OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Report

The Social Security Administration's Process to Identify and Monitor the Security of Hardware Devices Connected to its Network

A-14-13-13050 | October 2013

OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: October 1, 2013 Refer To:

To: The Commissioner

From: Inspector General

Subject: The Social Security Administration's Process to Identify and Monitor the Security of Hardware Devices Connected to its Network (A-14-13-13050)

The attached final report presents the results of our audit. Our objective was to determine whether the Social Security Administration's process for identifying and monitoring hardware devices connected to its network effectively differentiated unapproved devices and ensured devices were at a reasonable system security level.

If you wish to discuss the final report, please call me or have your staff contact Steven L. Schaeffer, Assistant Inspector General for Audit, at (410) 965-9700.

Patrick P. O'Carroll, Jr.

Attachment

The Social Security Administration's Process to Identify and Monitor the Security of Hardware Devices Connected to its Network
A-14-13-13050

October 2013 **Office of Audit Report Summary**

Objective

To determine whether the Social Security Administration's (SSA) process for identifying and monitoring hardware devices connected to its network effectively differentiated unapproved devices and ensured devices were at a reasonable system security level.

Background

SSA's Fiscal Year 2012 *Federal Information Security Management Act of 2002* report stated that its automated processes identified 276,165 hardware devices connected to its network. SSA uses automated tools to provide the Department of Homeland Security with security metrics. The metrics include the number of hardware devices connected to the network, whether there are secure configuration baselines, and the number of certain security incidents detected.

We selected a sample of hardware devices identified by the Agency's network scanning tool to determine whether SSA approved these devices and the devices were operating at a reasonable system security level.

Our Findings

While the Agency has a process to identify hardware devices connected to its network, we determined the Agency's inventory was incomplete and inaccurate. Additionally, SSA did not approve all of the hardware devices connected to its network. Moreover, although SSA has processes to monitor the security level of connected devices, these processes were inconsistent with Agency policy in effect at the time of our audit.

Our Recommendations

We recommend the Agency:

1. Pursue implementing systems, through a risk-based process, to ensure only approved and security-compliant hardware devices are connected to its network.
2. Revise its policy to document who or which Agency component manages each hardware device connected to its network and is responsible for adequately securing these devices. The policy should better describe and define roles and responsibilities for monitoring security levels for all hardware devices.
3. Ensure hardware devices identified in this audit are at a reasonable security level.

SSA agreed with our recommendations.

TABLE OF CONTENTS

ABBREVIATIONS

DHS	Department of Homeland Security
FISMA	*Federal Information Security Management Act of 2002*
FY	Fiscal Year
ISSH	Information Systems Security Handbook
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
SP	Special Publication
SSA	Social Security Administration
TSRP	Telephone System Replacement Project
U.S.C.	United States Code

OBJECTIVE

Our objective was to determine whether the Social Security Administration's (SSA) process for identifying and monitoring hardware devices connected to its network effectively differentiated unapproved devices and ensured devices were at a reasonable system security level.[1]

BACKGROUND

Each Federal agency must submit an annual report to the Department of Homeland Security (DHS)[2] providing an overview of the adequacy and effectiveness of its information security policies, procedures, practices, and compliance with the *Federal Information Security Management Act of 2002* (FISMA) requirements.[3] SSA uses automated tools to provide DHS with security metrics. The metrics[4] include the number of hardware devices connected to the network, whether there are secure configuration baselines, and the number of certain security incidents detected. OMB includes these metrics, along with those of other Federal agencies, in its annual FISMA report to Congress.[5] SSA's Fiscal Year (FY) 2012 FISMA report[6] stated that its automated processes identified 276,165 hardware devices connected to its network, which it stated represented 100 percent of the hardware devices connected to its network.

SSA has an automated tool that scans its network and identifies hardware devices. This inventory is available at an Agency level. SSA stated that as of January 2013, it had about 326,000 hardware devices connected to its network.[7]

---

[1] For the purposes of this review, we defined a reasonable system security level to be one where the manufacturer supports the operating system and the device is at a current release.

[2] Office of Management and Budget (OMB), M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)*, July 6, 2010. Among its other responsibilities, DHS oversees the Government-wide and agency-specific implementation of, and reporting on, cyber-security policies and guidance.

[3] Pub. L. No. 107-347, Title III, Section 301 §3544(c)(1), 44 U.S.C. §3544(c)(1).

[4] These are a sample of the metrics reported to DHS.

[5] OMB, *Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002*, March 2013.

[6] SSA, *Chief Information Officer Section Report, 2012 Annual FISMA Report*.

[7] The Agency's network scanning tool provided this number and it represents the network addresses connected to the Agency's network. This does not represent the Agency's hardware inventory, as there could be multiple network addresses for a hardware device; and the network scanning tool cannot enumerate devices that are turned off. SSA stated it was replacing desktops and refreshing servers in January 2013. This explains the difference between what the Agency reported in its FY 2012 FISMA report, and the number they provided in January 2013 for this review.

