

Audit Report

The Social Security Administration's
Reporting Under the Federal
Information Security Modernization
Act

MEMORANDUM

Date: June 2, 2021 **Refer To:**

To: The Commissioner

From: Inspector General

Subject: The Social Security Administration's Reporting Under the Federal Information Security Modernization Act (A-14-18-50450)

The attached final report presents the results of the Office of Audit's review. The objective was to determine whether the Social Security Administration's (SSA) responses to the end of Fiscal Year (FY) 2019 Chief Information Officer (CIO) *Federal Information Security Modernization Act of 2014* (FISMA) metrics were reliable.

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



Gail S. Ennis

Attachment

The Social Security Administration's Reporting Under the Federal Information Security Modernization Act

A-14-18-50450



June 2021

Office of Audit Report Summary

Objective

To determine whether the Social Security Administration's (SSA) responses to the end of Fiscal Year (FY) 2019 Chief Information Officer (CIO) *Federal Information Security Modernization Act of 2014* (FISMA) metrics were reliable.

Background

FISMA requires that the head of each Federal agency 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.”

Under FISMA, *Chief Financial Officers Act* agencies—including SSA—are required to respond quarterly to security posture questions, referred to as CIO metrics. The metrics assess agencies’ implementation of information security capabilities in various risk areas and measure their effectiveness. Risk areas include management of assets, configurations, vulnerabilities, access, and incidents. Agencies are required to submit metrics data using CyberScope. The Office of Management and Budget compiles agencies’ metrics into the Annual FISMA Report to Congress.

In 2019, agencies needed to respond to 87 metrics.

Findings

SSA provided sufficient documentation to support its responses to 14 of the 45 CIO metrics we sampled but was unable to support its responses to 12 metrics because it did not have a process in place to retain evidence to corroborate these responses. In addition, the Agency provided incorrect responses for 19 metrics. We were unable to determine whether the 12 unsupported CIO metric responses were reliable and determined that the 19 incorrect metric responses were not reliable. Without reliable data, OMB and Congress may not be able to properly assess the state of SSA’s cybersecurity. The Agency stated it plans to enhance its processes to capture the point-in-time evidence of its CIO metric reporting.

Agency Actions Resulting from the Audit

As of February 2021, the Agency had enhanced its process to collect artifacts, including the date of data collection, the description of how the reported values were obtained (including the tool used), and screen shots of the original information when available. The Agency also created a site to retain the evidence to support its responses to the metrics.

Because SSA has taken steps to improve its processes, we are not making any recommendations.

TABLE OF CONTENTS

Objective.....	1
Background	1
The Social Security Administration's Metric Reporting Process	3
Recordkeeping Requirements	3
Scope and Methodology	3
Results of Review	4
Identify.....	5
Protect	7
Detect	9
Respond.....	9
Recover	10
Agency Actions Resulting from the Audit.....	10
Appendix A – Scope and Methodology	A-1
Appendix B – Sampled Metric Responses	B-1
Appendix C – Agency Comments.....	C-1

ABBREVIATIONS

ATO	Authorization to Operate
CIO	Chief Information Officer
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
FISMA	<i>Federal Information Security Modernization Act of 2014</i>
FY	Fiscal Year
GFE	Government Furnished Equipment
IaaS	Infrastructure as a Service
OIG	Office of the Inspector General
OIS	Office of Information Security
OMB	Office of Management and Budget
PaaS	Platform as a Service
SSA	Social Security Administration
SaaS	Software as a Service

OBJECTIVE

Our objective was to determine whether the Social Security Administration's (SSA) responses to the end of Fiscal Year (FY) 2019 Chief Information Officer (CIO) *Federal Information Security Modernization Act of 2014* (FISMA) metrics were reliable.

BACKGROUND

FISMA requires that *Chief Financial Officers Act* agencies—including SSA—respond quarterly to security posture questions, referred to as CIO metrics.¹ While these are titled CIO metrics, FISMA requires that head of each Federal agency 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.² The metrics assess agencies’ implementation of information security capabilities in various risk areas, and measure their effectiveness. Risk areas include management of assets, configurations, vulnerabilities, access, and incidents as well as data and boundary protection. In 2019, agencies needed to respond to 87 metrics.

Agencies are required to submit metrics data using the Department of Homeland Security’s (DHS) CyberScope platform, a Web-based application designed to streamline information technology security reporting for Federal agencies. CyberScope gathers and standardizes data from Federal agencies to support FISMA compliance. The Office of Management and Budget (OMB) and DHS compile agencies’ metric responses into the Annual FISMA Report to Congress and may use the “. . . reporting to compile agency-specific or government-wide risk management assessments.”³

Each year OMB releases a report to the public regarding the state of Federal cybersecurity, including recommended actions to congress and the Federal agencies, which are informed by agency responses. CIO metrics help agencies and OMB to fulfill congressional reporting requirements. OMB also uses the CIO metrics responses to construct ratings for Risk Management Assessments.⁴ When considering the need for additional cybersecurity funding for agencies, OMB considers performance in the Risk Management Assessment. Finally, OMB uses

¹ FISMA, Pub. L. No. 113-283, § 3554(a)(1)(B), 128 Stat. 3073, p. 3078 (2014); Office of Management and Budget, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, M-19-02, section I, part I, p. 2 (October 25, 2018).

