Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Management Advisory Report

Summary of the Audit of the Social Security Administration's Information Security Program and Practices for Fiscal Year 2022

A-14-22-51179 September 2022

Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: September 30, 2022 **Refer to:** A-14-22-51179

To: Kilolo Kijakazi
Acting Commissioner

From: Gail S. Ennis,
Inspector General

Subject: Summary of the Audit of the Social Security Administration's Information Security Program and Practices for Fiscal Year 2022

The attached final report summarizes Grant Thornton LLP's (Grant Thornton) Fiscal Year (FY) 2022 review of the Social Security Administration's (SSA) information security program and practices, as required by the *Federal Information Security Modernization Act of 2014* (FISMA).

FISMA requires that the Inspector General, or an independent external auditor as determined by the Inspector General, annually assess and test the effectiveness of SSA's information security policies, procedures, and practices. Under a contract the Inspector General monitored, Grant Thornton, an independent certified public accounting firm, reviewed SSA's overall information security program and practices for FY 2022. Grant Thornton met with SSA staff and management frequently and reviewed evidence the Agency provided. As required, we submitted to the Office of Management and Budget Grant Thornton's responses to the FY 2022 FISMA Inspector General reporting metrics on July 29, 2022.

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

If you wish to discuss the final report, please contact Michelle L. Anderson, Assistant Inspector General for Audit.

Attachment

Summary of the Audit of the Social Security Administration's Information Security Program and Practices for Fiscal Year 2022
A-14-22-51179

September 2022 **Office of Audit Report Summary**

Objective

To determine whether the Social Security Administration's (SSA) overall information security program and practices were effective and consistent with the *Federal Information Security Modernization Act of 2014* (FISMA) requirements, as defined in the Fiscal Year (FY) 2022 core Inspector General (IG) FISMA reporting metrics.

Background

Under FISMA, SSA must develop, document, and implement an Agency-wide information security program. In addition, the Commissioner of Social Security is responsible for providing information security protections commensurate with the risk and magnitude of the harm that results from the unauthorized access, use, disclosure, disruption, modification, or destruction of Agency information and information systems.

FISMA requires that the Office of the Inspector General, or an independent external auditor as determined by the IG, annually evaluate the Agency's information security program and practices to determine their effectiveness.

We engaged Grant Thornton LLP (Grant Thornton) to conduct this performance audit in conjunction with the audit of SSA's FY 2022 Financial Statements. Grant Thornton used the FY 2022 core IG FISMA reporting metrics in evaluating SSA's overall information security program and practices.

Results

Based on the FY 2022 core IG FISMA reporting metrics guidance, Grant Thornton concluded SSA's overall security program was "Not Effective."

Although SSA had established an Agency-wide information security program and practices, Grant Thornton identified deficiencies that may limit the Agency's ability to adequately protect its systems and information. While SSA continued executing its risk-based approach to strengthen controls over its information systems and address weaknesses, Grant Thornton's audit continued to identify persistent deficiencies in both the design and operation of controls related to the FY 2022 core IG FISMA reporting metrics.

SSA should make protecting its networks and information systems a top priority and dedicate the resources needed to protect the confidentiality, integrity, and availability of information the American public entrusts to SSA.

Recommendations

In addition to the recommendations provided throughout the performance audit, Grant Thornton provided SSA with nine overarching recommendations to address the identified issues.

Office of the Inspector General Comments

SSA must improve its risk management processes and ensure the appropriate design and operating effectiveness of information security controls.

Agency Comments

SSA stated that protecting its networks and information remains a critical priority.

TABLE OF CONTENTS

ABBREVIATIONS

CIGIE	Council of the Inspectors General on Integrity and Efficiency
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
Cybersecurity Framework	Framework for Improving Critical Infrastructure Cybersecurity
DHS	Department of Homeland Security
FCEB	Federal Civilian Executive Branch
FISMA	*Federal Information Security Modernization Act of 2014*
FY	Fiscal Year
Grant Thornton	Grant Thornton, LLP
IG	Inspector General
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
Pub. L. No.	Public Law Number
SP	Special Publication
SSA	Social Security Administration
U.S.C.	United States Code

OBJECTIVE

The objective was to determine whether the Social Security Administration's (SSA) overall information security program and practices were effective and consistent with the *Federal Information Security Modernization Act of 2014* (FISMA)[1] requirements, as defined in the Fiscal Year (FY) 2022 core Inspector General (IG) FISMA reporting metrics.[2]

BACKGROUND

Agency Requirements Under the Act

FISMA requires that SSA develop, document, and implement an Agency-wide information security program.[3] In addition, the Commissioner of Social Security is responsible for providing 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.[4]

FISMA requires that the Office of the Inspector General (OIG), or an independent external auditor as determined by the IG, annually evaluate the Agency's information security program and practices to determine their effectiveness.[5] We engaged Grant Thornton LLP (Grant Thornton) to conduct this performance audit in conjunction with the audit of SSA's FY 2022 Financial Statements.