OMB requires that agencies protect Government information commensurate with the risk and magnitude of harm that would result from its loss, misuse, or unauthorized access.[8] Agencies must remain vigilant to defend information systems, especially in a resource-constrained environment, while balancing system security with operational capability through a risk-management process.[9]

To achieve our objective, we reviewed SSA's processes for identifying and monitoring hardware devices connected to its network. We categorized the hardware devices based on the operating system provided by the Agency's network scanning tool. We selected a sample of hardware devices by the various categories to determine whether SSA approved these devices and the devices were operating at a reasonable system security level. For the purposes of this review, we defined a reasonable system security level to be one where the manufacturer supports the operating system and the device is at a current release. For additional scope and methodology, see Appendix A.

RESULTS OF REVIEW

While SSA has a process to identify hardware connected to its network, it needs to improve the process to comply with Federal requirements.[10] Although SSA stated it identified all hardware devices connected to its network, we determined the Agency's inventory of hardware devices was incomplete and inaccurate. Additionally, SSA did not approve all of the hardware devices connected to its network.[11]

Further, the Agency's processes for monitoring[12] reasonable system security levels for hardware devices connected to its network were inconsistent with SSA policy. Additionally, not all hardware devices were operating at a reasonable system security level.[13]

---

[8] OMB Circular No. A-130, Revised, (Transmittal Memorandum No. 4), *Management of Federal Information Resources*, 8.a.1.(g).

[9] DHS, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, FISMA 12-02, February 15, 2012.

[10] FISMA requires that Federal agencies comply with Federal Information Processing Standards and therefore agencies may not waive their use; they are compulsory and binding. National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006 requires agencies meet minimum security requirements through the use of security controls in accordance with NIST Special Publication (SP) 800-53. NIST SP 800-53 includes security controls for information system component inventory (CM-8).

[11] This represents sampled hardware devices where SSA could not provide acquisition documentation.

[12] Monitoring in the context of this review means to ensure the hardware device is at a reasonable security level.

[13] See Footnote 1.

Hardware Device Information Missing in Agency Systems

SSA provided a list of hardware devices connected to its network.[14] From this list, we selected 183 devices to review. We found that for 48 hardware devices, the device specifications,[15] machine name,[16] or network address[17] was incomplete. FISMA reporting requires that agencies report the number of hardware devices where SSA collects these details as part of asset management.[18] Additionally, Federal standards list these detailed items, along with others, as information to achieve effective property accountability.[19]

FISMA requires that Federal agencies secure information systems that support their operations and assets.[20] In doing so, agencies must assess the risk and magnitude of harm resulting from unauthorized access. Agencies must know what devices (authorized and unauthorized) are connected to its network so they can secure those devices. In its FY 2012 FISMA report to DHS, SSA reported it identified 100 percent of its hardware devices connected to its network. Per FY 2012 FISMA reporting guidance,[21] agencies must provide the number of devices for which they were able to collect the (1) network address, (2) machine name, and (3) unique hardware number or serial number.[22]

We used multiple SSA tools[23] to locate required hardware device information. For 85 (46 percent) of 183 sampled hardware devices, SSA's tools provided all required information. For 48 (26 percent) of 183 sampled hardware devices, 1 or more pieces of required information was missing[24] (see Appendix B for details). Further, we removed 50 (27 percent) of 183 hardware devices from our sample[25] (see Table 1). In addition, after we finished our fieldwork, we noted that SSA updated one of its tools to more easily provide the unique hardware number.

---

[14] See Footnote 7.

[15] Can include serial number or unique hardware number.

[16] The name assigned to a hardware device connected to the network.

[17] A unique way to identify the location of a hardware device on a network.

[18] DHS, *FY 2012 Chief Information Officer Federal Information Security Management Act Reporting Metrics*, p. 15.

[19] NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. F-44, CM-8.

[20] Pub. L. No. 107-347, Title III, Section 301 §3544(a)(2), 44 U.S.C. §3544(a)(2).

[21] DHS, Supra note 18, p. 15.

[22] This is a key FISMA metric, meaning the expected level of performance is adequate security.

[23] See Appendix A.

[24] Some hardware devices, by their nature, may not have one of the required pieces of information. In these cases, we did not count that as missing information for the sample.

[25] Thirteen sampled hardware devices were no longer connected to the network, and 37 sampled hardware devices were misidentified as described in the next section of the report.

Table 1 – Hardware Device Information in SSA's Systems

Availability of (1) Computer Network Address, (2) Machine Name, and (3) Unique Hardware Number or Serial Number	Number of Sampled Hardware Devices	Percent of Total Sampled Hardware Devices
All Information Available	85	46
One or More Pieces of Information Missing	48	26
Removed from Review[26]	50	27
TOTAL	**183**	**99***

* Numbers do not add up to 100 due to rounding.