² FISMA, Pub. L. No. 113-283, § 3554(a), 128 Stat. 3073, p. 3078 (2014).

³ Office of Management and Budget, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, OMB M-19-02, section I, part I, p. 2 (October 25, 2018).

⁴ Cybersecurity risk management comprises the full range of activities undertaken to protect information technology and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting information technology and data, and to mitigate the impact of, respond to, and recover from incidents.

responses to the CIO metrics when considering policy areas to address or update and to track progress on and evaluate the success of those policies.

Since FY 2016, OMB and DHS have organized the CIO metrics around the Cybersecurity Framework's five functions.⁵

1. Identify – develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities to assist agencies with their inventory of the hardware and software systems and assets that connect to their networks. Identifying these systems and assets helps agencies facilitate their management of cybersecurity risks to systems, assets, data, and capabilities.
2. Protect – develop and implement appropriate safeguards to ensure delivery of critical services to ensure agencies safeguard their systems, networks, and facilities with appropriate cybersecurity defenses. This supports agencies' ability to limit or contain the impact of potential cybersecurity events.
3. Detect – develop and implement appropriate activities to identify the occurrence of a cybersecurity event to assess the extent the agencies can discover cybersecurity events in a timely manner. This enables the timely discovery of cybersecurity events.
4. Respond – develop and implement appropriate activities to take action regarding a detected cybersecurity incident to ensure that agencies have policies and procedures in place that detail how their enterprise will respond to cybersecurity events. This supports the ability to contain the impact of a potential cybersecurity incident.
5. Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. This supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

The five functions “. . . aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving [cybersecurity activities] by learning from previous activities. The functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity.”⁶ Agencies should perform the functions concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk.⁷

⁵ DHS, *FY 2019 CIO FISMA Metrics Version 1*, p. 2 (December 2018).

⁶ National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, p. 6 (April 2018).

⁷ National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, p. 7 (April 2018).

The Social Security Administration's Metric Reporting Process

SSA's Division of Compliance and Assessments within the Office of Information Security (OIS), Office of the Deputy Commissioner of Systems, collects and reports all of the information required for the Agency's submission to CyberScope. SSA's CIO, Chief Information Security Officer, and Deputy Chief Information Security Officer are ultimately responsible for ensuring the Agency submits accurate and supported information.

OIS collected the data for the fourth quarter of FY 2019 from points of contact, compared them to the values entered for the third quarter, and asked the points of contact to explain increases of 10 percent or greater and decreases of 5 percent or greater. SSA's senior managers—including the CIO and Chief Information Security Officer—reviewed and approved the metric responses, and OIS submitted them in CyberScope in October 2019.

Recordkeeping Requirements

According to the National Archives and Records Administration, an Agency has to keep records related to FISMA submissions for 5 years or longer if retention is required for business use.⁸

Scope and Methodology

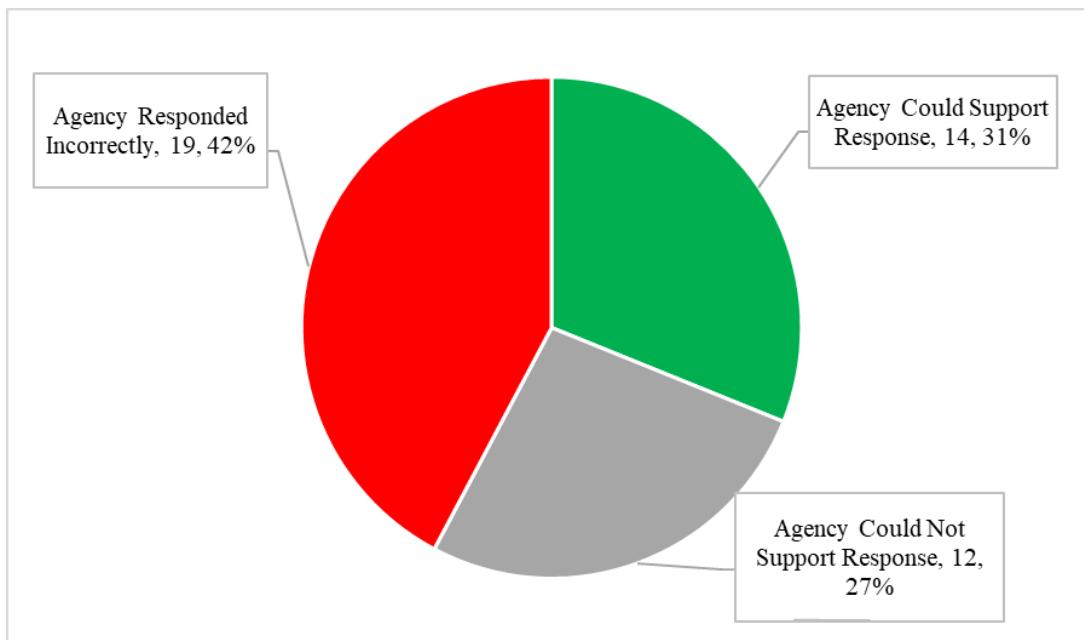
To achieve our objective, we interviewed Agency personnel responsible for responding to the CIO metrics; reviewed the Agency's underlying processes for responding to CIO metrics; and sampled 45 of the 87 metrics to verify that SSA had support for its FY 2019 fourth quarter responses. In selecting our sample, we selected metrics based on issues identified in previous OIG audits, objective evidence the audit team could readily verify, and past CIO responses applied to several metrics. We ensured our sample contained at least one metric from each function. We reviewed evidence to support the SSA's responses to the sampled metrics. See Appendix A for more details on our scope and methodology.

