records on separate physical systems or components also preserves the confidentiality and integrity of audit records and facilitates the management of audit records as an organization-wide activity.²⁴ We reviewed SSA’s firewall logs access controls and found deficiencies.

Firewall Configuration Backup

Back-up and recovery strategies are important because—in the event of a hardware failure, software corruption, or security incident—an organization can restore the firewall’s configuration, policies, and rules. Organizations should create backups of system-level information with an “. . . organization-defined frequency consistent with recovery time and recovery point objectives.”²⁵ Firewall policies and rulesets should be backed up regularly.²⁶ We reviewed SSA’s firewall configuration back-up process and found deficiencies.

²¹ A log records events that occur in an organization’s system or network. The log comprises entries that contain information specific to the occurrence or activity. NIST, *Guide to Computer Security Log Management*, 800-92, sec. Executive Summary, p. ES-1 (September 2006).

²² NIST, *Guidelines on Firewalls and Firewall Policy*, 800-41 Rev. 1, sec. Executive Summary, p. ES-2 (September 2009).

²³ NIST, *Guide to Computer Security Log Management*, 800-92, sec. 5.1.3, p. 5-4 (September 2006).

²⁴ NIST, *Security and Privacy Controls for Information Systems and Organizations*, 800-53 Rev. 5, sec. AU-9, p. 74 (September 2020).

²⁵ NIST, *Security and Privacy Controls for Information Systems and Organizations*, 800-53 Rev. 5, sec. CP-9, pp. 125 (September 2020).

²⁶ NIST, *Guidelines on Firewalls and Firewall Policy*, 800-41 Rev. 1, sec. 5.5, p. 5-7 (September 2009).

Advanced Firewall Features

SSA has developed an expansive network that includes multiple physical locations and a vast amount of network infrastructure, including numerous switches, routers, computers, virtual private networks, and firewall devices. Along with the network's vast size, increasingly complex cyber-threats continue to evolve. Traditional firewalls filter network traffic based on organization-defined policies, while next-generation firewalls build on the foundation of traditional firewalls but incorporate advanced features that can more deeply inspect network traffic. The deeper network traffic inspection can detect and block more sophisticated and complex cyber-attacks.

Network security should include a defense-in-depth approach. Defense-in-depth involves creating multiple layers of security that allow risk to be better managed. If an attacker compromises one layer of defense, another layer is there to contain the attack.²⁷ NIST notes, "For defense-in-depth to be truly effective, firewalls should be part of an overall security program that also includes products such as antimalware and intrusion detection software."²⁸ We reviewed SSA's advanced firewall features and found deficiencies.

Firewall Account and Password Controls

The Government Accountability Office (GAO) states, "Logical access controls require users to authenticate themselves and limit the files and other resources that authenticated users can access and the actions that they can execute."²⁹ Additionally, "Ineffective access controls may result in unauthorized access to, modification of, or disclosure of sensitive data and programs and disruption of critical operations."³⁰ GAO notes that password-based authenticators should be adequately and appropriately defined in accordance with NIST SP 800-53, IA-05 and IA-06.³¹

According to NIST, organizations should "Manage system authenticators by . . . [ensuring] that authenticators have sufficient strength of mechanism for their intended use."³² Additionally, organizations should ". . . [obscure] feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals."³³ We reviewed SSA's firewall account and password controls and found deficiencies. After our review, SSA remediated the issues. Therefore, we are not making a recommendation related to this finding.

²⁷ NIST, *Guidelines on Firewalls and Firewall Policy*, 800-41 Rev. 1, sec. 5.1, p. 5-1 (September 2009).

²⁸ NIST, *Guidelines on Firewalls and Firewall Policy*, 800-41 Rev. 1, sec. 5.1, pp. 5-1 through 5-2 (September 2009).

²⁹ GAO, *Federal Information System Controls Audit Manual*, GAO-24-107026, sec. 540.01, p. 245 (September 2024).

³⁰ GAO, *Federal Information System Controls Audit Manual*, GAO-24-107026, sec. 540.03, p. 245 (September 2024).