Grant Thornton used the FY 2022 IG FISMA reporting metrics in evaluating SSA's overall information security program and practices.

---

[1] *Federal Information Security Management Act of 2014*, Pub. L. No. 113-283, § 2, 128 Stat. 3073, 3075-3078 (2014).

[2] Office of Management and Budget (OMB), Office of the Federal Chief Information Officer, *FY 2022 Core IG Metrics Implementation Analysis and Guidelines* (April 2022). (dhs.gov/fisma).

[3] 44 U.S.C. § 3554(b).

[4] 44 U.S.C. § 3554(a)(1)(A).

[5] 44 U.S.C. §§ 3555(a)(1) and (b)(1).

Cyber-security Framework Functions and Related Inspector General Metric Domains

The FY 2022 core IG FISMA reporting metrics were developed by representatives from OMB, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), the Federal Civilian Executive Branch (FCEB) Chief Information Security Officers (CISO) and their staffs, and the Intelligence Community. The FY 2022 core IG FISMA reporting metrics continue using the maturity model approach for all security domains and are fully aligned with the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) function areas.[6] Table 1 includes the in-scope reporting metric domains for the performance audit.

Table 1: Aligning the Cyber-security Framework with the FY 2022 Core IG FISMA Metric Domains

Cyber-security Framework Function	FY 2022 IG FISMA Metric Domains
Identify	Risk Management Supply Chain Risk Management
Protect	Configuration Management Identity and Access Management Data Protection and Privacy Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Fiscal Year 2022 Metric Changes

In FY 2022, OMB, CIGIE, the FCEB CISO, and the Intelligence Community identified 20 core IG metrics (referred to as performance metrics), which is approximately one-third of the metrics tested in prior years. Representatives agreed that the 20 core IG metrics should provide sufficient data to determine the effectiveness of an agency's information security program with a high level of confidence. The performance metrics consisted of 20 questions across the 9 FISMA domains, descriptions of the 5 maturity levels for each core question, and related criteria.[7] Table 2 includes a general description of the five maturity levels.

[6] OMB, Office of the Federal Chief Information Officer, *FY 2022 Core IG Metrics Implementation Analysis and Guidelines* (April 2022). (dhs.gov/fisma).

[7] OMB, Office of the Federal Chief Information Officer, *FY 2022 Core IG FISMA Metrics Evaluation Guide,* (April 2022). (dhs.gov/fisma).

Table 2: IG Assessment Maturity Levels[8]

Maturity Level			Description
Not Effective	1	Ad-hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
	2	Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
	3	Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Effective	4	Managed and Measurable	Quantitative and qualitative measures of the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
	5	Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Federal agencies are required to use the Department of Homeland Security's (DHS) CyberScope tool to report core IG FISMA metric evaluation results.[9] CyberScope calculated the ratings based on historical IG FISMA reporting guidance. This included using either a simple majority or the most frequent maturity level determination across the questions to determine the domain, function, and overall agency program ratings.[10] The FY 2022 core IG FISMA metrics further state that an agency's overall security program is considered effective if it is determined to be at least at Level 4, *Managed and Measurable*.[11]

[8] Maturity level definitions were documented in OMB, Office of the Federal Chief Information Officer, *FY 2021 IG FISMA Reporting Metrics,* p. 6 (May 2021). (dhs.gov/fisma). While the FY 2022 core IG FISMA metrics named the same five maturity levels, the document did not provide a written description for each.

[9] OMB, Office of the Federal Chief Information Officer, *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*, p. 3 (May 2022). (dhs.gov/fisma).

[10] If multiple maturity levels were assessed in the same frequency, Grant Thornton rated SSA at the higher maturity level, in accordance with CyberScope recommendations.

[11] OMB, Office of the Federal Chief Information Officer, *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*, p. 2 (May 2022). (dhs.gov/fisma).

GRANT THORNTON'S SCOPE AND METHODOLOGY

For each metric, SSA management communicated to Grant Thornton what it considered SSA's maturity levels to be. Grant Thornton assessed SSA's information security program for each domain according to the Agency's self-assessed maturity level for each metric question.

