



Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

Audit Summary

Summary of the Audit of the Social Security Administration's Information Security Program and Practices for Fiscal Year 2023

142306 *September 2023*



Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: September 25, 2023

Refer to: 142306

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 2023

The attached final report summarizes Ernst & Young LLP's (Ernst & Young) Fiscal Year (FY) 2023 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, Ernst & Young, an independent certified public accounting firm, reviewed SSA's overall information security program and practices for FY 2023. Ernst & Young met with SSA staff and management frequently and reviewed evidence the Agency provided. As required, on July 31, 2023, we submitted to the Office of Management and Budget Ernst & Young's responses to the FY 2023 FISMA Inspector General reporting metrics.

Ernst & Young'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 Ernst & Young's detailed findings and recommendations and excluded from this report certain sensitive information because of the potential damage if the information is misused. 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 2023 142306



September 2023

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) 2023 Inspector General (IG) FISMA reporting metrics as of July 31, 2023.

Background

Under FISMA, SSA must develop, document, and implement an Agency-wide information security program. 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 Ernst & Young LLP (Ernst & Young) to conduct this performance audit in conjunction with the audit of SSA's FY 2023 Financial Statements. Ernst & Young used the FY 2023 IG FISMA reporting metrics in evaluating SSA's overall information security program and practices.

Results

Based on the FY 2023 IG FISMA reporting metrics guidance, Ernst & Young concluded SSA's overall security program was "Not Effective." Ernst & Young made this determination because SSA did not meet the *Managed and Measurable* maturity level for four of the five function areas: Identify, Protect, Detect, and Recover.

Recommendations

In addition to the recommendations provided during the performance audit, Ernst & Young recommended SSA focus on five core areas to strengthen its enterprise-wide, cyber-security program.

1. Continue refining the enterprise architecture system inventory and software and hardware asset inventories.
2. Continue implementing the cyber-security risk management strategy to obtain a comprehensive assessment of risks in the Agency and follow a standardized process to accept and monitor these risks.
3. Implement ongoing authorization to ensure Agency-wide systems are continuously assessed.
4. Continue improving the process for integrating and formalizing risk-based decisions into cyber-security program monitoring activities.
5. Improve oversight and management of user accounts.

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 agreed with Ernst & Young's recommendations.

TABLE OF CONTENTS

Objective.....	1
Background.....	1
Agency Requirements Under the Act	1
Cyber-security Framework Functions and Related Inspector General Metric Domains.....	2
Fiscal Year 2023 Metric Changes.....	2
Ernst & Young’s Scope and Methodology	3
Our Evaluation of Ernst & Young’s Performance.....	4
Results of Ernst & Young’s Review	5
Examples of Ernst & Young’s Findings	6
Ernst & Young’s Recommendations to the Agency	6
Office of the Inspector General’s Comments.....	7
The Office of the Inspector General’s Conclusions.....	8
Agency Comments.....	8
Appendix A – Scope and Methodology	A-1
Appendix B – Fiscal Year 2023 Maturity Model Scoring.....	B-1
Appendix C – Agency Comments.....	C-1

ABBREVIATIONS

CIGIE	Council of the Inspectors General on Integrity and Efficiency
DHS	Department of Homeland Security
EO	Executive Order
ERM	Enterprise Risk Management
FISMA	<i>Federal Information Security Modernization Act of 2014</i>
FIPS	Federal Information Processing Standards
FY	Fiscal Year
Ernst & Young	Ernst & Young, LLP
IG	Inspector General
ISCM	Information Security Continuous Monitoring
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) 2023 Inspector General (IG) FISMA reporting metrics as of July 31, 2023.²

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 Ernst & Young LLP (Ernst & Young) to conduct this performance audit in conjunction with the audit of SSA's FY 2023 Financial Statements.