⁸ National Archives and Records Administration, *The General Records Schedules, Transmittal 31*, schedule 4.2, item 080, page 53 (April 2020).

RESULTS OF REVIEW

SSA provided sufficient documentation to support its responses to 14 of the 45 metrics we sampled but was unable to support its responses to 12 metrics because it did not have a process in place to retain the supporting evidence. The Agency provided incorrect responses for the remaining 19 metrics. We were unable to determine whether the 12 unsupported CIO metric responses were reliable and determined that the 19 incorrect metric responses were not reliable. Without reliable data, OMB and Congress may not be able to properly assess the state of SSA's cybersecurity. (For our sample results, see Figure 1.)

Figure 1: Conclusions on Sample CIO Metrics



Identify

We sampled 16 of the 19 metrics in this function. While SSA was able to support its responses for seven metrics, it could not support its responses or provided incorrect responses for nine others; see Table 1.⁹

Table 1: Unsupported or Incorrect Metrics for *Identify* Function

Number	Metric	Conclusion
Systems		
1.1.1	Number of operational unclassified information systems by organization categorized at the Organization - Operated Systems level.	Incorrect
1.1.2	Number of operational unclassified information systems by organization categorized at the Contractor - Operated Systems level.	Incorrect
1.1.3	Number of Systems (from 1.1.1 and 1.1.2) with Security Authorization to Operate (ATO). ¹⁰	Incorrect
Hardware		
1.2	Number of hardware assets connected to the organization's unclassified network(s). (Note: 1.2. is the sum of 1.2.1. through 1.2.3.)	Incorrect
1.2.1	Number of Government Furnished Equipment ¹¹ (GFE) endpoints. ¹²	Incorrect
1.2.4	Number of GFE hardware assets (from 1.2.1 – 1.2.3) covered by an automatic hardware asset inventory capability (for example, scans/device discovery processes) at the enterprise level.	Incorrect
1.2.5	Number of GFE endpoints (from 1.2.1) covered by an automated software asset inventory capability at the enterprise level.	Incorrect
Mobile Devices		
1.3.3	Number of mobile devices operating under enterprise-level mobile device management (GFE).	Unsupported
Cloud Services		
1.4	Report the types of Cloud Services your agency is using by cloud service provider(s) and service(s) you are receiving (for example, mail, database, etc.).	Incorrect

⁹ See Appendix B for the full list of metrics we sampled.

¹⁰ An ATO is the official management decision given by a senior official to authorize operation of an information system. National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations, Special Publication 800-37, revision 2*, Appendix B, p. 91 (December 2018).

¹¹ This is equipment owned and used by the Government or made available to a contractor.

¹² This includes servers, workstations, and virtual machines that can be identified by Internet Protocol address or any other method to communicate to the network.

Following are examples of metrics for which SSA could not support its responses or provided incorrect responses.

Systems

In response to metric 1.1.3, SSA reported 26 systems had Security ATOs at the end of FY 2019. However, in the first quarter of FY 2020, the Agency more than doubled the total number of systems to 54. Additionally, three systems¹³ did not have current Security ATOs because they expired before the end of FY 2019. Finally, the Agency did not include cloud systems in its fourth quarter FY 2019 response; therefore, the Agency incorrectly reported the number of systems that had Security ATOs. OIS informed us “In [the fourth quarter of] FY 2019, the Agency reported the major systems. In [the first quarter of] FY 2020, the Agency reported all systems with a Security ATO.” The Agency made these changes after consultation with DHS’ Federal Network Resiliency team (now the Cybersecurity and Infrastructure Security Agency).

Hardware

In response to metrics 1.2 and 1.2.1, SSA reported there were 273,144 hardware assets and 141,658 endpoints connected to its network at the end of FY 2019. SSA provided evidence that showed it incorrectly reported the number of hardware assets and endpoints. The Agency discovered it had included the number of mobile devices in the counts for these metrics and, as a result, metrics 1.2 and .1.2.1 were incorrect.