Network Scanning Tool Unable to Provide Sufficient Hardware Identification

The Agency's network scanning tool[27] provided incorrect results for 40 (22 percent) of 183 sampled hardware devices. For example, the Agency's network scanning tool identified 37 (20 percent) of 183 sampled hardware devices as Toshiba digital copiers (an Input/Output peripheral), but we determined these devices were Telephone System Replacement Project (TSRP)[28] equipment. We reclassified the Toshiba digital copiers as TSRP telephones (see Table 2). In this instance, the misidentification of hardware equipment is a lower risk to the Agency since SSA monitors TSRP telephones but does not monitor Input/Output Peripherals.[29]

[26] Id.

[27] This tool uses weighted criteria to identify the operating system of hardware devices connected.

[28] TSRP is SSA's project to implement transport voice traffic (telephone calls) over its network.

[29] SSA stated it had not found a commercial tool to monitor Input/Output peripherals.

Table 2 – Hardware Devices Connected as of January 2013

Hardware Category[30]	Original Count	Original Percent of Total	New Count	Percent of Total
Desktop	131,561	40.36	131,561	40.36
Input/Output Peripheral	**92,647**	**28.42**	**18,032**	**5.53**
Network Device	48,803	14.97	48,803	14.97
TSRP Telephone	**17,037**	**5.23**	**91,652**	**28.12**
Multi-Platform	14,327	4.40	14,327	4.40
Server	11,154	3.42	11,154	3.42
[Unknown]	**4,940**	**1.52**	**4,940**	**1.52**
Appliance	3,097	0.95	3,097	0.95
Storage Device	1,050	0.32	1,050	0.32
Video Device	571	0.18	571	0.18
Virtual Machine	561	0.17	561	0.17
Server/iSeries	172	0.05	172	0.05
Uninterruptable Power Supply	58	0.02	58	0.02
Private Branch Exchange	3	0.00	3	0.00
TOTAL	**325,981**		**325,981**	**100***

* Numbers do not add up to 100 due to rounding.

As of January 2013, SSA had 4,940 hardware devices that were not associated with an operating system and were reported as "unknown" (see Table 2). When the Agency's network scanning tool cannot identify an operating system, it classifies the system as "unknown." This represented about 1.5 percent of all hardware devices connected to the Agency's network as of January 2013. In its FY 2012 FISMA report,[31] SSA stated that it could track the installed operating system vendor, product, version, and patch-level combination(s) in use on the hardware devices.[32]

We sampled 50 hardware devices categorized as unknown. Using SSA tools,[33] we determined that 17 (34 percent) of 50 sampled hardware devices were used in the TSRP implementation, and 10 (20 percent) of 50 were network devices. However, for 18 (36 percent) of 50 devices, we obtained some details about the operating system but not enough to identify the device. Finally, 5 (10 percent) of 50 unknown devices were no longer connected to SSA's network (see Table 3).

[30] Descriptions of the hardware categories are located in Appendix C.

[31] SSA, Supra, note 6.

[32] DHS, Supra, note18, p. 16, question 2.4.

[33] See Appendix A.

Table 3 - Unknown Hardware Devices

Identification Status	Number of Sampled Hardware Devices	Percent of Total Sampled Hardware Devices
Identified as TSRP Devices	17	34
Identified as Network Devices	10	20
Unable to Identify and Locate Device	18	36
Device no Longer Connected to Network	5	10
TOTAL	**50**	**100**

Because cyber-security is an important factor for agencies to provide essential services to citizens, in FY 2011 the Administration identified continuous monitoring[34] as one of three FISMA priorities.[35] Furthermore, DHS affirmed that asset management was one of the first areas where continuous monitoring needed to be developed. Agencies must know which hardware devices are connected before they can manage the devices for vulnerabilities.[36]

According to FY 2012 FISMA[37] reporting requirements, agencies must provide DHS the number of hardware devices connected to their respective networks where a computer-generated report provides Agency-level inventory information.[38] An accurate and current inventory, controlled by tools that scan network addresses managing configuration, can reduce the chance of attackers finding unauthorized and unprotected systems to exploit. To identify weaknesses, agencies rely on their ability to correctly identify the operating system of hardware devices. If the Agency cannot correctly identify the hardware devices connected to its network, it is unable to manage the necessary security controls.[39] However, the Agency uses layers of security – such as intrusion detection systems and system monitoring – to identify indicators of potential issues before they occur.

In January 2012, SSA developed a *Cyber Security Engineering Strategy*,[40] in which it stated the Agency plans to improve its ability to secure hardware devices by addressing ". . . audit findings in the area of network access controls to eliminate the ability for an unknown hardware device to

[34] Continuous monitoring is a technique to address the security impacts on an information system resulting from changes to the hardware, software, firmware, or operational environment.