For controls Grant Thornton determined met criteria for Level 2, *Defined*, it conducted tests to determine whether the criteria met requirements for maturity Level 3, *Consistently Implemented*. Grant Thornton conducted tests based on the nature of the controls; observed system settings; conducted security testing (for example, penetration testing); and/or, when applicable, used a sampling approach based on the Government Accountability Office's *Financial Audit Manual*.[12]

Likewise, for controls Grant Thornton determined met Level 3, *Consistently Implemented*, criteria it conducted tests to determine whether the criteria met the requirements for maturity Level 4, *Managed and Measurable*. For controls Grant Thornton determined met Level 4, *Managed and Measurable*, it conducted tests to determine whether they met the requirements for maturity Level 5, *Optimized*.

Grant Thornton only tested up to SSA's self-assessed level—not beyond. For example, SSA management believed its controls to prevent data exfiltration and enhance network defenses were at maturity Level 4, *Managed and Measurable,* for the Incident Response domain. Therefore, Grant Thornton tested whether the requirements up to Level 4 were met and did not test to determine whether the requirements for Level 5 were met. In conducting its review, Grant Thornton:

- varied the timing, nature, and extent of testing based on applicable standards and risk;
- assessed SSA's maturity levels for the FISMA metrics, domains, functions, and overall security program; and
- summarized these maturity levels in a report to OIG.

OIG reported Grant Thornton's detailed assessments of maturity levels for each metric, domain, and overall security program in CyberScope.

Grant Thornton frequently met with SSA management and staff throughout the audit period and reviewed evidence the Agency provided. Grant Thornton conducted its performance audit in accordance with generally accepted government auditing standards. Those standards require that Grant Thornton plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the audit objectives. For additional information about the scope and methodology, see Appendix A.

[12] Government Accountability Office, *Financial Audit Manual,* GAO-22-105894, Vol. I, Sections 450.03 and 450.06, pp. 450-1 through 450-3 (June 2022).

Our Evaluation of Grant Thornton's Performance

We were responsible for technical and administrative oversight regarding Grant Thornton's performance under the contract terms. To fulfill our responsibilities under the *Inspector General Act of 1978*,[13] we monitored Grant Thornton's review by:

- reviewing Grant Thornton's approach and planning;
- evaluating Grant Thornton personnel's qualifications and independence;
- monitoring Grant Thornton's progress;
- examining Grant Thornton's documentation and deliverables to ensure they comply with our requirements;
- coordinating the issuance of Grant Thornton's results; and
- performing other procedures as deemed necessary.

We did not conduct our review of Grant Thornton's work under generally accepted government auditing standards. Our review was not intended to enable us to express, and accordingly we do not express, an opinion about the effectiveness of SSA's information security policies, procedures, and practices. However, our monitoring review, as qualified above, disclosed no instances where Grant Thornton did not comply with our requirements.

Grant Thornton's audit results contain information that, if not protected, could result in adverse effects to the Agency's information systems. In accordance with government auditing standards,[14] we have separately transmitted to SSA management Grant Thornton's detailed findings and recommendations and excluded from this summary certain sensitive information because of the potential damage that could result if the information is misused. We have determined the omitted information neither distorts the audit results described in this report nor conceals improper or illegal practices.

Results of Grant Thornton's Review

Based on the FY 2022 core IG FISMA reporting metrics guidance, Grant Thornton concluded SSA's overall security program was "Not Effective." Although SSA had established an Agency-wide information security program and practices, Grant Thornton identified deficiencies that may limit the Agency's ability to adequately protect the organization's systems and information. While SSA continued executing its risk-based approach to strengthen controls over its information systems and address weaknesses, Grant Thornton's audit continued identifying persistent deficiencies in both the design and operation of controls related to the FY 2022 core IG FISMA reporting metrics.

---

[13] *Inspector General Act of 1978, 5 U.S.C. app., amended by Whistleblower Protection Coordination Act, Pub. L. No. 115-192, 132 Stat. 1502 (2018). (as amended through Pub. L. No. 115-192, enacted June 25, 2019).*

[14] Government Accountability Office, *Government Auditing Standards, 2018 Revision*, GAO-21-568G, 9.66, pp. 209 and 210 (July 2018).

Grant Thornton stated that SSA should make protecting its networks and information systems a top priority and dedicate the resources needed to protect the confidentiality, integrity, and availability of information the American public entrusts to SSA. Table 3 summarizes SSA's self-assessments and Grant Thornton's conclusions. For a summary of Grant Thornton's conclusions for the metrics within each domain, see Appendix B.