Mobile Devices

In response to metric 1.3.3, SSA reported 3,429 mobile devices were operating under enterprise-level mobile device management at the end of FY 2019. However, OIS could not provide evidence to support this amount because it had not retained it and was unable to reproduce it.

Cloud Services

In response to metric 1.4, SSA reported it had 8 Cloud Service Providers and 12 Cloud Service Offerings at the end of FY 2019. In addition, for each of these, the Agency reported the ATO date and service type. SSA’s inventory, however, included 10 Cloud Service Providers and 21 Cloud Service Offerings. Finally, the ATO dates the Agency reported for five systems did not match the dates in the Agency’s inventory. OIS acknowledged it did not have a complete inventory of cloud services used Agency-wide, and it will work with the appropriate stakeholders to define component roles and responsibilities as well as define processes to categorize and inventory cloud services used throughout the enterprise.

¹³ The three systems included the Enterprise Data Warehouse; the Enterprise wide Mainframe & Distributed Network Telecommunications Services and Systems; and the Quality Assurance System.

Protect

We sampled 18 of the 45 metrics in this function. While SSA was able to support its responses for 6 metrics, it could not support its responses or provided incorrect responses for 12 others (see Table 2).¹⁴

Table 2: Unsupported or Incorrect Metrics for Protect Function

Number	Metric	Conclusion
Devices Assessed for Vulnerabilities		
2.1	Number of devices on network (from 1.2) assessed for vulnerabilities by a solution centrally visible at the enterprise level.	Incorrect
2.2.1	Number of GFE hardware assets with each Operating System.	Incorrect
2.2.2	The common security configuration baseline for each Operating System listed.	Incorrect
Unprivileged and Privileged Network Users		
2.4.1	Number of users with network accounts. (Exclude non-user accounts.)	Unsupported
2.4.3	Number of users (from 2.4.1) that use a username and password as their primary method for network authentication.	Unsupported
Network and Local System Accounts		
2.6.1	Number of users with privileged local system accounts.	Unsupported
2.6.2	Number of users with privileged local system accounts (from 2.6.1) that can access the Agency's network and are required to authenticate to the network through machine-based or user-based enforcement of a two-factor Personal Identity Verification credential or Level 3 credential.	Unsupported
Remote Access and Removable Media		
2.10.1a	Virtual Private Network - Percent utilizing Federal Information Processing Standards 140-2 validated cryptographic modules.	Incorrect
2.10.1b	Virtual Desktop Infrastructure/Remote Desktop Protocol - Percent utilizing Federal Information Processing Standards 140-2 validated cryptographic modules.	Incorrect
2.14	Number of unique unresolved Common Vulnerabilities and Exposures with a critical risk score (Common Vulnerability Scoring System Score of 9.0 - 10.0) on High Value Assets systems (outstanding for greater than 30 days).	Incorrect
2.14.1	Number of unique unresolved Common Vulnerabilities and Exposures with a high risk score (Common Vulnerability Scoring System Score of 7.0 – 8.9) on High Value Assets systems outstanding for greater than 60 days.	Incorrect
Security Training and Testing		
2.15	Complete the table to detail the number of users that participated in training exercises to increase awareness of phishing in the previous quarter.	Incorrect

Following are examples of metrics for which SSA could not support its responses or provided incorrect responses.

Devices Assessed for Vulnerabilities

In response to metric 2.1, SSA stated it assessed all devices that were on its network (from 1.2) for vulnerabilities by a solution centrally visible at the enterprise-level. The Agency stated it

¹⁴ See Appendix B for the full list of sampled metrics.

historically reported the same number for metric 2.1 as it did for metric 1.2. Specifically, SSA reported for metric 1.2 that it had 141,658 endpoints, 23,206 networking devices, and 108,280 input/output devices connected to its network at the end of FY 2019 and, for metric 2.1, it reported it assessed all of them for vulnerabilities. The Agency response for metrics 1.2¹⁵ and 2.1 were incorrect.

In response to metric 2.2.1, SSA provided the number of hardware assets for 16 different operating systems at the end of FY 2019. However, based on the evidence SSA provided, we could not reconcile the totals for 13 of the 16 operating systems, including multiple Windows operating systems. Therefore, SSA provided an incorrect response to Metric 2.2.1 as well as the corresponding Metric 2.2.3.¹⁶

Unprivileged and Privileged Users

In response to metrics 2.4.1 and 2.4.3, SSA stated it could provide screenshots within a 30-day period. Since SSA had not retained the evidence and more than 30 days had elapsed, the Agency was unable to support its reported numbers for the end of FY 2019.

Remote Access and Removable Media

In response to metric 2.14, SSA reported that—as of the end of FY 2019—there were 3,477 vulnerabilities with a critical risk score that had been outstanding for longer than 30 days, and 2,845 with a high-risk score that had been outstanding for greater than 60 days. However, because the query analysts were using to obtain the values for the number of unique unresolved common vulnerabilities and exposures requested events from the previous 60 days, any common vulnerabilities and exposures that were on a High Value Assets for longer than 60 days were not included. The Agency explained it was “working on improving this process.”

