The Social Security Administration's Information Technology Security Program and Practices for Fiscal Year 2021 (A-14-20-50958)

Objective

The objective of the performance audit was to determine whether the Social Security Administration's (SSA) overall information security program and practices were effective and consistent with *Federal Information Security Modernization Act of 2014* (FISMA)[1] requirements, as defined by the Department of Homeland Security (DHS).

Background

FISMA includes the following key requirements:

- each agency must develop, document, and implement an agency-wide information security program;[2]
- each agency head 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;[3] and
- the agency's Inspector General (IG), or an independent external auditor, must perform an independent evaluation of the agency's information security program and practices to determine their effectiveness.[4]

We engaged Grant Thornton LLP to conduct the Fiscal Year (FY) 2021 FISMA performance audit in accordance with Government Auditing Standards. Grant Thornton assessed the effectiveness of SSA's information security controls, including its policies, procedures, and practices, on a representative subset of the Agency's information systems by leveraging work performed as part of the financial statement audit and performing necessary additional testing procedures.

[1] 44 U.S.C. § 3555(a)(1).

[2] 44 U.S.C. § 3554(b).

[3] 44 U.S.C. § 3554(a)(1)(A).

[4] 44 U.S.C. §§ 3555(a)(1) and (b)(1).

Grant Thornton's Scope and Methodology

Grant Thornton used the FY 2021 IG FISMA Reporting Metrics in evaluating SSA's overall information security program and practices.[5] The FY 2021 Metrics continued using the maturity model approach for all security domains and were fully aligned with the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) function areas. Table 1 describes the DHS in-scope reporting Metric domains for the performance audit.

Table 1: Aligning the Cyber-security Framework with the FY 2021 IG FISMA Metric Domains

Cybersecurity Framework Function	FY 2021 IG FISMA Metric Domains
Identify	Risk Management Supply Chain Risk Management[6]
Protect	Configuration Management Identity and Access Management Data Protection and Privacy Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

In FY 2021, the Council of the Inspectors General on Integrity and Efficiency, in partnership with the Office of Management and Budget (OMB) and DHS, continued refining these Metrics. The Metrics consisted of specific questions (performance Metrics) for each Metric domain and the descriptions of the five maturity levels for each Metric. Table 2 includes DHS' general description of the five maturity levels.

[5] OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency, *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics,* V1.1 (May 2021).

[6] OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency, FY 2021 *Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics,* V1.1 (May 2021), p. 7, paragraph 2, states, "To provide agencies with sufficient time to fully implement NIST 800-53, Rev 5., in accordance with OMB A-130, these new Supply Chain Risk Management metrics should not be considered for the purposes of the Identify framework function rating."

Table 2: IG Assessment Maturity Levels

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.

The DHS guidance states that ratings throughout the domains will be by a simple majority, where the most frequent level across the questions will serve as the domain rating. OMB strongly encourages IGs to use the domain ratings to inform the overall function ratings and the five function ratings to inform the overall agency rating. The guidance further states that Level 4, Managed and Measurable, is considered to be an effective level of security at the domain, function, and overall security program levels.[7]

For each Metric question, SSA management communicated self-assessment maturity levels of Defined, Consistently Implemented, or Managed and Measurable. Grant Thornton evaluated SSA's information security program for each domain against the respective self-assessment level in the FY 2021 IG FISMA Reporting Metrics.

[7] To drive continued improvements in cyber-security maturity across the Federal landscape and focus agency efforts, the FY 2021 IG FISMA Metric also introduced a pilot concept of weighting specific FISMA Metrics for assessment and scoring. Ten priority Metrics (that is, 5,10,31, 32, 36, 37, 47, 54, 55, 63) were proposed based on a combination of the lowest average performing metrics from previous assessments, administration priorities, and the highest value controls. As part of the proposed weighted average approach to scoring, these priority Metrics were weighted twice as much in the maturity calculation. This pilot approach will help evaluate the impacts of these Metrics and prepare agencies for the possibility of changing the calculation process in a future update to this document.

For each Metric question, Grant Thornton tested the design of the control(s) through inquiry with management and inspection of management policies and procedures. For controls Grant Thornton determined were Level 2, Defined, the firm tested the controls to determine whether they were Level 3, Consistently Implemented. Likewise, for controls Grant Thornton determined were Level 3, Consistently Implemented, the firm tested the controls to determine whether they were Level 4, Managed and Measurable. When SSA management self-assessed a Metric to be less than Managed and Measurable, Grant Thornton tested up to and including the self-assessed level. Grant Thornton varied the timing, nature, and extent of testing based on applicable standards and risk. It also inspected SSA's documented rationale for Metric questions that were not assessed at Level 4, Managed and Measurable, but the Agency felt were effective. Based on its test results and inspection of SSA rationale, Grant Thornton assessed SSA's maturity levels for the FISMA Metrics, domains, functions and overall security program.[8]

Grant Thornton met with SSA staff and management frequently 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.

Office of the Inspector General's Evaluation of Grant Thornton's Performance

We monitored Grant Thornton's performance by:

- reviewing Grant Thornton's audit approach and planning;
- evaluating Grant Thornton's auditors' qualifications and independence;
- monitoring the audit progress;
- examining Grant Thornton's working papers;
- reviewing Grant Thornton's report to ensure it complies with *Government Auditing Standards*;
- coordinating the issuance of the audit report; and
- performing other procedures as deemed necessary.