Table 3: Assessed Maturity-level Determinations

Function/Domain	SSA's Self-Assessment	Grant Thornton's Assessment
IDENTIFY	**Level 3**	**Level 2**
Risk Management	Level 3	Level 2
Supply Chain Risk Management	Level 3	Level 2
PROTECT	**Level 4**	**Level 3**
Configuration Management	Level 3	Level 2
Identity and Access Management	Level 4	Level 3
Data Protection and Privacy	Level 4	Level 4
Security Training	Level 5	Level 4
DETECT	**Level 3**	**Level 2**
Information Security Continuous Monitoring	Level 3	Level 2
RESPOND	**Level 5**	**Level 4**
Incident Response	Level 5	Level 4
RECOVER	**Level 4**	**Level 3**
Contingency Planning	Level 4	Level 3
Overall Security Program Effectiveness	**Effective**	**Not Effective**

Examples of Grant Thornton's Findings

Following are examples of some of the deficiencies Grant Thornton identified.[15]

Identify

- SSA had not fully defined and implemented specific aspects of its risk-management program and strategy across the Agency.
- SSA had not fully implemented its risk monitoring and communication tools and procedures to provide a centralized and enterprise view of risks.
- SSA needed to fully implement its policies and processes for maintaining a complete and accurate inventory of information systems, hardware, and software

[15] Because of their sensitive nature, we shared Grant Thornton's findings with SSA management in a separate document.

- SSA needed to continue revising system boundaries and control inheritance.
- SSA needed to maintain a complete and accurate inventory of contractor systems and improve procedures for supply chain risk management.

Protect

- Grant Thornton's security and diagnostic testing identified deficiencies.

Detect

- SSA had not fully defined and documented certain elements of its information security continuous monitoring program.
- SSA had not fully implemented its plan to transition to ongoing security assessments and authorization.

Recover

- SSA did not conduct an annual contingency plan exercise for a cloud-based system.
- SSA had not fully integrated its system- and Agency-level business impact analyses to guide the Agency's contingency planning efforts.

Agency Efforts to Resolve Weaknesses and Potential Causes for Deficiencies

In FY 2022, SSA continued executing a risk-based approach to strengthen controls over its systems and address weaknesses. In addition, SSA continued implementing several plans, strategies, and initiatives to address security gaps within each functional area of the NIST Cybersecurity Framework. SSA leadership also restated its commitment to address deficiencies. However, Grant Thornton identified issues in the design and operation of controls that were similar to those cited in past reports. Grant Thornton believes that, in many cases, these deficiencies still existed because of one, or a combination, of the following:

- SSA relied on manually intensive processes. Given the amount, and sensitivity, of data in SSA's information technology environment, the Agency needs to employ further automation, software, and other tools to address areas of risk, including network security, identity and access management, network access control, and configuration management.
- SSA established a governance and oversight board but had not fully implemented procedures to address the root cause(s) of deficiencies or prioritized corrective actions to address the highest areas of risk.
- SSA had not fully implemented enhanced or new controls to address risks and recommendations provided in past audits.

GRANT THORNTON'S RECOMMENDATIONS TO THE AGENCY

To be consistent with the FISMA requirements, Grant Thornton believes SSA should strengthen its information security risk-management framework; enhance information technology oversight and governance to address these weaknesses; and adhere to its information security policies, procedures, and controls. SSA should continue making protecting its networks and information systems a top priority; consider automation and software to replace manually intensive processes; and dedicate additional resources, if needed, to ensure the appropriate design and operating effectiveness of its information security controls and prevent unauthorized access to sensitive information. In addition to the recommendations provided in the performance audit, Grant Thornton provided SSA nine overarching recommendations to address the identified issues.[16]

THE OFFICE OF THE INSPECTOR GENERAL'S COMMENTS

Table 4 summarizes the results of Grant Thornton's independent evaluations of SSA's information security programs since FY 2019.

Table 4: Summary Results By Function—FYs 2019 to 2022

FUNCTION/Domain	FY 2019	FY 2020	FY 2021	FY 2022
IDENTIFY	**Level 2**	**Level 2**	**Level 2**	**Level 2**
Risk Management	Level 2	Level 2	Level 2	Level 2
Supply Chain Risk Management	N/A	N/A	Level 2	Level 2
PROTECT	**Level 2**	**Level 2**	**Level 3 ▲**	**Level 3**
Configuration Management	Level 2	Level 2	Level 2	Level 2
Identity and Access Management	Level 2	Level 2	Level 3 ▲	Level 3
Data Protection and Privacy	Level 2	Level 2	Level 2	Level 4 ▲
Security Training	Level 2	Level 2	Level 3 ▲	Level 4 ▲
DETECT	**Level 2**	**Level 2**	**Level 2**	**Level 2**
Information Security Continuous Monitoring	Level 2	Level 2	Level 2	Level 2
RESPOND	**Level 2**	**Level 4 ▲**	**Level 4**	**Level 4**
Incident Response	Level 2	Level 4 ▲	Level 4	Level 4
RECOVER	**Level 2**	**Level 2**	**Level 3**	**Level 3**
Contingency Planning	Level 2	Level 2	Level 3	Level 3
Overall Security Program Effectiveness	***Not Effective***	***Not Effective***	***Not Effective***	***Not Effective***