[35] DHS, Supra, note18, p. 5.

[36] Id. at p. 17.

[37] Id. at p. 15.

[38] This control was selected as one of the highest impact controls for government-wide application based on input from multiple cyber security experts, who considered public, private, and intelligence threat information.

[39] DHS, Supra, note18, p. 17.

[40] SSA, *Cyber Security Engineering Strategy*, January 2012, p. 7.

attach to SSA's network." During our review period, SSA provided a presentation[41] in which it stated it is ". . . investigating the feasibility of implemented [sic] a Network Access Control Solution" to mitigate network access control findings. According to the Agency, ". . . this solution will verify all systems meet SSA configuration requirements prior to being permitted to access production network resources." We believe the Agency should pursue implementing systems, through a risk-based process, to ensure only approved and security-compliant hardware devices are connected to its network.

Not All Hardware Devices Are Approved for Connection to the Network

We reviewed a sample of 162 hardware devices to determine whether SSA approved them to be connected to its network.[42] We found that SSA had not approved all of the devices we reviewed. Per SSA's Information Systems Security Handbook (ISSH),[43] hardware devices are considered approved to be connected to the Agency's network as long as they are procured through an SSA-sanctioned requisition process.[44] However, SSA has no approval process ensuring hardware devices are adequately secured after purchase. According to FISMA, Federal agencies are required to provide information security to reduce the risk of unauthorized access.[45] Also, Federal guidelines[46] state agencies should include in their inventories, information deemed necessary by the organization to achieve effective property accountability; this can include system owner.[47] More specifically, FISMA reporting requirements state that a hardware device is approved when it is assigned to a particular person or group at a low enough level to ensure effective responsibility and security.

For 55 (34 percent) of 162 sampled hardware devices, we verified that SSA approved the hardware connected to its network. We found 82 (51 percent) of 162 sampled hardware devices were not approved before they were connected to the Agency's network.[48] For 25 (15 percent) of 162 sampled hardware devices,[49] there was not enough information to determine whether the devices were approved (see Table 4). There was not enough information because SSA's processes to identify a system owner were inconsistent and undocumented.

---

[41] SSA, *Office of Information Security, Division of Technical Operations.*

[42] See Appendix A for sampling methodology.

[43] SSA, ISSH Version 2.7, April 2013 § 11.3.1.

[44] SSA's procurement process does not ensure the device is secure.

[45] Pub. L. No. 107-347, Title III, Section 301, 3544(a)(2)(A) – (C), 44 U.S.C. §3544(a)(2)(A) – (C).

[46] NIST SP 800-53 Revision 3, August 2009, p. F-44, CM-8(a).

[47] An individual or organizational unit responsible for the operation and maintenance of hardware device.

[48] This represents sampled hardware devices where SSA could not provide acquisition documentation.

[49] Twenty-two of these were part of the unknown hardware category.

Table 4 –Approving Hardware Devices

State	Number of Sampled Hardware Devices	Percent of Total Sampled Hardware Devices
Approved to be Connected	55	34
Not approved to be Connected	82	51
Not Enough Information Available	25	15
TOTAL	**162**	**100**

It is essential to ensure hardware devices operate as intended. SSA cannot achieve this without proper policies and procedures to ensure hardware devices are approved prior to installation. SSA stated it has layers of security controls in place to reduce the probability of threat. However, a key goal of managing hardware is to identify and remove unmanaged hardware devices before they can be exploited and used to attack other assets.[50] In July 2013, after completion of our fieldwork, SSA implemented a revised policy[51] for managing hardware, software, and platform configuration. We reviewed the revised policy and believe it begins to address our concerns but is still vague on who manages all of the hardware devices. We believe SSA should revise its policy to document who or which Agency component manages each hardware device connected to its network and is responsible for adequately securing the device.

Monitoring Process Inconsistent with Policy

The Agency had processes for monitoring[52] most hardware devices connected to its network to ensure they operate at a reasonable system security level. However, the processes were inconsistent with policy in effect during our audit period. Further, SSA did not have processes to monitor input/output peripherals, appliances, or uninterruptable power supplies – about 6 percent of the hardware devices connected to its network. We found that groups in SSA's Headquarters monitored 59 of 162 sampled hardware devices.[53] We found that SSA local managers (outside the Office of Systems) were responsible for monitoring 9 of the 162 sampled hardware devices. However, managers we interviewed did not understand they were responsible for monitoring the sampled devices, so they did not monitor security in compliance with SSA's ISSH.[54] There was

[50] DHS, Supra, note 18, p. 17, ". . . an underlying assumption is that if hardware devices are unmanaged, they are probably vulnerable, and will be exploited if not removed or approved quickly."

