Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Summary

Mobile Phone Security

142314 | September 2023

Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: September 28, 2023 **Refer To:** 142314

To: Kilolo Kijakazi
Acting Commissioner

From: Gail S. Ennis
Inspector General

Subject: Mobile Phone Security

The attached final report summarizes the results of the Office of Audit's review. The objective was to determine whether the Social Security Administration's mobile phone security conformed with Federal standards and guidelines.

Our audit report (A-14-19-50811) contain 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 detailed findings and recommendations and excluded from this report 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 summary report nor conceals improper or illegal practices.

If you wish to discuss the final report, please call me or have your staff contact Michelle L. Anderson, Assistant Inspector General for Audit.

Attachment

Mobile Phone Security
142314

September 2023 **Office of Audit Report Summary**

Objective

To determine whether the Social Security Administration's (SSA) mobile phone security conformed with Federal standards and guidelines.

Background

Use of mobile devices expose organizations to a unique and evolving set of threats. Devices like mobile phones are an attractive target for attackers seeking to compromise Government data.

SSA provides mobile phones to employees who have a business need. Employees use these mobile phones to access SSA email accounts, the Agency's intranet site, certain SSA-approved applications, and internet websites.

The *Federal Information Security Modernization Act of 2014* requires that agencies develop, document, and implement an Agency-wide information security program. The National Institute of Standards and Technology developed a Risk Management Framework to select, implement, and assess controls, and authorize and monitor systems.

Results

SSA's mobile phone security did not fully conform with Federal standards and guidelines. Although SSA had some policies, procedures, and practices to protect sensitive information from the threats against mobile phone use, we identified areas of noncompliance with standards and guidelines that increased the risk of unauthorized access to the Agency's sensitive information. We identified several issues related to the security of SSA's mobile phones.

Improvements in these areas could provide SSA with greater protection of the confidentiality, integrity, and availability of the information on the mobile phones and the Agency's systems accessed by mobile phones.

Recommendations

We made seven recommendations to improve the security of the Agency's mobile phones.

Agency Comments

SSA agreed with our recommendations.

TABLE OF CONTENTS

ABBREVIATIONS

CMP	Configuration Management Plan
DISA	Defense Information Systems Agency
EWANS	Enterprise Wide Mainframe and Distributed Network Telecommunications Services and System
ISP	Information Security Policy
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
Pub. L. No.	Public Law Number
SAR	Security Assessment Report
SCS	Security Configuration Standards
SSA	Social Security Administration
SSP	System Security Plan
STIG	Security Technical Implementation Guide
U.S.C.	United States Code

OBJECTIVE

Our objective was to determine whether the Social Security Administration's (SSA) mobile phone security conformed with Federal standards and guidelines.[1]

BACKGROUND

Use of mobile devices expose organizations to a unique and evolving set of threats. Devices like mobile phones are an attractive target for attackers seeking to compromise Government data. SSA systems hold significant amounts of personally identifiable information on nearly every U.S. citizen, as well as non-citizens with a valid reason to request a Social Security number. In addition to accessing personally identifiable information, SSA's mobile phones can access sensitive system information. Compromise of this information could adversely affect the organization's operations, assets, or individuals.

The Agency's Use of Mobile Phones

SSA provides mobile phones to employees who have a business need. These mobile phones can access SSA email accounts, the Agency intranet, certain SSA-approved applications, and internet websites.[2]

SSA uses commercial services to manage mobile phone provisioning, inventory, and security. One commercial service manages mobile phone configuration settings and access to applications. Another commercial service is SSA's source for mobile phone inventory information. Employees use these services to initiate mobile phone requests and returns to the Agency. Staff also use the services to manage the mobile phone inventory and identify mobile phones as lost or stolen.

[1] A mobile phone is, ". . .a portable computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (to wirelessly transmit or receive information); possesses local, non-removable data storage; and is powered on for extended periods of time with a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations." National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Information Systems and Organizations*, *800-53 Revision 5*, Appendix A, p. 408 (September 2020).

[2] SSA stated it blocked the public application store on Agency-issued mobile phones. SSA permits installations only from the Agency's enterprise application store, which includes only SSA-approved applications.