³¹ GAO, *Federal Information System Controls Audit Manual*, GAO-24-107026, table 11, sec. AC.02.01.05, pp. 263-64 (September 2024).

³² NIST, *Security and Privacy Controls for Information Systems and Organizations*, 800-53 Rev. 5, sec. IA-5, p.138 (September 2020).

³³ NIST, *Security and Privacy Controls for Information Systems and Organizations*, 800-53 Rev. 5, sec. IA-6, p. 143 (September 2020).

Physical Firewall Security

Physical security is essential to an organization's comprehensive security strategy and involves safeguarding the physical firewall devices from unauthorized access, tampering, or any other physical damage. Effective physical security measures, including access controls, surveillance, environmental controls, and physical barriers, are essential to maintaining the firewalls' integrity and availability. Unauthorized physical access to key network security devices, such as Agency firewalls, could allow unapproved modification and physical device damage and compromise the Agency's network resources. Agencies should establish

. . . a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel; Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.³⁴

We reviewed SSA's physical firewall security access controls and found no deficiencies.

CONCLUSION

Agency firewalls are the front line of network security and are an important tool to better securing the Agency's important and highly sensitive data and resources. To achieve this, SSA and its information technology administrators must appropriately and effectively administer Agency firewalls. If SSA implements our recommendations, it can better administer and secure its network and would be better positioned to defend and secure its resources and assets from cyber-attacks and inappropriate access that could compromise critical Agency data.

RECOMMENDATIONS

We made 13 recommendations and transmitted the recommendations to SSA management separately.

AGENCY COMMENTS

SSA agreed to implement our recommendations; see Appendix B.

³⁴ NIST, *Security and Privacy Controls for Information Systems and Organizations*, 800-53 Rev. 5, sec. MA-5, p.167 (September 2020).

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

To accomplish our objective, we:

- Reviewed applicable Federal laws, regulations, and guidance related to managing and maintaining Agency firewalls, including the following.
 - National Institute of Standards and Technology *Guidelines on Firewalls and Firewall Policy, Special Publication 800-41, Revision 1* (September 2009) and
 - National Institute of Standards and Technology *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology, Special Publication 800-40, Revision 4* (April 2022).
- Reviewed the Social Security Administration's (SSA) policies, procedures, and documentation pertaining to firewall administration.
- Selected a non-statistical sample of 40 firewalls and reviewed supporting documentation for each sampled firewall.
- Interviewed SSA personnel responsible for managing and maintaining Agency firewalls.

We conducted our audit from January 2024 through March 2025. The principal entity reviewed was the Office of Systems Operations and Hardware Engineering, Division of Network Engineering.

We assessed the reliability of SSA's firewall inventory by reviewing files for invalid or missing records. We also examined the inventory management process for firewalls by inquiring with the Agency and interviewing appropriate staff. Although we identified deficiencies with inventory management and maintenance procedures, we determined that the data were sufficiently reliable for the purpose of this review. Our report notes deficiencies with the inventory process and we provided a recommendation for SSA to address this finding.

We assessed the significance of internal controls necessary to satisfy the audit objective. This included an assessment of the five internal control components: control environment, risk assessment, control activities, information and communication, 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 the audit objective.

- Component 2: Risk Assessment
 - Principle 6 – Define objectives and risk tolerances
 - Principle 7 – Identify, analyze, and respond to risk
 - Principle 9 – Identify, analyze and respond to change
- Component 3: Control Activities
 - Principle 10 – Design control activities
 - Principle 11 – Design activities for the information system
 - Principle 12 – Implement control activities

- Component 5: Monitoring
 - Principle 16 – Perform monitoring activities

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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix B – AGENCY COMMENTS




SOCIAL SECURITY Office of the Commissioner

MEMORANDUM

Date: July 21, 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, "Firewall Administration" (142315) --
INFORMATION

Thank you for the opportunity to review the draft report. We agree with the recommendations. Last year, we initiated a strategic effort to streamline our firewall infrastructure by consolidating under a single vendor. This approach simplifies patch installation, reduces costs, and enhances our overall security posture.

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.