Ernst & Young used the FY 2023 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), Council of the Inspectors General on Integrity and Efficiency (CIGIE), *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (February 10, 2023). (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 2023 IG FISMA reporting metrics were developed by representatives from the Office of Management and Budget (OMB) and the Council of Inspectors General on Integrity and Efficiency (CIGIE), with review and feedback by several stakeholders, including the Federal Chief Information Officer and Chief Information Security Officers councils. The FY 2023 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 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 2023 IG FISMA Metric Domains

Cyber-security Framework Function	FY 2023 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 2023 Metric Changes

In FY 2022, the IG FISMA metrics included 20 core performance metrics for annual evaluation. These performance metrics represent a combination of OMB priorities, high-impact security processes, and functions essential to determining security program effectiveness. IGs would evaluate the remaining supplemental performance metrics on a 2-year cycle, beginning in FY 2023. Supplemental performance metrics represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.⁷

The FY 2023 IG metrics included 20 supplemental performance metrics for evaluation in addition to the 20 core performance metrics. The metrics also incorporate updates to determine Agency progress in implementing other cyber-security requirements. The FY 2023 IG metrics consisted of questions across the nine FISMA domains, descriptions of the five maturity levels for each core question, and related criteria.

⁶ OMB and CIGIE, *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (February 10, 2023). (dhs.gov/fisma).

⁷ See Footnote 6.

Table 2 includes a general description of the five maturity levels.

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.

Federal agencies are required to use the Department of Homeland Security’s (DHS) CyberScope tool to report IG FISMA metric evaluation results. Previous FISMA guidance directed IGs to use a mode-based scoring approach to assess agency maturity levels. However, OMB and CIGIE determined that scoring based on averages more closely aligned with IGs’ maturity assessments. Therefore, for FY 2023, CyberScope calculated overall, function, and domain averages for core and supplemental performance metrics. In determining maturity levels and the overall effectiveness of the Agency’s information security program, OMB strongly encouraged IGs to focus on the results of the core metrics. IGs should use the averages of the supplemental metrics to support their risk-based determination of overall program and function level effectiveness. The FY 2023 IG FISMA metrics further state an agency’s overall security program is considered effective if it is determined to be at least at Level 4, *Managed and Measurable*.⁸

ERNST & YOUNG’S SCOPE AND METHODOLOGY

In FY 2023, Ernst & Young performed procedures to assess, based on OMB and DHS guidance, SSA’s program effectiveness with FISMA. Ernst & Young tested SSA’s information security controls at two regional offices and three disability determination services. Ernst & Young also selected 18 systems at SSA Headquarters that represented the broader information technology environment implemented at SSA. Further, Ernst & Young selected technologies for technical diagnostic testing and conducted internal, external, wireless, and cloud security penetration testing.

⁸ OMB and CIGIE, *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (February 10, 2023). (dhs.gov/fisma).

To assess SSA's FISMA effectiveness, Ernst & Young leveraged the FY 2023 IG FISMA Evaluator's Guide and SSA's self-assessed maturity levels to develop its procedures.⁹ Ernst & Young also mapped SSA's key information security controls to the metrics in the FY 2023 FISMA domains.

For each IG FISMA metric, Ernst & Young tested the control design through management inquiry and inspecting management policies and procedures. For controls Ernst & Young determined SSA defined adequately, it tested the controls to determine whether they were effectively and consistently implemented. Based on the test results, Ernst & Young determined whether SSA met the associated metric maturity. Ernst & Young provided SSA with a Notice of Findings and Recommendations for each finding identified during testing.

Ernst & Young 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 Ernst & Young's detailed assessments of maturity levels in CyberScope.

Ernst & Young conducted its performance audit in accordance with generally accepted government auditing standards. Those standards require that Ernst & Young 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.

OUR EVALUATION OF ERNST & YOUNG'S PERFORMANCE

We were responsible for technical and administrative oversight regarding Ernst & Young's performance under the contract terms. To fulfill our responsibilities under the *Inspector General Act of 1978*,¹⁰ we monitored Ernst & Young's review by:

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

We did not conduct our review of Ernst & Young'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 Ernst & Young did not comply with our requirements.

⁹ OMB, CIGIE, *FY 2023 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Metrics Evaluator's Guide*, (April 2023). (dhs.gov/fisma).

¹⁰ *Inspector General Act of 1978*, 5 U.S.C. Chapter 4 (2022).