▲ Indicates a higher maturity rating from the prior FY.

[16] Because of their sensitive nature, we shared Grant Thornton's recommendations with SSA management in a separate document.

We note that the FY 2022 results are not directly comparable to those in prior years because the maturity-level determinations are not based on the same metrics as in prior years. Specifically, the FY 2022 core IG FISMA reporting metrics guidance included only 20 metrics—approximately one-third of the metrics tested in prior years. As a result, the maturity-level determinations in FY 2022 were generally based on the results of fewer metrics than in prior years. For example:

- The maturity-level determination for the *Protect* function was based on the results of 26 metrics in FY 2021 but only 8 core metrics in FY 2022.
- The maturity-level determination for the Risk Management domain was based on the results of 10 metrics in FY 2021 but only 5 core metrics in FY 2022.
- The maturity-level determination for the Security Training domain was based on the results of 5 metrics in FY 2021 but only 1 core metric in FY 2022.

With fewer metrics in a function or domain, each tested metric has greater influence on the overall maturity-level determination. In addition, because some metrics from prior years were not within the scope of the FY 2022 review, they were not tested and therefore Grant Thornton did not consider them in the overall maturity-level determination.

In FY 2022, the Agency continued its efforts to improve and mature its information security program and practices to protect it from cyber-security threats. Specifically, based on the FY 2022 FISMA core metrics, the assessed maturity for SSA's Data Protection and Privacy domain improved from Level 2, *Defined*, in FY 2021 to Level 4, *Managed and Measurable*. In addition, Grant Thornton concluded the maturity of SSA's Security Training domain improved from Level 3, *Consistently Implemented*, in FY 2021 to Level 4, *Managed and Measurable*, in FY 2022.

Although Grant Thornton determined SSA had achieved higher maturity levels for certain metrics and their respective domains, Grant Thornton's ratings for the higher-level functions did not change from FY 2021. Also, as in FY 2021, Grant Thornton concluded SSA's overall information security program in FY 2022 was "Not Effective" because the FY 2022 core IG FISMA reporting metrics guidance considers Level 4, *Managed and Measurable*, or higher to be an effective level of security.

THE OFFICE OF THE INSPECTOR GENERAL'S CONCLUSIONS

SSA houses sensitive information about each person who has been issued a Social Security number. Without appropriate security, the Agency's systems, and the sensitive data they contain, are at risk. Inappropriate and unauthorized access to, or theft of, this information can result in significant harm and distress to millions of numberholders. As such, it is imperative that the Agency continue making protecting its networks and information a top priority.

Since FY 2013, auditors have identified deficiencies in SSA's information systems controls. In the following years, auditors continued identifying deficiencies that limited SSA's ability to adequately protect SSA's information and information systems. SSA must improve its risk-management processes and ensure the appropriate design and operating effectiveness of information security controls.

AGENCY COMMENTS

SSA stated that protecting its networks and information remains a critical priority, as recognized by Grant Thornton who noted the Agency's efforts to improve and mature its information security program and practices. See Appendix C for the full text of SSA's comments.

Michelle L. Anderson
Assistant Inspector General for Audit

APPENDICES

Appendix A – Scope and Methodology

Grant Thornton LLP (Grant Thornton) mapped the Social Security Administration's (SSA) key information security controls to the metrics in the Fiscal Year (FY) 2022 *Federal Information Security Modernization Act of 2014* (FISMA) domains. For each metric question, Grant Thornton tested the control's design through inquiry with management and inspection of management policies and procedures, including, but not limited to, the Agency's *Information Security Policy* and Security Assessment and Authorization artifacts, such as system security plans, system assessment reports, authorizations to operate, and plans of action and milestones. For controls Grant Thornton determined SSA defined adequately, it performed tests to determine whether they were effectively and consistently implemented. Depending on the nature of the controls, Grant Thornton observed system settings, inspected supporting documentation, and/or conducted security testing (for example, vulnerability scans and penetration testing). For some control tests, Grant Thornton evaluated the entire population of instances while, in other tests, it performed random sampling to assess the controls. Based on the results of these tests, Grant Thornton determined whether SSA met the associated metric maturity level.