Security Training and Testing

In response to metric 2.15, SSA indicated 31,476 users reported receiving spoofed emails as part of the Agency’s third-quarter phishing exercise; however, this response did not include 857 users who manually reported the phishing exercise. Per the Agency, “In [Quarter] 3 FISMA CIO Metric, manual reports were not included because . . . there was significant overlap between users who manually reported and those who used the [automated reporting tool in the email application].” Therefore, SSA incorrectly reported the number of employees who informed Agency authorities they received the spoofed emails in the third-quarter phishing exercise.¹⁷

¹⁵ See the Hardware section for more information on Metric 1.2.

¹⁶ CIO Metric 2.2.3 was not in our sample.

¹⁷ SSA correctly indicated the number of users who received spoofing emails as part of the fourth-quarter phishing exercise.

Detect

We sampled 7 of the 13 metrics in this function. While SSA was able to support its responses for one metric, it could not support its responses for six others (see Table 3).¹⁸

Table 3: Unsupported Metrics for the *Detect* Function

Number	Metric
Intrusion Detection and Prevention	
3.4	Number of GFE endpoints (from 1.2.1) covered by an antivirus solution that provides file reputation services that check suspicious files against continuously updated malware information in near real-time.
Network Defense	
3.9	Percent of the organization's unclassified network that has implemented a technology solution centrally visible at the enterprise-level to detect and alert on the connection of unauthorized hardware assets.
3.9.1	Mean time to detect a new device (time between scans in 3.9). ¹⁹
3.9.2	Percent of the organization's unclassified network that has implemented a technology solution centrally visible at the enterprise-level to block network access of unauthorized hardware assets.
3.10	Number of GFE endpoints (from 1.2.1) covered by a software asset management capability centrally visible at the enterprise-level that is able to detect unauthorized software and alert appropriate security personnel.
3.10.1	Number of GFE endpoints (from 1.2.1) covered by a software asset management capability centrally visible at the enterprise-level that is able to block or prevent unauthorized software from executing.

SSA was unable to provide evidence to support its responses to metrics 3.4, 3.9, 3.9.1, and 3.9.2 because it had not retained it and was unable to reproduce it.

In response to metrics 3.10 and 3.10.1, SSA reported it had 124,342 endpoints capable of detecting, alerting, blocking or preventing unauthorized software at the end of FY 2019. The Agency was unable to provide evidence for its responses. However, the Agency set up a daily scheduled job that—going forward—will run this specific report and log the compliance numbers, which will allow the Agency to pull numbers for this metric for a specific date and track it over time.

Respond

We sampled three of the six metrics in this function. SSA could not support its responses or provided incorrect responses for these three metrics (see Table 4).²⁰

¹⁸ See Appendix B for the full list of sampled metrics.

¹⁹ This is the sum of time between detections divided by the number of detections.

²⁰ See Appendix B for the full list of sampled metrics.

Table 4: Unsupported or Incorrect Metrics for the *Respond* Function

Number	Metric	Conclusion
4.1	Mean time for the organization to detect system intrusion or compromise over the prior 12 months (past 365 days).	Incorrect
4.1.1	Mean time for the organization to contain a system intrusion or compromise after detection over the prior 12 months (past 365 days).	Incorrect
4.2	Percent of the organization’s network covered by an automated mechanism to assist in the tracking of security incidents and the collection and analysis of incident information.	Unsupported

In response to metrics 4.1 and 4.1.1, the Agency reported the mean time to detect system intrusion or compromise in the prior 12 months was 1.65 hours and the mean time for the organization to contain a system intrusion in the prior 12 months was 1.66 days. However, SSA informed us there were no system intrusions during the specified timeframe;²¹ therefore, the Agency’s response should have been “Not applicable; no intrusions or compromises.” The Agency has since updated its interpretation of the metrics and has reported that it has “. . . not had a system intrusion or compromise.”

Recover

We sampled one of the four metrics in this function,²² and the Agency provided an incorrect response. In response to metric 5.2, the Agency reported the mean time to restore operations following the containment of a system intrusion or compromise in the prior 12 months was zero hours. However, SSA informed us there were no system intrusions during the specified timeframe; therefore, the response should have been “Not applicable; no intrusions or compromises.”

AGENCY ACTIONS RESULTING FROM THE AUDIT

As of February 2021, the Agency had enhanced its process to collect artifacts, including the date of data collection, the description of how the reported values were obtained (including the tool

²¹ The Agency provided the timeframes for security incidents.

²² See Appendix B for the full list of sampled metrics.

used), and screen shots of the original information when available. The Agency also created a site to retain the evidence to support its responses to the metrics.

Because SSA has taken steps to improve its processes, we are not making any recommendations. See Appendix C for the Agency's comments.