Ernst & Young’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,¹¹ we have separately transmitted to SSA management Ernst & Young’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 ERNST & YOUNG’S REVIEW

Based on the FY 2023 IG FISMA reporting metrics guidance, Ernst & Young concluded SSA’s overall security program was “Not Effective.” Ernst & Young made this determination based on SSA not meeting *Managed and Measurable*, Level 4, maturity for four of the five function areas: Identify, Protect, Detect, and Recover. Table 3 summarizes SSA’s self-assessments and Ernst & Young’s conclusions.

Table 3: Assessed Maturity-level Determinations

Function/Domain	SSA’s Self-Assessment ¹²	Ernst & Young’s Assessment		
		Core Metric Average	Supplemental Metric Average	Maturity
IDENTIFY	Level 3	2.00	2.00	Level 2
Risk Management	Level 3	2.00	2.00	Level 2
Supply Chain Risk Management	Level 3	2.00	2.00	Level 2
PROTECT	***	2.88	3.30	Level 3
Configuration Management	Level 3	2.00	3.33	Level 3
Identity and Access Management	Level 3	2.67	3.25	Level 3
Data Protection and Privacy	Level 4	3.50	2.00	Level 4
Security Training	Level 4	4.00	4.00	Level 4
DETECT	Level 3	2.50	3.00	Level 2
Information Security Continuous Monitoring	Level 3	2.50	3.00	Level 2
RESPOND	Level 4	4.00	4.00	Level 4
Incident Response	Level 4	4.00	4.00	Level 4
RECOVER	Level 3	3.00	3.50	Level 3
Contingency Planning	Level 3	3.00	3.50	Level 3
Overall Security Program Effectiveness	***	2.88	3.16	Not Effective

For a summary of Ernst & Young’s conclusions for the metrics in each domain, see Appendix B.

¹¹ Government Accountability Office, *Government Auditing Standards, 2018 Revision*, GAO-21-568G, 9.66, pp. 209 and 210 (April, 2021).

¹² SSA did not provide self-assessments for the overall Protect function or the Overall Effectiveness determination.

EXAMPLES OF ERNST & YOUNG’S FINDINGS

Following are examples of some of the deficiencies Ernst & Young identified.¹³

Identify

- SSA was not fully performing its defined cyber-security functions and responsibilities.
- 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.
- SSA’s supply chain risk-management policies did not fully address requirements.

Protect

- Ernst & Young’s security and diagnostic testing identified deficiencies.

Detect

- SSA had not completed continuous-monitoring activities for some systems.
- SSA had not completely updated and communicated responsibilities and assignments for control providers.
- SSA had not fully implemented its plan to transition to ongoing security assessments and authorization.
- SSA’s continuous-monitoring strategy did not incorporate performance measures to track effectiveness.

Recover

- SSA had not completed business-impact analyses for all systems.
- SSA had not introduced risk-based allocations of resources to manage the program or defined measurement criteria to hold individuals accountable for fulfilling their roles and responsibilities.
- SSA had not employed automated mechanisms to test system-contingency plans.

ERNST & YOUNG’S RECOMMENDATIONS TO THE AGENCY

In addition to the recommendations provided throughout the performance audit, Ernst & Young recommended SSA focus on five core areas to strengthen its enterprise-wide, cyber-security program.

¹³ Because of their sensitive nature, we shared Ernst & Young’s findings with SSA management in a separate document.

1. Continue refining the enterprise architecture system inventory and software and hardware asset inventories.
2. Continue implementing the cyber-security risk management strategy to obtain a comprehensive oversight of risks in the Agency and follow a standardized process to accept and monitor these risks.
3. Implement ongoing authorization to ensure Agency-wide systems are continuously assessed.
4. Continue improving the process for integrating and formalizing risk-based decisions into cyber-security program monitoring activities.
5. Improve oversight and management of user accounts.

OFFICE OF THE INSPECTOR GENERAL’S COMMENTS

Table 4 summarizes the results of the independent evaluations of SSA’s information security programs since FY 2020.