[51] SSA, ISSH Version 3.1, July 2013 § 11.5.

[52] There are many types of monitoring for hardware devices. Monitoring in the context of this review means to ensure that the hardware device is at a reasonable system security level.

[53] Includes desktops, network devices, and Server/iSeries.

[54] SSA, ISSH Version 2.7, April 2013, Chapter 11 § 11.3.4.

not enough information to determine whether SSA monitored the remaining 94 sampled devices[55] (see Table 5).

Table 5 – Monitoring Hardware Devices

State	Number of Sampled Hardware Devices	Percent of Total Sampled Hardware Devices
Centrally Monitored	59	36
Locally Assigned	9	6
Not Enough Information Available	94	58
TOTAL	**162**	**100**

We determined that, of the 59 centrally monitored hardware devices, 55 were at a reasonable system security level. However, SSA did not have sufficient information to make a determination on the remaining four hardware devices. For the nine sampled hardware devices assigned to local managers, four were not at a reasonable system security level and five did not have enough information for us to make a determination. For the remaining 94 hardware devices, we could not verify whether those devices were at a reasonable system security level. [56]

SSA's ISSH states that local managers are responsible for monitoring the use of approved non-standard hardware.[57] Moreover, SSA's ISSH[58] states local managers are responsible for securing SSA-owned hardware. However, local staff we interviewed stated Headquarters or the regional offices were responsible for monitoring hardware devices for reasonable system security levels. Within the Office of Systems, the Office of Information Security develops and maintains information security policies, standards, and procedures. The Office of Information Security also manages the reporting and monitoring processes that ensure compliance with Government policies. Additionally, the Office of Telecommunications and Systems Operations provides the telecommunications infrastructure and network security and policies. SSA's policies, in effect at the time of our audit, are not clear on who is responsible for monitoring the hardware devices to ensure they operate at a reasonable security level. In July 2013, after completion of our fieldwork, SSA revised its policy, but the policy does not define roles and responsibilities for monitoring the security of hardware devices.

---

[55] For 50 sampled hardware devices (TSRP telephones), SSA did not monitor these hardware devices for security compliance, but stated that a TSRP telephone must meet the established security configuration before it can connect to the network. SSA did not provide documentation to support that it installed the phones at a reasonable security level. SSA could not locate 2 hardware devices, identify the owner of 21 hardware devices, and provide documentation for 24 hardware devices.

[56] For 23 hardware devices, we could not locate the device to identify its system security level. For 71 of the hardware devices, the Agency was unable to provide documentation showing the system security level.

[57] SSA, ISSH Version 2.7, April 2013, Chapter 11 § 11.3.4.a. Per SSA, non-standard hardware is purchased by local offices.

[58] Id., Chapter 11 § 11.3.4.f.

Federal guidelines[59] recommend that the Agency group that monitors security should define which hardware devices and operating systems they support and clearly communicate this information to those who manage technical aspects – for SSA, this includes local managers. Additionally, local support staff ". . . should be taught how to independently monitor and remediate unsupported hardware equipment, operating systems, and software applications."[60]

We believe the Agency should resolve the inconsistencies among its policies and procedures for monitoring hardware devices. Additionally, SSA should revise its policy to better describe and define roles and responsibilities for monitoring security levels for all hardware devices. Finally, SSA should ensure the hardware devices identified in this audit are at a reasonable security level.

CONCLUSIONS

According to DHS, cyber security is constantly shifting because of the relentless and dynamic threat environment, emerging technologies, and new vulnerabilities.[61] Therefore, Federal agencies must remain vigilant to defend information systems, especially in a resource-constrained environment, balancing system security with operational capability.

While the Agency has a process to identify hardware devices connected to its network, we determined the Agency's inventory was incomplete and inaccurate. Additionally, SSA did not approve all of the hardware devices connected to its network. Moreover, although SSA has processes to monitor the security level of connected devices, these processes were inconsistent with Agency policy in effect at the time of our audit.

RECOMMENDATIONS

We recommend the Agency:

1. Pursue implementing systems, through a risk-based process, to ensure only approved and security-compliant hardware devices are connected to its network.

2. Revise its policy to document who or which Agency component manages each hardware device connected to its network and is responsible for adequately securing these devices. The policy should better describe and define roles and responsibilities for monitoring security levels for all hardware devices.

3. Ensure hardware devices identified in this audit are at a reasonable security level.

---

[59] NIST SP 800-40 Version 2.0, *Creating a Patch and Vulnerability Management Program*, November 2005, p. 2-6, 2.2.3.1.

[60] Id.

[61] DHS, Supra, note 18, p. 4.

AGENCY COMMENTS

SSA agreed with our recommendations. See Appendix D for the full text of the Agency's comments. In addition to the formal comments, SSA provided a technical comment, which has been addressed, where appropriate, in this report.