Because of the extensive work on the internal control system completed as part of the annual financial statement audit, Grant Thornton incorporated the FISMA test procedures to address the FY 2022 core IG FISMA reporting metrics while completing information technology (IT) controls testing in support of the financial statement audit. To maximize efficiencies and minimize the impact to SSA management during the FISMA performance audit, Grant Thornton used the Government Accountability Office's *Federal Information System Controls Audit Manual* Appendix IX—*Application of Federal Information System Controls Audit Manual to FISMA,* to leverage testing performed on the in-scope financial systems during the financial statement audit. In some cases, Grant Thornton designed and executed test procedures for those instances when FISMA tests were unique from those of the financial statement audit.

In FY 2022, Grant Thornton tested SSA's information security controls at two regional offices and three disability determination services. Grant Thornton also tested multiple systems at SSA Headquarters and followed up on the status of prior-year findings.

Technical Security Testing

Grant Thornton performed technical security testing to support both the financial statement and FISMA audits. In 2022, Grant Thornton performed:

- external and internal penetration testing at SSA Headquarters;
- a share assessment at SSA Headquarters and two regional offices;
- vulnerability assessments at SSA Headquarters, including testing of the Cybersecurity & Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities;
- wireless testing at SSA Headquarters;
- assessment of configuration management, patch management, and vulnerability management processes;

- IT diagnostic security testing of selected UNIX production servers, mainframe production logical partitions (including DB2), Windows production servers, AS/400 production servers, firewalls, routers, Oracle and SQL databases, and WebSphere and IIS Webservers—all of which are part of the representative set of SSA systems;
- mainframe access and configuration management control testing; and
- testing of management's corrective actions to determine whether prior-year IT security findings had been remediated.

Criteria

Grant Thornton focused the FISMA audit approach on Federal information security guidance developed by the National Institute of Standards and Technology (NIST) and Office of Management and Budget (OMB). NIST Special Publications (SP) provide guidelines that are considered essential to the development and implementation of agencies' security programs. Following are the criteria Grant Thornton used to conduct the FY 2022 FISMA performance audit:

- FISMA law.
- OMB guidance, including OMB Memorandums.
  - M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*
  - M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*
  - M-21-30, *Protecting Critical Software Through Enhanced Security Measures*
  - M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*
  - M-21-07, *Completing the Transition to Internet Protocol Version 6 (IPv6)*
  - M-20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*
  - M-19-17, *Enabling Mission Delivery Through Enhanced Improved Identity, Credential and Access Management*
  - M-19-03, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program*
  - M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*
  - M-16-17, *OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource*.
- FY 2022 Core IG Metrics Implementation Analysis and Guidelines.
- FY 2022 Core IG FISMA Metrics Evaluation Guide.
- Annual FISMA Chief Information Officer reporting Metrics, *FY 2022 Chief Information Officer Federal Information Security Modernization Act of 2014* Reporting Metrics V1.1, March 2022.

- DHS Binding Operational Directive 18-01, *Enhance Email and Web Security*.
- DHS Binding Operational Directive 18-02, *Securing High Value Assets*.
- DHS Binding Operational Directive 19-02, *Vulnerability Remediation Requirements For Internet-Accessible Systems*, DHS Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*.
- Standards and guidelines issued by NIST, including the following.
  - Federal Information Processing Standards Publication - 199, *Standards for Security Categorization of Federal Information and Information Systems*
  - Federal Information Processing Standards Publication - 201-2, *Personal Identity Verification of Federal Employees and Contractors*
  - NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*
  - NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*
  - NIST SP 800-37 Revision 2, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach*
  - NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
  - NIST SP 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies*
  - NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
  - NIST SP 800-53 Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*
  - NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*
  - NIST SP 800-63, *Digital Identity Guidelines*
  - NIST SP 800-70 Revision 4, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*
  - NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
  - NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organization*s
  - NIST SP 800-152, *A Profile for U.S. Federal Cryptographic Key Management Systems*
  - NIST SP 800-157, *Guidelines for Derived Personal Identity Verification Credentials*
  - NIST SP 800-181, *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework*
  - NIST SP 800-207, *Zero Trust Architecture*
  - NIST SP 800-218, *Secure Software Development Framework Version 1.1*
  - NIST Interagency Report 8011 Volumes I and II, *Automation Support for Security Control Assessments*