Table 4: Summary Results By Function—FYs 2020 Through 2023

FUNCTION/Domain	FY 2020	FY 2021	FY 2022	FY 2023
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	Level 2	Level 2	Level 2
PROTECT	Level 2	Level 3 ▲	Level 3	Level 3
Configuration Management	Level 2	Level 2	Level 2	Level 3 ▲
Identity and Access Management	Level 2	Level 3 ▲	Level 3	Level 3
Data Protection and Privacy	Level 2	Level 2	Level 4 ▲	Level 4
Security Training	Level 2	Level 3 ▲	Level 4 ▲	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 4 ▲	Level 4	Level 4	Level 4
Incident Response	Level 4 ▲	Level 4	Level 4	Level 4
RECOVER	Level 2	Level 3	Level 3	Level 3
Contingency Planning	Level 2	Level 3	Level 3	Level 3
Overall Security Program Effectiveness	<i>Not Effective</i>	<i>Not Effective</i>	<i>Not Effective</i>	<i>Not Effective</i>

▲ Indicates a higher maturity rating from the prior FY.

We note the results are not directly comparable across all years because the maturity level determinations are not based on the same number of metrics. Specifically, the results for FYs 2020 and 2021 included all metrics, FY 2022 results included only 20 core metrics, and FY 2023 results include 20 core metrics and 20 supplemental metrics.

In FY 2023, 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 2023 FISMA metrics, the assessed maturity for SSA’s Configuration Management domain improved from Level 2, *Defined*, in FY 2022 to Level 3, *Consistently Implemented*.

Although Ernst & Young determined SSA had achieved higher maturity levels for certain metrics and one domain, Ernst & Young's ratings for the higher-level functions did not change from FY 2022. Also, as in FY 2022, Ernst & Young concluded SSA's overall information security program in FY 2023 was "Not Effective" because the FY 2023 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 agreed with Ernst & Young's recommendations. See Appendix C for the full text of the Agency's response.



Michelle L. Anderson
Assistant Inspector General for Audit

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

The *Federal Information Security Modernization Act of 2014* (FISMA) directs each agency's Inspector General (IG) to perform, or have an independent external auditor perform, an annual independent evaluation of the agency's information security programs and practices as well as a review of an appropriate subset of agency systems.¹

Scope

The objective was to determine whether the Social Security Administration's (SSA) overall information security program and practices were effective and consistent with the FISMA requirements, as defined in the Fiscal Year (FY) 2023 IG FISMA reporting metrics as of July 31, 2023.²

The FY 2023 IG FISMA reporting metrics were assessed at SSA and based on the aggregation of their results. In FY 2023, Ernst & Young tested SSA's information security controls at two regional offices and three disability determination services and on 18 systems at SSA Headquarters. Ernst & Young also mapped the current year Notices of Findings and Recommendations to prior year findings.

Methodology

Ernst & Young mapped SSA's key information security controls to the metrics in the FY 2023 FISMA domains. For each metric question, Ernst & Young tested the design of the control by inquiring with managers and inspecting management policies and procedures. For controls Ernst & Young determined SSA defined adequately, the firm tested controls to determine whether they were effectively and consistently implemented. Depending on the control, Ernst & Young performed procedures for the 18 in-scope systems, random sampling, or inspection of system settings. For specific controls identified for testing, Ernst & Young considered suggested controls outlined in the cyber-security and privacy framework profile of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* along with the security and privacy control baselines identified in NIST for the Government and tailored this guidance to assist in the control selection process.³

¹ 44 U.S.C. §§ 3555(a)(1) and (b)(1).

² *Federal Information Security Management Act of 2014*, Pub. L. No. 113-283, § 2, 128 Stat. 3073, 3075-3078 (2014). Office of Management and Budget (OMB), Council of the Inspectors General on Integrity and Efficiency (CIGIE), *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (February 10, 2023). (dhs.gov/fisma).

³ NIST, *Security and Privacy Controls for Information Systems and Organizations, 800-53 Revision 5* (September 2020).