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

To accomplish the audit objective, we:

- Reviewed applicable Federal laws, regulations, guidelines, and standards as well as Social Security Administration (SSA) policies and procedures.
- Reviewed *Federal Information Security Management Act of 2002* (FISMA) reporting requirements, and SSA's Chief Information Officer section of the 2012 annual FISMA report.
- Reviewed prior Office of the Inspector General reports.
- Obtained a list of the 325,981 hardware devices connected to SSA's network as of January 2013 and categorized them by operating system for sampling (see Table 2).
- Selected a random sample of 183 hardware devices (see Hardware Device Sample section below).
- Attempted to determine the system owner and location of the sampled hardware devices and device details (computer network address, machine name, unique hardware number) using the following SSA developed tools *IP Address to Switch Port*, *IP Address Mapping Tool*, *OTSO Networking Database* and *PinView*; and SSA's implementation of *Microsoft System Center Configuration Manager 2007*.
- Attempted to determine the actual type of hardware device for the "unknown" samples.
- Interviewed system owners of the sampled hardware devices and obtained screen shots and procurement documentation.
- Analyzed data obtained.
- Compared the operating system version and release level to the most recent versions and releases supported by the manufacturer; we did not look at the specific system configuration of the hardware.

We obtained a sufficient understanding of information systems controls as they related to this review. We assessed the completeness, accuracy, and validity of the data from the scanning tools. We determined the data from SSA's network scanning tool were sufficient to enumerate hardware devices.

We conducted our audit from November 2012 through April 2013 in Baltimore, Maryland. The entities reviewed were the Offices of Budget, Finance and Management; Disability Adjudication and Review; Operations; and Systems. 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Hardware Device Sample

In its FY 2012 FISMA report,[1] the Agency identified 276,165 hardware devices[2] connected to its network. We obtained a more recent list and sorted the devices into 14 categories (see Table 2).

Based on the ZIP code provided by the Agency, we identified hardware devices within a 50-mile radius of an audit office; this was approximately 39 percent of the total population. Because of limited budget resources, we decided Office of Audit staff could conduct the interviews and on-site inspections within a 50-mile radius of their office. However, during our review, we decided to conduct telephone interviews of local staff to save additional monies. From the list of hardware devices within a 50-mile radius of an audit office, we randomly selected 50 items each from the Desktop and Input/Output peripheral categories (100 sample items), since they were the 2 categories that comprised 50 percent of the total population. We randomly selected 50 unknown hardware devices. We also randomly selected 3 items from the remaining 11 categories (33 sample items). The total sample size was 183.

We attempted to identify a system owner[3] for each of the sampled hardware devices from the network address[4] provided by the Agency's network scanning tool. The Agency did not have a tool to identify a system owner based on the network address of a device. Instead, SSA identified tools to assist us in our research but stated the tools were not designed for this function. As we conducted our review, we removed nine sampled hardware devices from our population because the devices moved on the network. For these sampled hardware devices, we were unable to determine whether the hardware device was the same hardware device identified during the original network scan results received from SSA. As a result, our sample size decreased from 183 to 174.

Because SSA's scanning tool incorrectly identified some Input/Output peripherals, we reclassified those devices based on what the devices actually were— Telephone System Replacement Project (TSRP) equipment (see Table 2). Consequently, the percentage of hardware devices categorized as Input/Output Peripherals and TSRP telephone categories changed. TSRP telephone was now the second largest hardware category (originally it was fourth), and Input/Output Peripherals were fourth (originally second)—effectively the categories switched places. In this instance, the misidentification of hardware equipment is a lower risk to the Agency, since SSA monitors TSRP telephones but does not monitor Input/Output Peripherals. Because of this adjustment for percent of total in 2 hardware categories, we changed our sample; reducing it to 177 hardware devices.

---

[1] SSA, *Chief Information Officer Section Report, 2012 Annual FISMA Report.*

[2] The FY 2012 FISMA population and the most recent inventory difference may be due to purchases and retirement as well as devices and networks that are off, not operational, or disconnected from the network.

[3] Person responsible for the operation and maintenance of the hardware device.

[4] A unique way to identify the location of a hardware device on a network.

Additionally we found some hardware devices were removed from the network. Therefore, we altered our sample size from 183 to 162 hardware devices as shown in Table A-1 below.

Table A–1: Sample Size Changes

Reason for Change	Added	Removed	Sample Size
Starting Sample Size			**183**
Hardware Devices Moved on the Network		9	173
Incorrectly Identified Input/Output Devices		37	137
Extra Input/Output Peripheral Samples		7	130
Extra Telephone System Replacement Project Samples		3	127
New Telephone System Replacement Project Samples[5]	50		177
Devices No Longer Connected to the Network		15	162
Ending Sample Size			**162**

[5] Since they were one of the two hardware categories that now made up 50 percent of the total population.