Federal Security Criteria

Information systems include such devices as mobile phones.[3] The *Federal Information Security Modernization Act of 2014*[4] requires that agencies develop, document, and implement an Agency-wide information security program.[5] In addition, agency heads must provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of agency information and information systems.[6]

NIST developed a Risk Management Framework, which has seven essential steps.[7]

1. **Prepare to execute the Risk Management Framework** from an organization- and system-level perspective by establishing a context and priorities for managing security and privacy risk.

2. **Categorize the system** and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss.

3. **Select an initial set of controls** for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.

4. **Implement the controls** and describe how they are employed in the system and its environment of operation.

5. **Assess the controls** to determine whether the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.

6. **Authorize the system** or common controls based on a determination the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.

7. **Monitor the system** and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

---

[3] NIST, *Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy*, *800-37 Revision 2*, ch. 1, p. 1 (December 2018).

[4] *Federal Information Security Modernization Act of 2014*, Pub. L. No. 113-283, § 2, 128 Stat. 3073, pp. 3075 through 88.

[5] 44 U.S.C. § 3554(b).

[6] 44 U.S.C. § 3554(a)(1)(A).

[7] NIST, *Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy*, *800-37 Revision 2*, ch. 2.2, pp. 8 and 9 (December 2018).

SCOPE AND METHODOLOGY

We limited our scope to SSA-provided mobile phones and their authorized users. According to the Agency, only SSA-provided mobile phones can connect to the Agency's network. To meet our objective, we:

- reviewed related Federal law, standards, and guidance;
- reviewed relevant Agency policies, procedures, and security documentation, including SSA's Information Security Policy (ISP), Personal Property Management Handbook, and security control and authorization documents;
- met with pertinent Agency subject-matter experts to obtain information on SSA's management of mobile phone security and controls; and
- tested a sample of 50 mobile phones to determine whether they complied with SSA's configuration standards.

See Appendix A for additional information about our scope and methodology.

RESULTS OF REVIEW

SSA's mobile phone security did not fully conform with Federal standards and guidelines. Although SSA had some policies, procedures, and practices to protect sensitive information from the threats of their unauthorized access while the mobile phone is being used, we identified areas of noncompliance with standards and guidelines that increased the risk of unauthorized access to the Agency's sensitive information.

Security Boundary

SSA requires that every information technology asset be included in an information system boundary and be covered by that boundary's Authorization to Operate.[8] However, SSA did not include mobile phones within an authorization boundary.

[8] SSA, *ISP*, *Authorized Hardware and Software*, sec. 2.1.2 (June 5, 2023). An authorization boundary defines a system to facilitate risk management and accountability. An Authorization to Operate is a formal declaration the Authorizing Official authorizes operation of an information system or business product and explicitly accepts the risk to agency operations. Any information system or business product that collects, maintains, processes, transmits, or stores federal information, for or on behalf of SSA, requires an authorization decision.

In addition, SSA did not identify mobile phones or their operating systems in its authorized hardware or software lists. SSA was conducting an Agencywide initiative to revise its system boundaries as it transitioned to ongoing authorizations.[9] In addition, the Agency was updating the System Security Plan (SSP) of one of its commercial services to include mobile phone security controls.

Security Management Issues

Although the commercial services' configuration management and inventory systems do not contain mobile phones, they impact the security of SSA's mobile phones. Therefore, we included them in our review. We found a lack of oversight resulted in SSA not properly performing risk assessments and not appropriately developing and maintaining security documentation.

Risk Assessments

According to the Agency, it included risk assessment information within its SSPs. However, one commercial service's SSP did not identify system-specific risk assessment controls, and the other service's SSP only included one risk assessment control (for security categorization). Neither SSP addressed the determination of risk based on the identification of threats and vulnerabilities and determination of their likelihood of occurrence and magnitude of impact.[10]

Incomplete and Incorrect Documentation

We reviewed the documentation SSA provided for its commercial services and noted several issues.

Control Inheritance

Agencies should document, in the SSPs, their risk-based decisions on tailoring security and privacy control baselines for information systems. Tailoring can include identifying and designating common controls from which multiple systems can inherit full or partial protection.[11]

[9] Ongoing authorization refers to "the ongoing determination and acceptance of information security risk. Rather than enforcing a static, point-in-time reauthorization process, agencies shall conduct ongoing authorizations of their information systems and environments in which those systems operate. . . ." Office of Management and Budget, *Enhancing the Security of Federal Information and Information Systems*, *M-14-03*, pp. 1 and 2 (2013).