Michelle L. Anderson
Assistant Inspector General for Audit

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

To accomplish our objective, we:

- Reviewed applicable Federal laws and related guidance to metric responses, including the following.
 - *Federal Information Security and Modernization Act of 2014* (FISMA).
 - Office of Management and Budget, *Managing Information as a Strategic Resource, Circular A-130*, July 28, 2016.
 - Office of Management and Budget, *Fiscal Year (FY) 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, October 25, 2018.
 - Department of Homeland Security, *Fiscal Year 2019 Chief Information Officer* (CIO) FY 2019 CIO FISMA Metrics, version 1, dated December 2018.
- Reviewed the Social Security Administration's (SSA) *Information Security Policy*.
- Interviewed or contacted SSA staff from components related to the CIO FISMA metric responses, including the following.
 - Office of Systems, Office of Information Security, Division of Compliance and Assessments.
 - Office of Systems, Office of Information Security, Division of Security Customer Service, Collaboration, and Tracking Branch.
 - Office of Systems, Office of Information Security, Division of Security Engineering, Security Administration Branch.
- Obtained and reviewed documentation including the following.
 - SSA's official cloud system inventory.
 - Inventory of local and network administration accounts.
 - System Security Categorization and Authorization to Operate letters for 26 systems.
 - Inventory of the number of users involved in phishing exercises.
 - Inventory of Agency Government Furnished Equipment endpoints.
- Selected 45 of the 87 CIO FISMA metrics for which SSA provided responses at the end of Fiscal Year 2019. For each metric, we gained an understanding of the process used to collect the responses and reviewed evidence to support the Agency's response to the metric.
 - We considered multiple factors when we selected the sample, including, but not limited to, the following.
 - Based on prior audit work (from the Office of the Inspector General, Government Accountability Office, etc.), we knew SSA had issues in the past.
 - Based on objective evidence we could readily verify.
 - Selected at least one metric from each section.

- Requested supporting evidence for selected metrics.
- Reviewed sampled CIO FISMA metrics responses by comparing the evidence SSA provided to the reported data. For the items the Agency could not support with evidence, we asked the Agency for assistance. While SSA was able to assist by providing some additional evidence, for some metrics the Agency had no documentation.

We conducted our audit at SSA Headquarters in Baltimore, Maryland, from October 2019 through December 2020. The principal entity reviewed was the Division of Compliance and Assessments within the Office of Information Security under the Office of the Deputy Commissioner for Systems. SSA provided documentation to support the information it reported for 14 of the 45 CIO FISMA responses we sampled; therefore, we determined the data were sufficiently reliable for purposes of our review. However, as described in the report, we could not determine whether data were reliable for the 12 sampled FY 2019 CIO FISMA responses the Agency was not able to support. For the 19 responses that were incorrect, we determined the data were not reliable.

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. We assessed the significance of internal controls and compliance with laws and regulations 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 component and principle as significant to the audit objective.

- Component 4: Information and Communication
 - Principle 13: Use quality information

Appendix B – SAMPLED METRIC RESPONSES

Chief Financial Officers Act agencies—including SSA—are required under FISMA to respond quarterly to security posture questions, referred to as Chief Information Officer (CIO) metrics.¹ The metrics assess agencies' implementation of information security capabilities in various risk areas and measure their effectiveness. Risk areas include management of assets, configurations, vulnerabilities, access, and incidents as well as data and boundary protection. In Fiscal Year (FY) 2019, agencies needed to respond to 87 metrics. We sampled 45 of the 87 metrics, as shown in Table B–1 through Table B–4.

Of the 45 metrics we sampled, SSA provided documentation to support its responses to 9 (20 percent) for the end of FY 2019; see Table B–1.

Table B–1: Sampled Metrics SSA Was Able to Support for End of FY 2019

Metric	Description	SSA Response
1.1.4	Systems (from 1.1.1 and 1.1.2) that are in Ongoing Authorization.	0
1.1.5	Total count of Agency submitted High value Assets.	8
1.2.2	Number of GFE networking devices.	23,206
1.2.3	Number of GFE input/output devices.	108,280
1.3.2	Number of mobile devices [Non-GFE (for example, Bring Your Own Device Assets)].	0
1.3.4	Number of mobile devices operating under enterprise-level mobile device management. [Non-GFE (for example, Bring Your Own Device Assets)].	0
2.5.5	Frequency with which privileged user privileges are reviewed, according to agency policy	1 year
2.16	Number of High Value Assets systems with adversarial testing ² performed within the last year.	5
3.2	Percent incoming of email traffic analyzed for suspicious or potentially malicious attachments without signatures that can be tested in a sandboxed environment or detonation chamber.	100%

Of the 45 metrics we sampled, SSA was unable to provide documentation to support its responses to 5 (11 percent) for the end of FY 2019; however, SSA provided evidence to support its first quarter FY 2020 metric responses. Because SSA used the same processes to prepare its responses for 2020 as it did for 2019, and because the 2020 responses were supported, we

¹ FISMA, Pub. L. No. 113-283 , § 3554(a)(1)(B), 128 Stat. 3073, p. 3078 (2014); Office of Management and Budget, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, M-19-02, section I, part I, p. 2 (October 25, 2018).