  - NIST Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management*
  - NIST Interagency Report 8276, *Key Practices in Cyber Supply Chain Risk Management*
  - NIST *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018
- *Federal Cybersecurity Workforce Assessment Act of 2015*.
- Department of Homeland Security (DHS) Federal Continuity Directive 1, *Federal Executive Branch National Continuity Program and Requirements.*
- DHS Emergency Directive 19-01, *Mitigate DNS Infrastructure Tampering*.
- Other Federal guidance and standards cited in the DHS annual FISMA IG reporting metrics.
- Applicable SSA policies, including the Information Security Policy, Program Operations Manual System, and Interconnection Approval Process Guide.
- Executive Order 14028, *Executive Order on Improving the Nation's Cybersecurity.*
- CISA Cybersecurity & Incident Response Playbooks.
- CISA Cybersecurity & Vulnerability Response Playbooks.
- CISA Cybersecurity Incident & Vulnerability Response Playbooks.
- Federal Enterprise Architecture Framework, version 2.
- CIS Top 18 Security Controls, version 8.
- CISA Zero Trust Maturity Model, version 1.0.
- *The Federal Acquisition Supply Chain Security Act of 2018*.
- Federal Risk and Authorization Management Program Control Specific Contract Clauses.
- Homeland Security Presidential Directive 12: *Policy for a Common Identification Standard for Federal Employees and Contractors.*
- National Cybersecurity Workforce Framework, version 1.0.
- United States Computer Emergency Readiness Team Incident Response Guidelines (2015).

Grant Thornton conducted this performance audit in accordance with *Government Auditing Standards*. Those standards require that Grant Thornton plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the audit objective. Grant Thornton believes that the evidence obtained provides a reasonable basis for its findings and conclusions based on the audit objective.

Appendix B – Fiscal Year 2022 Maturity Model Scoring

The Fiscal Year 2022 core Inspector General *Federal Information Security Modernization Act of 2014* reporting metrics continue using the maturity model approach for all security domains and are fully aligned with the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity function areas.[1] Tables B–1 through B–5 summarize Grant Thornton's maturity assessments of the function areas, including each security domain, for the Social Security Administration (SSA). Table B–6 summarizes Grant Thornton's assessment of the Agency's overall information security program.

Table B–1: Assessment Summary of the Identify Function

FUNCTION: IDENTIFY				**DEFINED (LEVEL 2)**
Domain: Risk Management				**Defined (Level 2)**
"The program and supporting process to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time." *National Institute of Standards and Technology (NIST) Special Publication, Security and Privacy Controls for Information Systems and Organization, 800-53 Revision 5, Appendix A, p. 415 (September 2020).*				
Count of Metrics by Maturity Level:				
Ad Hoc (Level 1)	Defined (Level 2)	Consistently Implemented (Level 3)	Managed and Measurable (Level 4)	Optimized (Level 5)
0	5	0	0	0
Domain: Supply Chain Risk Management				**Defined (Level 2)**
"A systematic process for managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and developing risk response strategies to the risks presented by the supplier, the supplied products and services, or the supply chain." *NIST Special Publication, Security and Privacy Controls for Information Systems and Organization, 800-53 Revision 5, Appendix A, p. 420 (September 2020)*.				
Count of Metrics by Maturity Level:				
Ad Hoc (Level 1)	Defined (Level 2)	Consistently Implemented (Level 3)	Managed and Measurable (Level 4)	Optimized (Level 5)
0	1	0	0	0

[1] Office of Management and Budget, Office of the Federal Chief Information Officer, *FY 2022 Core IG Metrics Implementation Analysis and Guidelines* (April 2022). (dhs.gov/fisma).