Appendix B – Missing Device Identifiers

The following table details the hardware categories and the missing identifying information (machine name, serial number, unique hardware number).[1] Knowing all identifying information helps the Agency rapidly find the specific security control for hardware equipment that has been compromised or breached or is in need of mitigation. Additionally, it can aid in determining location of, and person responsible for, the hardware equipment.

Missing Information	Desktop	I/O Peripheral	Multi-Platform	Server	UPS	Video Device	Unknown	TSRP Phone	Appliance	Storage Device	Virtual Machine	Server (iSeries)	Total
Machine Name Only			2	1			13		1	3			20
Serial Number Only							9						9
Unique Hardware Number and Serial Number							6	2				2	10
Machine Name, Unique Hardware Number, and Serial Number	1		1			1	6						9
TOTAL	1		3	1		1	34	2	1	3		2	48

[1] The machine name is the name assigned to a hardware device connected to the network.

Appendix C – GLOSSARY OF TERMS

This section provides a glossary of terms used within this report. While these terms may have broader definitions, we defined them as we used them in the context of this review.

Adequate Security/Adequately Secure – security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information, assuring that systems operate effectively and provide appropriate confidentiality, integrity, and availability. [1]

Appliance – see Hardware Category.

Approved to be Connected – any item procured through an SSA-sanctioned requisition process.

Asset Management –activities across the enterprise related to items that have value (to include, but not limited to, information technology systems, hardware, software, and networks).

Automated capability – product or report is generated by a computer.[2]

Continuous Monitoring – a technique to address the security impacts on an information system resulting from changes to the hardware, software, firmware, or operational environment.[3]

Cyber-Attack – an attempt to disrupt, disable, destroy, or maliciously control a computer environment; or destroy the integrity of or steal the data on a computer network or system.

Cyber Security – measures taken to protect a computer or computer system against unauthorized access or cyber-attack.

Desktop – see Hardware Category.

Digital Copiers – device that uses optical technology to scan documents, store the image, and then print the stored image.

Hardware Category – groups used to classify SSA's hardware devices.

---

[1] Office of Management and Budget Circular No. A-130, Appendix III, *Security of Federal Automated Information Resources*, A.2.a

[2] Department of Homeland Security, *FY 2012 Chief Information Officer Federal Information Security Management Act Reporting Metrics*, p. 19.

[3] National Institute of Standards and Technology SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010, page G-1.

Appliance – hardware designed for a specific information technology function in a closed architecture that may contain an operating system, storage, and specific applications; they may be external to a hardware device or internal (embedded devices).

Desktop –a type of computer used in a stationary location.

Input/Output Peripheral – device assigned a network address that inputs or outputs data.

Multi-Platform – devices whose operating system could run on hardware devices falling into more than one hardware category on SSA's network.

Network Devices – includes routers, switches, load balancers, and firewalls.

Private Branch Exchange – an in-house telephone switching system hat interconnects telephone extensions.

Server – computer on a network that manages access to a centralized resource or services in a network.

Server/iSeries – is IBM's (AS/400) midrange server.

Storage Device – hardware devices capable of holding information and includes disk storage, tape drives and tape libraries.

TSRP Phone – telephones deployed in SSA's implementation to transport voice traffic over its network.

Uninterruptable Power Supply – device that provides backup power when the electrical power fails or drops to an unacceptable voltage level.

[Unknown] – devices for which the operating system could not be determined when scanned to identify the population of devices connected to the Agency's network.

Video Devices – includes video equipment for the audio-video conferencing as well as the cameras used for security.

Virtual Machine – software that emulates a physical computing environment.

Hardware Device – includes any machine assigned a network address and connected to the Agency's network.

Input/Output Peripheral – see Hardware Category.

Machine Name – the name assigned to a hardware device connected to the network.

Multi-Platform – see Hardware Category.

Network Address – unique way to identify the location of a hardware device on a network.

Network Devices – see Hardware Category.

Network Scanning Tool – application that examines the network systematically to obtain data about connected hardware devices.

Operating System – software that controls the processes of a hardware device.

Sanctioned Requisition Process – term used within SSA's Information Systems Security Handbook to describe how SSA procures hardware devices.

Security Controls – safeguards and countermeasures prescribed for IT systems designed to protect the confidentiality, integrity, and availability of information processed, stored, and transmitted by those IT systems.

Server – see Hardware Category.

Server/iSeries – see Hardware Category.

Storage Device – see Hardware Category.

Switch – a device that channels data and determines its intended hardware destination.

System Monitoring – collection and display of real-time performance data for a local computer or remote computers according to defined criteria.

System Owner – the individual or organizational unit responsible for the operation and maintenance of the hardware device.

System Security Level – operating system version and release supported by manufacturer.