To accomplish its objectives, Ernst & Young performed the procedures outlined in the Planned Scope and Methodology section of its Statement of Work. This included using Federal guidance to:

- Review applicable Federal laws, regulations, and guidance.
- Gain an understanding of the current security program at SSA.
- Inquire of SSA's self-assessment for each FISMA reporting metric.
- Assess the status of SSA's security program against Agency cyber-security program policies, other standards and guidance issued by SSA management, and reporting metrics.
- Inspect and analyze selected artifacts including, but not limited to, system security plans, evidence to support testing of security controls, Plans of Action and Milestones records, security training records, asset compliance reports, system inventory reports and account management documentation.
- Inspect internal assessments performed on behalf of SSA management that had a similar scope to the FY 2023 IG FISMA metrics and incorporate the results as part of the FY 2023 IG FISMA assessment.
- Inspect artifacts SSA provided related to prior-year ineffective areas to determine the extent to which testing of corrective actions was applicable to the current audit objectives.

Finally, Ernst & Young performed detailed technical security controls testing with SSA's information systems staff's knowledge and consent. For this testing, Ernst & Young's team collaborated with the OIG and SSA's designated points of contact to agree on the Rules of Engagement that defined the nature, timing, and extent of our technical security work (that is, diagnostic or technical security testing outside of Ernst & Young's controls work). Ernst & Young used the NIST SP 800-115 guidance as the foundation to define the attributes of the technical security testing.⁴ This testing focused on selected internal, external, wireless, and cloud systems at SSA.

Ernst & Young conducted these procedures in accordance with generally accepted government auditing standards. Those standards require that Ernst & Young plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. Ernst & Young believes that the evidence obtained provides a reasonable basis for its findings and conclusions based on the audit objectives.

Criteria

The principal criteria used by Ernst & Young for its performance audit included:

- Department of Homeland Security (DHS) Binding Operational Directive 18-02, *Securing High Value Assets*, (May 07, 2018)
- DHS Binding Operational Directive 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*, (April 29, 2019)

⁴ NIST, *Technical Guide to Information Security Testing and Assessment, 800-115* (September 2008).

- DHS Binding Operational Directive 22-01, *Reducing Significant Risk of Known Exploited Vulnerabilities*, (November 03, 2021)
- Executive Order on Improving the Nation's Cybersecurity (EO 14028) (May 12, 2021)
- IG FISMA Metrics Evaluation Guide (2023 Publication)
- *Federal Information Security Modernization Act of 2014* (December 2014)
- Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004).
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006).
- NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems* (May 2010).
- NIST SP 800-37, revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (December 2018).
- NIST SP 800-53, revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations* (September 2020).
- NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide* (August 2012).
- NIST IR 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)* (October 2020)
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (September 2011).
- Office of Management and Budget (OMB) M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007).
- OMB M-19-03, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program* (December 10, 2018)
- OMB M-19-07, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management* (May 21, 2019)
- OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*
- OMB M-21-30, *Protecting Critical Software Through Enhanced Security Measures* (August 10, 2021)
- OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021)
- OMB M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (October 08, 2021)
- OMB M-22-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements* (December 2, 2022)
- OMB M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements* (December 6, 2021)
- OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (January 26, 2022)

Ernst & Young conducted this performance audit in accordance with *Government Auditing Standards*. Those standards require that Ernst & Young 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. Ernst & Young believes that the evidence obtained provides a reasonable basis for its findings and conclusions based on the audit objective.

Appendix B – FISCAL YEAR 2023 MATURITY MODEL SCORING

The Fiscal Year 2023 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 Ernst & Young’s maturity assessments of the function areas, including each security domain, for the Social Security Administration (SSA). Table B–6 summarizes Ernst & Young’s assessment of the Agency’s overall information security program.

¹ Office of Management and Budget, Council of the Inspectors General on Integrity and Efficiency, *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (February 10, 2023). (dhs.gov/fisma).