[10] NIST, *Guide for Conducting Risk Assessments*, *800-30 Revision 1*, ch. 3.2, p. 29 (September 2012).

[11] NIST, *Guide for Developing Security Plans for Federal Information Systems*, *800-18 Revision 1*, ch. 2.5, p. 13 (February 2006). NIST, *Control Baselines for Information Systems and Organizations, 800-53B,* ch. 2.4, pp. 9 and 10 (October 2020).

One commercial service's SSP indicated it fully inherited some common controls, but the SSP did not describe the controls or identify the control providers. The authorizations to operate both commercial services stated each leveraged common controls from the Enterprise Wide Mainframe and Distributed Network Telecommunications Services and System (EWANS); however, neither SSP mentioned EWANS. Moreover, EWANS did not have a current authorization.[12]

In addition, SSA did not include complete information about control inheritance in its Security Assessment Reports (SAR) for the commercial services.[13] Also, SSA's SAR for one of the commercial services contained incorrect control inheritance information. Specifically, the SAR identified certain controls as inherited from the cloud service provider; however, these controls required organizationally defined policies, procedures, or settings.[14] In addition, SSA did not identify in the SAR which controls the commercial service leveraged from EWANS and the authorizations noted in the SSP.[15]

Security Responsibilities

Cloud services operate under a shared responsibility model, where cloud service providers assume responsibility for some security tasks and organizations assume responsibility for others. Roles and responsibilities vary based on service agreements.

We noted inconsistencies between the customer responsibilities documented by the cloud service provider and the control documentation in SSA's SSPs for the commercial services. For one commercial service provider, we identified 24 inconsistencies from the 41 controls for which SSA had responsibility. Of the 24 controls, the SSP:

- did not include 8;
- missed some information for 13; and
- had inconsistent information for 3.

For the other commercial service provider, from the 38 controls for which SSA was responsible, we found inconsistencies in 6 controls. Of the six, the SSP:

- did not identify SSA's responsibility for, or describe SSA's implementation of, two;
- did not describe SSA's implementation of another three; and
- did not address the control in one implementation description.

[12] SSA was splitting EWANS into multiple systems.

[13] We considered the Security Requirements Traceability Matrix as part of the SAR.

[14] The commercial service providers use cloud services, which deliver computing services over the internet.

[15] For example, system owners and authorizing officials leverage security and privacy information about inherited controls from assessments conducted by the control providers.

Based on these inconsistencies, the Agency may not have a complete and accurate understanding of the security responsibilities for these systems. This could impair SSA's ability to properly manage system security and make appropriate authorization decisions.

Outdated Information

The SSP for one of the commercial services identified the authorizing official as a Chief Information Officer who left the Agency in 2017. It also noted the service leveraged authorizations for other systems from 2013 and 2016, but these systems should have more current authorizations.[16]

Without properly assessing risks and understanding who is responsible for implementing security controls, the Agency could not be sure whether controls sufficiently protect the commercial services and who manages control activities. In addition, SSA considered it imperative to keep SSPs current to provide accurate representations of systems, and noticeable errors may indicate that other less apparent information had also not been properly updated.[17] Further, authorizing officials use SARs as key documents when they determine risk, and SARs should include an appropriate level of detail to understand the risks regarding inherited controls.[18] The Agency provided a draft of one updated SSP that remediated some of the issues we identified. In addition, the Agency stated it reviews contractor security documents annually.

Configuration Management Plan

SSA did not have a Configuration Management Plan (CMP) for mobile phones. Both NIST guidance and SSA policy detailed the need to develop, document, and implement a CMP for information systems.[19] The ISP required documentation of ". . . an information system-specific CMP to define the system-specific roles, processes, and procedures for configuration management throughout the system lifecycle. A CMP cannot be inherited from another system. . . ."[20]

The Agency provided two documents in response to our request for a CMP; however, neither document addressed CMP requirements. A properly developed and regularly updated CMP documents and explains the roles, responsibilities, and tasks involved with the effective configuration management of a system.

The lack of a CMP increased the likelihood SSA may not have effectively maintained mobile phones.

---

[16] SSA required reauthorization of systems every 3 years. However, the Agency is transitioning from a static authorization cycle to a dynamic Ongoing Authorization Program.

[17] SSA, *ISP*, *System Security Plan (SSP)*, sec. 2.4.1.2 (June 5, 2023).