Threat environment – the circumstances, objects, or conditions by which surround the potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

Uninterruptable Power Supply – see Hardware Category.

Unknown Hardware Devices – see Hardware Category.

Unmanaged Devices – devices not assigned to a particular person or group at such a level as to effectively assign responsibility.

Video Devices – see Hardware Category.

Virtual Machine – see Hardware Category.

Appendix D– AGENCY COMMENTS

SOCIAL SECURITY

MEMORANDUM

Date: September 13, 2013 Refer To: S1J-3

To: Patrick P. O'Carroll, Jr.
Inspector General

From: Katherine Thornton /s/
Deputy Chief of Staff

Subject: Office of the Inspector General Draft Report, "The Social Security Administration's Process to Identify and Monitor the Security of Hardware Devices Connected to its Network" (A-14-13-13050)--INFORMATION

Thank you for the opportunity to review the draft report. Please see our attached comments.

Please let me know if we can be of further assistance. You may direct staff inquiries to Gary S. Hatcher at (410) 965-0680.

Attachment

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL DRAFT REPORT, "THE SOCIAL SECURITY ADMINISTRATION'S PROCESS TO IDENTIFY AND MONITOR THE SECURITY OF HARDWARE DEVICES CONNECTED TO ITS NETWORK" (A-14-13-13050)

Recommendation 1

Pursue implementing systems, through a risk-based process, to ensure only approved and security-compliant hardware devices are connected to its network.

Response

We agree. We will continue our efforts to pursue, procure, and implement solutions to ensure the identification of connected devices on our network. We have implemented the foundational steps in enumerating all connected devices to identify if they are authorized or unauthorized. With our recently implemented Hardware, Software, and Platform Configuration Policy, we provide clear guidance for security compliance, requiring users to select from an authorized list of hardware, software, and platforms that follow security configuration guidelines. Our new policy was a prerequisite for any additional enhancement in ensuring only security compliant devices are connected.

Recommendation 2

Revise its policy to document who or which Agency component manages each hardware device connected to its network and is responsible for adequately securing the device. The policy should better describe and define roles and responsibilities for monitoring security levels for all hardware devices.

Response

We agree. On July 19, 2013, we published a revised Information Systems Security Handbook, combining Chapter 11, "Hardware, Software, and Platform Configuration Policy" with Chapter 17, "Removable Media and Protection from Data Loss." However, the revised policy clearly addresses the issues of hardware security levels by using and relying on agency standard configurations and states the expectations and responsibilities of the Information Technology (IT) Security Staff, local managers and system owners for these as well as for any approved exceptions.

Recommendation 3

Ensure hardware devices identified in this audit are at a reasonable security level.

Response

We agree. We have implemented an effective penetration-testing program to complement the existing processes for identifying vulnerabilities. The penetration-testing program assists in identifying security gaps that may still exist in the overall IT security program, defining areas of necessary improvements. We are confident the penetration-testing program will assist us in identifying vulnerabilities and reducing the risks to our IT systems.

Appendix E – Major Contributors

Brian Karpe, Director, Information Technology Audit Division

Mary Ellen Moyer, Audit Manager, Information Technology Audit Division

Jan Kowalewski, Auditor in Charge

Cheryl Dailey, Auditor

MISSION

By conducting independent and objective audits, evaluations, and investigations, the Office of the Inspector General (OIG) inspires public confidence in the integrity and security of the Social Security Administration's (SSA) programs and operations and protects them against fraud, waste, and abuse. We provide timely, useful, and reliable information and advice to Administration officials, Congress, and the public.

CONNECT WITH US

The OIG Website (http://oig.ssa.gov/) gives you access to a wealth of information about OIG. On our Website, you can report fraud as well as find the following.

- OIG news
- audit reports
- investigative summaries
- Semiannual Reports to Congress
- fraud advisories
- press releases
- congressional testimony
- an interactive blog, "Beyond The Numbers" where we welcome your comments

In addition, we provide these avenues of communication through our social media channels.


Watch us on YouTube


Like us on Facebook


Follow us on Twitter


Subscribe to our RSS feeds or email updates

OBTAIN COPIES OF AUDIT REPORTS

To obtain copies of our reports, visit our Website at http://oig.ssa.gov/audits-and-investigations/audit-reports/all. For notification of newly released reports, sign up for e-updates at http://oig.ssa.gov/e-updates.

REPORT FRAUD, WASTE, AND ABUSE

To report fraud, waste, and abuse, contact the Office of the Inspector General via

Website:	http://oig.ssa.gov/report-fraud-waste-or-abuse
Mail:	Social Security Fraud Hotline P.O. Box 17785 Baltimore, Maryland 21235
FAX:	410-597-0118
Telephone:	1-800-269-0271 from 10:00 a.m. to 4:00 p.m. Eastern Standard Time
TTY:	1-866-501-2101 for the deaf or hard of hearing