Table B–2: Assessment Summary of the Protect Function

FUNCTION: PROTECT	CONSISTENTLY IMPLEMENTED (LEVEL 3)
Domain: Configuration Management	**Defined (Level 2)**
Provides assurance the system in operation is the correct version (configuration), and any changes to be made are reviewed for security implications.	
Count of Metrics by Maturity Level:	
Ad Hoc (Level 1): 0	Defined (Level 2): 2
Consistently Implemented (Level 3): 0	Managed and Measurable (Level 4): 0
Optimized (Level 5): 0	
Domain: Identity and Access Management	**Consistently Implemented (Level 3)**
Includes policies to control user access to information system objects, including devices, programs, and files.	
Count of Metrics by Maturity Level:	
Ad Hoc (Level 1): 0	Defined (Level 2): 1
Consistently Implemented (Level 3): 2	Managed and Measurable (Level 4): 0
Optimized (Level 5): 0	
Domain: Data Protection and Privacy	**Managed and Measurable (Level 4)**
Includes policies and procedures to protect Agency data, including personally identifiable information and other sensitive data, from inappropriate disclosure.	
Count of Metrics by Maturity Level:	
Ad Hoc (Level 1): 0	Defined (Level 2): 0
Consistently Implemented (Level 3): 1	Managed and Measurable (Level 4): 1
Optimized (Level 5): 0	
Domain: Security Training	**Managed and Measurable (Level 4)**
Agency-wide information security program for a Federal agency must include security awareness training. This training must cover (1) information security risks associated with users' activities and (2) users' responsibilities in complying with agency policies and procedures designed to reduce these risks.	
Count of Metrics by Maturity Level:	
Ad Hoc (Level 1): 0	Defined (Level 2): 0
Consistently Implemented (Level 3): 0	Managed and Measurable (Level 4): 1
Optimized (Level 5): 0	

Table B–3: Assessment Summary of the Detect Function

FUNCTION: DETECT				DEFINED (LEVEL 2)
Domain: Information Security Continuous Monitoring				**Defined (Level 2)**
Maintains ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.				
Count of Metrics by Maturity Level:				
Ad Hoc (Level 1)	Defined (Level 2)	Consistently Implemented (Level 3)	Managed and Measurable (Level 4)	Optimized (Level 5)
0	2	0	0	0

Table B–4: Assessment Summary of the Respond Function

FUNCTION: RESPOND				MANAGED AND MEASURABLE (LEVEL 4)
Domain: Incident Response				**Managed and Measurable (Level 4)**
According to *National Institute of Standards and Technology Special Publication* SP 800-12, the main benefits of an incident-handling capability are (1) containing and repairing damage from incidents and (2) preventing future damage. *NIST Special Publication, An Introduction to Information Security, 800-12 Revision 1*, ch. 10.9, p. 64 (June 2017).				
Count of Metrics by Maturity Level:				
Ad Hoc (Level 1)	Defined (Level 2)	Consistently Implemented (Level 3)	Managed and Measurable (Level 4)	Optimized (Level 5)
0	0	1	1	0

Table B–5: Assessment Summary of the Recover Function

FUNCTION: RECOVER				CONSISTENTLY IMPLEMENTED (LEVEL 3)
Domain: Contingency Planning				**Consistently Implemented (Level 3)**
Processes and controls to mitigate risks associated with interruptions (losing capacity to process, retrieve, and protect electronically maintained information) that may result in lost or incorrectly processed data.				
Count of Metrics by Maturity Level:				
Ad Hoc (Level 1)	Defined (Level 2)	Consistently Implemented (Level 3)	Managed and Measurable (Level 4)	Optimized (Level 5)
0	1	1	0	0

Table B–6: Assessment Summary of SSA's Overall Information Security Program

Overall Information Security Program	Not Effective
IDENTIFY	Defined (Level 2)
PROTECT	Consistently Implemented (Level 3)
DETECT	Defined (Level 2)
RESPOND	Managed and Measurable (Level 4)
RECOVER	Consistently Implemented (Level 3)
Conclusion	**Consistently Implemented (Level 3)**
Although SSA had established an Agency-wide information security program and practices, Grant Thornton identified several deficiencies. The weaknesses identified may limit the Agency's ability to adequately protect the organization's information and information systems. In addition, Grant Thornton assessed only three *Federal Information Security Modernization Act of 2014* domains as Level 4, *Managed and Measurable*. The Fiscal Year 2022 core Inspector General *Federal Information Security Modernization Act of 2014* reporting metrics defines an effective information security program as at least Level 4, *Managed and Measurable*).	

Appendix C – Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: September 28, 2022 Refer To: TQA-1

To: Gail S. Ennis
Inspector General

From: Scott Frey
Chief of Staff

Subject: Office of the Inspector General Draft Management Advisory Report "Summary of the Audit of the Social Security Administration's Information Security Program and Practices for Fiscal Year 2022" (A-14-22-51179)—INFORMATION

Thank you for the opportunity to review the draft report. Protecting our networks and the information we use to administer our programs remains a critical priority, as recognized by Grant Thornton who noted our efforts to improve and mature our information security program and practices. We work continuously to improve our cybersecurity controls and to elevate our Federal Information Security Management Act maturity levels.

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

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

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

Connect: OIG.SSA.GOV

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

Follow us on social media via these external links:


Twitter: @TheSSAOIG


Facebook: OIGSSA


YouTube: TheSSAOIG


Subscribe to email updates on our website.