[18] NIST, *Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy*, *800-37 Revision 2*, ch. 3.5, pp. 65 and 66 (December 2018).

[19] NIST, *Security and Privacy Controls for Information Systems and Organizations*, *800-53 Revision 5*, ch. 3.5, pp. 110 and 111 (September 2020). SSA, *ISP, Configuration Management Plan,* sec. 3.4.1.2 (June 5, 2023).

[20] SSA, *ISP*, *Configuration Management Plan*, sec. 3.4.1.2 (June 5, 2023).

Security Configuration Standards and Operating Systems

SSA requires that maintenance of baseline configurations be established for its information technology devices.[21] However, the Agency had outdated and incomplete Security Configuration Standards (SCS) for mobile phones. The Agency stated it based its SCS for mobile phones on the Defense Information Systems Agency's (DISA) Security Technical Implementation Guide (STIG), which contains the configuration standards for Department of Defense systems. SSA policy required annual review of SCSs.[22] However, management did not ensure the Agency followed its security configuration policies.

SSA did not provide evidence it reviewed the SCS for mobile phone operating system since the last published version. The Agency stated it was establishing an annual review process and developing a new SCS.

Controls to Ensure or Verify Sanitization

SSA requires that ". . . [p]rior to releasing to vendors, disposing, or donating information technology equipment . . . the media must be sanitized or destroyed in a manner that prevents unauthorized disclosure of sensitive information."[23] The Agency used a commercial service to sanitize returned mobile phones and requested sanitization by the manufacturer for mobile phones that users reported lost or stolen. However, SSA did not have complete and accurate inventory information to ensure or verify the sanitization of lost or stolen mobile phones.

There are various ways users can report lost or stolen mobile phones. However, not all methods provide automatic notification to the team responsible for requesting sanitization. Further, it is not possible to identify all lost or stolen mobile phones because not all reporting methods have a field for identifying information like a serial number, or even a specific field to identify that the loss was a mobile phone. The Agency stated it reviewed records for easily identifiable mobile phone losses and found that its inventory system did not always reflect that lost or stolen devices were missing.

In addition, SSA's Personal Property Management Handbook stated the Agency randomly tested information technology equipment to ensure proper sanitization.[24] However, according to SSA staff, the Agency stopped performing these tests when expanded telework began in March 2020. SSA resumed random sanitization testing in August 2022.

SSA lacked oversight and controls to ensure lost or stolen devices have been sanitized and the Agency's mobile phone inventory was accurate and complete. Without complete, accurate inventory records and oversight activities, SSA could not be sure of sanitization of lost or stolen mobile phones.

---

[21] SSA, *ISP*, *Configuration Management*, sec. 3.4.1 (June 5, 2023).

[22] SSA *ISP*, *Security Configuration Standards*, sec. 3.4.1.1 (June 5, 2023).

[23] SSA, *ISP*, *Media Sanitization*, sec. 3.4.6 (June 5, 2023).

[24] SSA, *Personal Property Management Handbook*, ch. 5.4, sec. A., p. 14 (October 2020). SSA's updated handbook, published in July 2023, did not mention random sanitization testing.

Controls to Identify Potentially Lost or Unused Mobile Phones

SSA had 90-day use reports that could help management make informed decisions about device allocation and identify lost or stolen devices. However, only SSA's Office of Operations received the monthly usage reports. Other components received reports on an undefined, as-needed basis. Use of data-driven methods to identify when users do not possess their assigned mobile phones could reduce SSA's risk of inappropriate network access and loss of personally identifiable information. SSA was able to restrict access and remotely sanitize these mobile phones, but this required that the Agency know when to take these actions.
In September 2021, SSA began sending all components weekly reports of mobile phones that did not comply with SSA security requirements. Since the Agency also implemented a control to limit the amount of time that noncompliant mobile phones can operate, the weekly reports can help identify staff that have not used their mobile phones for an extended period of time.

CONCLUSION

It is important to achieve adequate security for Federal information and systems and a consistent level of protection for such information and systems.[25] The success of organizations' missions and business functions depend on protecting information systems and the privacy of individuals.[26] Therefore, it is imperative that SSA properly manage information security risk. SSA should improve its security controls for mobile phones to minimize the risk to the Agency and its customers. Improvements in these areas could provide SSA with greater protection to the confidentiality, integrity, and availability of the information on the mobile phones and the Agency's systems accessed by mobile phones.