Grant Thornton is responsible for the auditor's report and the conclusions expressed therein. The Office of the Inspector General was responsible for technical and administrative oversight regarding Grant Thornton's performance under the contract terms. We did not conduct oversight of Grant Thornton's audit in accordance with generally accepted government auditing standards. Our oversight activities were not intended to enable us to express, and, accordingly, we do not express, an opinion about the effectiveness of SSA's information security policies,

[8] We reported the detailed assessed maturity levels for each Metric, domain, and overall security program in CyberScope. DHS and the Department of Justice developed CyberScope to streamline information technology security reporting for Federal agencies to support FISMA compliance. See OMB, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*, *M-21-02*, pp. 1 through 13.

procedures, and practices. However, as qualified above, our monitoring review disclosed no instances where Grant Thornton did not comply with applicable auditing standards.

Results of Grant Thornton's Review

Although SSA had established an information security program and security practices across the Agency, as required by FISMA, OMB policy and guidelines, and NIST standards and guidelines, Grant Thornton identified a number of deficiencies related to: (1) Risk Management; (2) Supply Chain Risk Management; (3) Configuration Management; (4) Identity and Access Management; (5) Data Protection and Privacy; (6) Security Training; (7) Information Security Continuous Monitoring; (8) Incident Response; and (9) Contingency Planning. Table 3 summarizes the overall assessed maturity levels for SSA information security program.

Table 3: Assessed Maturity Levels for SSA's Information Security Program

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[9]	Level 3	Level 2
PROTECT	**Level 3**	**Level 3**
Configuration Management	Level 3	Level 2
Identity and Access Management	Level 3	Level 3
Data Protection and Privacy	Level 3	Level 2
Security Training	Level 4	Level 3
DETECT Information Security Continuous Monitoring	**Level 3**	**Level 2**
RESPOND Incident Response	**Level 4**	**Level 4**
RECOVER Contingency Planning	**Level 3**	**Level 3**
Overall Security Program Effectiveness	**Effective**	**Not Effective**

Following are examples of some of the deficiencies Grant Thornton identified.

[9] OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency, FY 2021 *Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics,* V1.1 (May 2021), p. 7, paragraph 2, states, "To provide agencies with sufficient time to fully implement NIST 800-53, Rev 5., in accordance with OMB A-130, these new Supply Chain Risk Management metrics should not be considered for the purposes of the Identify framework function rating."

Identify

- SSA had not fully defined and implemented specific aspects of its risk management program across the Agency.
- SSA had not fully implemented its risk monitoring and communication tools and procedures.
- SSA needed to enhance its policies and processes for maintaining a complete and accurate inventory of information systems.
- SSA needed to improve documentation regarding the timing of completion for plans of action and milestones.
- SSA needed to improve procedures for supply chain risk management.

Protect

- SSA had not completed efforts to develop and document system inventory procedures to ensure a privacy impact analysis is completed for all systems as appropriate.
- SSA did not implement or require role-based privacy training.
- Grant Thornton's security and diagnostic testing identified deficiencies.
- Some new employees did not complete security awareness training timely.

Detect

- SSA's information security continuous monitoring policies, procedures, and strategy lacked certain elements necessary for monitoring the implementation of organization and system level controls.
- SSA had not fully implemented its plan to transition to ongoing security assessments and authorization.

Respond

- SSA defined and implemented incident response technology that was interoperable to the extent practicable. However, Grant Thornton identified some weaknesses.

Recover

- Some contingency plans were not up-to-date.
- System- and Agency-level business impact analyses were not fully integrated to guide contingency planning efforts.

Because of weaknesses the firm identified, Grant Thornton concluded SSA's overall security program was "Not Effective." The weaknesses identified may limit the Agency's ability to adequately protect the confidentiality, integrity, and availability of SSA's information systems and data.

Agency Efforts to Resolve Weaknesses and Potential Causes for the FISMA Deficiencies

In FY 2021, 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 believed that, in many cases, these deficiencies continued to exist 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, configuration management, and incident detection and response.
- SSA established a governance and oversight board but had not implemented procedures to address the root cause(s) of deficiencies and prioritized corrective actions to address the highest areas of risk.
- The design of enhanced or new controls was not fully implemented to address risks and recommendations provided in past audits.

Grant Thornton's Conclusions

Although SSA had established an Agency-wide information security program and practices, Grant Thornton identified numerous deficiencies that may limit its ability to adequately protect the organization's systems and information. Without appropriate security, SSA may not be able to protect its mission assets. Therefore, the Agency's systems, and the sensitive data they contain, are at risk. Some deficiencies Grant Thornton identified could negatively affect the confidentiality, integrity, and availability of the Agency's systems and personally identifiable information.

Grant Thornton's Recommendations to the Agency

To be consistent with FISMA, 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 the protection of 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 throughout the performance audit, Grant Thornton provided SSA with 12 overarching recommendations to address the identified issues.

Office of the Inspector General Comments

SSA houses sensitive information about each individual who has been issued a Social Security number. 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 SSA 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. Without appropriate security, the Agency's systems, and the sensitive data they contain, are at risk.

In FY 2021, the Agency continued its efforts to improve and mature its information security program and practices to protect it from cyber-security threats. Specifically, it achieved a Level 3, Consistently Implemented, rating for Identity and Access Management, Security Training, and Contingency Planning, improvements from the FY 2020 ratings of Level 2, Defined. Finally, SSA continued efforts to redesign its common control inheritance structure and implement its new Governance, Risk, and Compliance tool.

SSA must (1) ensure the appropriate design and operating effectiveness of information security controls; (2) prevent unauthorized access to the sensitive information the public entrusts to SSA; and (3) detect malicious or inappropriate activity.

Agency Comments

SSA management agreed with Grant Thornton's findings. Management's response does not impact the results, findings, and conclusion of Grant Thornton's audit.