² Organizations can use adversarial testing to inform themselves of the exploitable vulnerabilities inherent to their network. Periodic adversarial testing can help organizations identify and mitigate potential risk before it is exploited with malicious intent.

concluded—for purposes of this review—that the Agency’s 2019 responses were likely supported.

Table B–2: Sampled Metrics SSA Could Not Support; However, it Could Support Its Responses for the First Quarter 2020

Metric	Description	SSA Response
1.3.1	Number of mobile devices (GFE).	3,429
2.3	Percent of privileged users ³ with network accounts that have technical control limiting access to only trusted sites	100%
2.5.1	Number of privileged users with network accounts. (Exclude non-user accounts)	5,859
2.5.2	Number of privileged users (from 2.5.1) that are required to authenticate to the network through using a two-factor credential or other Level 3 credential	5,859
2.5.3	Number of privileged users (from 2.5.1.) that use a username and password as their primary method for network authentication.	0

Of the 45 metrics we sampled, SSA was unable to provide documentation to support its responses to 12 (27 percent); see Table B–3.

Table B–3: Sampled Metrics that SSA Could Not Support

Metric	Description	SSA Response
1.3.3	Number of mobile devices operating under enterprise-level mobile device management (GFE).	3,429
2.4.1	Number of unprivileged users with network accounts. (Exclude non-user accounts)	81,598
2.4.3	Number of unprivileged users (from 2.4.1.) that use a username and password as their primary method for network authentication.	926
2.6.1	Number of users with privileged local system accounts	642
2.6.2	Number of users with privileged local system accounts (from 2.6.1) that can access the Agency’s network and are required to authenticate to the network through the following machine-based or user-based enforcement of a two-factor credential or other Level 3 credential.	642
3.4	Number of GFE endpoints (from 1.2.1) covered by an antivirus solution that provides file reputation services that check suspicious files against continuously updated malware information in near real-time.	134,059
3.9	Percent of the organization’s unclassified network that has implemented a technology solution centrally visible at the enterprise-level to detect and alert on the connection of unauthorized hardware assets.	98%
3.9.1	Mean time to detect a new device (time between scans in 3.9.).	0.01 days
3.9.2	Percent of the organization’s unclassified network that has implemented a technology solution centrally visible at the enterprise-level to block network access of unauthorized hardware assets.	15%

³ These are user accounts with elevated permissions, and are typically allocated to system administration, database administrators, developers, and others who are responsible for all system/application control, monitoring, or administration functions.

Metric	Description	SSA Response
3.10	Number of GFE endpoints (from 1.2.1.) covered by a software asset management capability centrally visible at the enterprise-level that is able to detect unauthorized software and alert appropriate security personnel.	124,342
3.10.1	Number of GFE endpoints (from 1.2.1.) covered by a software asset management capability centrally visible at the enterprise-level that is able to block or prevent unauthorized software from executing.	124,342
4.2	Percent of the organization's network covered by an automated mechanism to assist in the tracking of security incidents and the collection and analysis of incident information.	100%

Of the 45 metrics we sampled, SSA provided incorrect responses to 19 (42 percent) (see Table B-4).

Table B-4: Sampled Metrics with Incorrect Responses for End of FY 2019

Metric	Description	SSA Response
1.1.1	Number of operational unclassified information systems by organization (i.e. Bureau or Sub-Department Operating Element) categorized at the <i>Organization - Operated Systems</i> level.	25
1.1.2	Number of operational unclassified information systems by organization (i.e. Bureau or Sub-Department Operating Element) categorized at the <i>Contractor - Operated Systems</i> level.	1
1.1.3	Number of Systems (from 1.1.1 and 1.1.2) with Security Authority to Operate.	26
1.2	Number of hardware assets connected to the organization's unclassified network(s). (Note: 1.2. is the sum of 1.2.1. through 1.2.3.)	273,144
1.2.1	Number of Government Furnished Equipment (GFE) endpoints.	141,658
1.2.4	GFE hardware assets (from 1.2.1 – 1.2.3.) covered by an automatic hardware asset inventory capability (e.g. scans/device discovery processes) at the enterprise-level	273,144
1.2.5	GFE endpoints (from 1.2.1) covered by an automated software asset inventory capability at the enterprise level.	141,658
1.4	Report the types of Cloud Services your agency is using by cloud service provider(s) and service(s) you are receiving (for example, mail, database, etc.).	Table B-5
2.1	Number of devices on network (from 1.2) assessed for vulnerabilities by a solution centrally visible at the enterprise-level.	273,144
2.2.1	Number of GFE hardware assets with each Operating System.	Table B-6
2.2.2	The common security configuration baseline for each Operating System listed.	Table B-6
2.10.1a	Virtual Private Network - Percent utilizing Federal Information Processing Standards 140-2 validated cryptographic modules.	100%
2.10.1b	Virtual Desktop Infrastructure/Remote Desktop Protocol - Percent utilizing Federal Information Processing Standards 140-2 validated cryptographic modules.	100%
2.14	Number of unique unresolved Common Vulnerabilities and Exposures with a critical risk score (Common Vulnerability Scoring System Score of 9.0 - 10.0) on High Value Assets systems (outstanding for greater than 30 days).	3,477
2.14.1	Number of unique unresolved Common Vulnerabilities and Exposures with a high risk score (Common Vulnerability Scoring System Score of 7.0 – 8.9) on High Value Assets systems outstanding for greater than 60 days.	2,845