RECOMMENDATIONS

We made seven recommendations to improve security related to the Agency's use of mobile phones and transmitted them to SSA under separate cover. Our recommendations addressed:

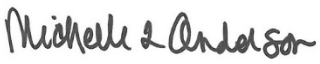
- risk management;
- accuracy and completeness of security documentation and responsibilities;
- maintaining up-to-date and properly configured mobile phones;
- ensuring staff sanitize mobile phones when appropriate; and
- improving decision-making for mobile phone allocation.

[25] Office of Management and Budget, *Managing Information as a Strategic Resource, A-130*, Appendix I, sec. 5.d, p. 18 (2016).

[26] NIST, *Risk Management Framework for Information Systems and Organizations, 800-37 Revision 2*, ch.1, p. 1 (December 2018).

AGENCY COMMENTS

SSA agreed with our recommendations. See Appendix B for the full text of the Agency's response.



Michelle L. Anderson
Assistant Inspector General for Audit

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

To accomplish our objective, we:

- Reviewed related Federal laws, standards, and guidance including:
  - Defense Information Systems Agency Security Technical Implementation Guides for mobile phones and tablets.
  - Federal Risk and Authorization Management Program required documents and the moderate baseline template for system security plans.
  - National Institute of Standards and Technology Special Publications:
    - *Guide for Developing Security Plans for Federal Information Systems*, 800-18 Revision 1 (February 2006).
    - *Guide for Conducting Risk Assessments*, 800-30 Revision 1 (September 2012).
    - *Risk Management Framework for Information Systems and Organizations – A System Life Cycle Approach for Security and Privacy*, 800-37 Revision 2 (December 2018).
    - *Security and Privacy Controls for Information Systems and Organizations*, 800-53 Revision 4 (April 2013) and Revision 5 (September 2020).
    - *Control Baselines for Information Systems and Organizations*, 800-53B (October 2020).
    - *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, 800-124 Revision 1 (June 2013).
  - Office of Management and Budget guidance:
    - Circular No. A-130, *Managing Information as a Strategic Resource* (July 2016).
- Reviewed relevant Social Security Administration (SSA) policies and procedures including:
  - Administrative Instructions Manual System.
  - *Information Security Policy (ISP) for the Social Security Administration,* Version 8.9 (June 5, 2023).
  - *Personal Property Management Handbook* (October 2020).
  - *Security Technical Implementation Guide Process for the Social Security Administration*, Version 1.1 (June 2021).
- Reviewed SSA security documentation, including System Security Plans, Security Assessment Reports, and Security Configuration Standards.

- Met with pertinent Agency subject-matter experts to obtain information on SSA's management of mobile phone security and controls.

- Tested a sample of 50 mobile phones to determine compliance with SSA's configuration standards.

We limited our scope to SSA-provided mobile phones and their authorized users. According to the Agency, only SSA-provided mobile phones can connect to its network.

We conducted our audit from June 2020 through September 2022. The principal entity reviewed was the Office of Systems.

We assessed the reliability of SSA's mobile phone inventory by reviewing files for duplicate, invalid, or missing records. We also examined the inventory management process for mobile phones by inquiring with the Agency and interviewing appropriate staff. Although we identified deficiencies with inventory management and sanitization procedures, we determined that the data was sufficiently reliable for the purpose of this review. Our report notes SSA lacked sufficient inventory records or controls to ensure or verify all phone sanitization. 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, including 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 two components and three principles as significant to the audit objective.

- Component 3: 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 findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix B – AGENCY COMMENTS

SOCIAL SECURITY

MEMORANDUM

Date: September 22, 2023 Refer To: TQA-1

To: Gail S. Ennis
Inspector G

From: Scott Frey
Chief of Sta

Subject: Office of the Inspector General Draft Summary Report "Mobile Phone Security" (142314)—INFORMATION

Thank you for the opportunity to review the draft report. We agree with the recommendations. We will continue to make improvements that align our mobile phone security with emerging guidelines and best practices.

Please let me know if I can be of further assistance. You may direct staff inquiries to Trae Sommer at (410) 965-9102.

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

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:

Twitter: @TheSSAOIG

Facebook: OIGSSA

YouTube: TheSSAOIG

Subscribe to email updates on our website.