Table B-1: Assessment Summary of the Identify Function

FUNCTION: IDENTIFY		DEFINED (LEVEL 2)												
Domain: Risk Management		Defined (Level 2)												
<p>“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.” <i>National Institute of Standards and Technology Special Publication 800-53, Rev. 5, Appendix A, p. 415.</i></p> <p>Count of Metrics by Maturity Level:</p> <table border="1"> <thead> <tr> <th>Ad Hoc (Level 1)</th> <th>Defined (Level 2)</th> <th>Consistently Implemented (Level 3)</th> <th>Managed and Measurable (Level 4)</th> <th>Optimized (Level 5)</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>5 Core 3 Supplemental</td> <td>0</td> <td>0</td> <td>0</td> </tr> </tbody> </table>					Ad Hoc (Level 1)	Defined (Level 2)	Consistently Implemented (Level 3)	Managed and Measurable (Level 4)	Optimized (Level 5)	0	5 Core 3 Supplemental	0	0	0
Ad Hoc (Level 1)	Defined (Level 2)	Consistently Implemented (Level 3)	Managed and Measurable (Level 4)	Optimized (Level 5)										
0	5 Core 3 Supplemental	0	0	0										
Domain: Supply Chain Risk Management		Defined (Level 2)												
<p>“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.” <i>National Institute of Standards and Technology Special Publication 800-53, Rev 5, Appendix A, p. 420.</i></p> <p>Count of Metrics by Maturity Level:</p> <table border="1"> <thead> <tr> <th>Ad Hoc (Level 1)</th> <th>Defined (Level 2)</th> <th>Consistently Implemented (Level 3)</th> <th>Managed and Measurable (Level 4)</th> <th>Optimized (Level 5)</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>1 Core 2 Supplemental</td> <td>0</td> <td>0</td> <td>0</td> </tr> </tbody> </table>					Ad Hoc (Level 1)	Defined (Level 2)	Consistently Implemented (Level 3)	Managed and Measurable (Level 4)	Optimized (Level 5)	0	1 Core 2 Supplemental	0	0	0
Ad Hoc (Level 1)	Defined (Level 2)	Consistently Implemented (Level 3)	Managed and Measurable (Level 4)	Optimized (Level 5)										
0	1 Core 2 Supplemental	0	0	0										

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)	Defined (Level 2)	Consistently Implemented (Level 3)	Managed and Measurable (Level 4)	Optimized (Level 5)
0	2 Core 1 Supplemental	0	2 Supplemental	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)	Defined (Level 2)	Consistently Implemented (Level 3)	Managed and Measurable (Level 4)	Optimized (Level 5)
0	1 Core 1 Supplemental	2 Core 2 Supplemental	0	1 Supplemental
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)	Defined (Level 2)	Consistently Implemented (Level 3)	Managed and Measurable (Level 4)	Optimized (Level 5)
0	1 Supplemental	1 Core	1 Core	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)	Defined (Level 2)	Consistently Implemented (Level 3)	Managed and Measurable (Level 4)	Optimized (Level 5)
0	0	0	1 Core 2 Supplemental	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	1 Core	1 Core 1 Supplemental	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 <i>National Institute of Standards and Technology Special Publication SP 800-12</i> , the main benefits of an incident-handling capability are (1) containing and repairing damage from incidents and (2) preventing future damage.				
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 Core	2 Supplemental	1 Core

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	0	2 Core 1 Supplemental	1 Supplemental	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)	
<p>Although SSA established an Agency-wide information security program and practices, Ernst & Young identified deficiencies related to consistent implementation of the Identify function's domains of Risk Management and Supply Chain Risk Management and the Detect function. Further, Ernst & Young identified deficiencies related to management's ability to manage and measure program performance related to the Protect and Recovery functions. Ernst & Young identified no determination to deviate from the <i>Managed and Measurable</i> level as the "effective" state for FY 2023.</p>	

Appendix C – AGENCY COMMENTS



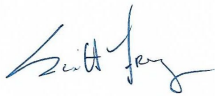
SOCIAL SECURITY

MEMORANDUM

Date: September 15, 2023

Refer To: TQA-1

To: Gail S. Ennis
Inspector General



From: Scott Frey
Chief of Staff

Subject: Office of the Inspector General Draft Report "Summary of the Audit of the Social Security Administration's Information Security Program and Practices for Fiscal Year 2023" (142306) — INFORMATION

Thank you for the opportunity to review the draft report. We agree with the recommendations. We are pleased that the report recognizes our continuing efforts to improve and mature our information security program. We are also pleased that SSA is one of the most improved agencies on the recent Federal Information Technology Acquisition Reform Act cybersecurity scorecard.

Protecting our networks and the information we use to administer our programs remains a critical priority for us, which we demonstrated by our responses to multiple critical threats. 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](https://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.