Metric	Description	SSA Response
2.15	Number of users that participated in training exercises to increase awareness to increase awareness of phishing in the previous quarter.	Table B-7
4.1	Mean time for the organization to detect system intrusion or compromise over the prior 12 months (past 365 days).	1.65 hours
4.1.1	Mean time for the organization to contain a system intrusion or compromise after detection over the prior 12 months (past 365 days).	1.66 days
5.2	Mean time for the organization to restore operations following the containment of a system intrusion or compromise over the prior 12 months (past 365 days).	0 hours

Some metrics require multiple responses, such as a list of the types of cloud services (see Table B-5), the number of GFE hardware assets (see Table B-6), and the number of users that participated in phishing training exercises (see Table B-7).

Table B-5: Response to Metric 1.4 – Types of Cloud Services

Cloud Service Provider	Cloud Service Offering	Agency Authority to Operate Date	Service	Service Type
Acquia	OIG Public Web System (Acquia)	August 11, 2016	External public web system	as a Service (PaaS)
Amazon	Enterprise Data Warehouse	September 26, 2016	Data analytics	Software as a Service (SaaS)
Amazon	Disability Case Processing System	March 16, 2017	Case Processing	SaaS
Amazon	Customer Communications Management Notices	July 6, 2017	SSA Notices	PaaS
Amazon	Agency Cloud Infrastructure	March 29, 2019	Development and Ops	Infrastructure as a Service (IaaS)
Microsoft	Microsoft Dynamics 365	May 4, 2018	SSA Frequently Asked Questions	SaaS
Microsoft	Microsoft Office 365	March 18, 2019	MSO365 Multi-Tenant	IaaS
Other – Qualtrics	Qualtrics XM Platform	March 28, 2019	Web based platform for surveys	SaaS
Other – AirWatch	Enterprise Mobile Management	December 21, 2017	Mobile device management	SaaS
Other – Everbridge Suite	Mass Emergency Notification Service	March 26, 2019	Emergency notifications	SaaS
Salesforce	Certificate of Coverage	February 2, 2017	Certificate of Coverage	PaaS
ServiceNow	Enterprise Managed Provisioning Service	May 17, 2018	Management of mobile asset	SaaS

Table B–6: Response to Metrics 2.2.1 – Number of GFE Hardware Assets and 2.2.2 – Common Security Configuration Baselines

Operating System	2.2.1 – Number of GFE Hardware Assets with each Operating System	2.2.2 – The Common Security Configuration Baseline for each Operating System listed.
Windows 10.x	82,429	Defense Information Systems Agency (DISA)
Windows 8.x	None Entered	
Windows 7.x	27,633	DISA
Windows Vista (Unsupported)	4	
Windows XP (Unsupported)	None Entered	
Windows Server 2016	8,889	DISA
Windows Server 2012	10,765	DISA
Windows Server 2008	478	DISA
Windows Server 2003 (Unsupported)	34	
Linux (all versions)	7,215	Center for Internet Security
Unix/Solaris (all versions)	384	Center for Internet Security
Mac OS X	1	Agency
Mobile Device – Windows Mobile (all versions)	None Entered	
Mobile Device – Apple iOS (all versions)	3,407	DISA
Mobile Device – Android OS(all versions)	None Entered	
Mobile Device – Blackberry OS (all versions)	22	DISA

Table B–7: Response to Metrics 2.15 – Number of Users that Participated in Phishing Training Exercises

Number of Users Involved	Targeted Community	Brief Summary of Test Procedures	Number of Users Who Successfully Passed the Exercise	Number of Users that Reported to Appropriate Authority
83,392	Agency Wide	SSA targeted users with a simulated benchmark phish and recorded user responses over the course of a week.	77,347	36,281
83,505	Agency Wide	SSA targeted users with a simulated benchmark phish and recorded user responses over the course of a week.	82,923	31,476

Appendix C – AGENCY COMMENTS



SOCIAL SECURITY

Office of the Commissioner

MEMORANDUM

Date: May 24, 2021 Refer To: TQA-1

To: Gail S. Ennis
Inspector General

A handwritten signature in blue ink, appearing to read "Scott Frey".

From: Scott Frey
Chief of Staff

Subject: Office of the Inspector General Draft Report “The Social Security Administration's Reporting Under the Federal Information Security Modernization Act” (A-14-18-50450)—
INFORMATION

Thank you for the opportunity to review the draft report. We continue to mature our information security reporting capabilities through well-defined, repeatable methodologies and expanding automation where feasible.

Please let me know if we 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.