Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Summary

The Social Security Administration's Information Security Program and Practices for Fiscal Year 2024

142401 September 2024

Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: September 26, 2024 **Refer to:** 142401

To: Martin O'Malley
Commissioner

From: Michelle L. Anderson Michelle L Anderson
Assistant Inspector General for Audit
as Acting Inspector General

Subject: The Social Security Administration's Information Security Program and Practices for Fiscal Year 2024

The attached final report summarizes Ernst & Young LLP's (Ernst & Young) Fiscal Year (FY) 2024 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 2024. Ernst & Young met with SSA staff and management frequently and reviewed evidence the Agency provided. As required, on July 31, 2024, we submitted to the Office of Management and Budget Ernst & Young's responses to the FY 2023-2024 FISMA Inspector General reporting metrics.

Ernst & Young's audit results contain information that, if not protected, could adversely affect 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 call me or have your staff contact Jeffrey Brown, Deputy Assistant Inspector General for Audit.

Attachment

The Social Security Administration's Information Security Program and Practices for Fiscal Year 2024
142401

September 2024 **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) 2023-2024 Inspector General FISMA reporting metrics as of July 31, 2024.

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 could result 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 Inspector General, 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 2024 Financial Statements.

Results

Based on the Inspector General 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 as well as the 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

ABBREVIATIONS

CIGIE	Council of the Inspectors General on Integrity and Efficiency
DHS	Department of Homeland Security
FISMA	*Federal Information Security Modernization Act of 2014*
FIPS	Federal Information Processing Standards
FY	Fiscal Year
Ernst & Young	Ernst & Young, LLP
IG	Inspector General
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) 2023-2024 Inspector General (IG) FISMA reporting metrics as of July 31, 2024.[2]

BACKGROUND

Agency Requirements Under the Act

FISMA requires that SSA develop, document, and implement an Agency-wide information security program.[3] 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 2024 Financial Statements. Ernst & Young used the 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 through 3082 (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).

[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

Representatives from OMB and CIGIE developed the IG FISMA Reporting Metrics with review and feedback by stakeholders, including the Federal Chief Information Officer and Chief Information Security Officers councils. The 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 2024 IG FISMA Reporting Metric Domains[7]

Identify	Protect	Detect	Respond	Recover
✓ Risk Management ✓ Supply Chain Risk Management	✓ Configuration Management ✓ Identity and Access Management ✓ Data Protection and Privacy ✓ Security Training	✓ Information Security Continuous Monitoring	✓ Incident Response	✓ Contingency Planning

Fiscal Year 2024 Metric Changes

In FY 2022, the IG FISMA Reporting 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.[8]

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

[7] OMB and CIGIE, *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics,* p.5 (February 10, 2023).

[8] See Footnote 6.

For FY 2024, IG metrics included 17 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 IG metrics comprise the nine FISMA domains, descriptions of the five maturity levels for each core question, and related criteria. Table 2 describes 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 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 Reporting Metric evaluation results. Previous FISMA guidance directed IGs to use a mode-based scoring approach to assess their agencies' maturity levels. However, OMB and CIGIE determined scoring based on averages more closely aligned with IGs' maturity assessments. Therefore, for FY 2024, 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 IG FISMA Reporting Metrics guidance 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*.[9]

[9] OMB and CIGIE, *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, p. 6 (February 10, 2023).

Ernst & Young's Scope and Methodology

In FY 2024, Ernst & Young assessed SSA's program effectiveness, based on OMB and DHS guidance for FISMA. Ernst & Young tested SSA's information security controls at two regional offices and three disability determination services. Ernst & Young also selected 11 systems at SSA Headquarters that represented the broader information technology environment implemented at SSA. Further, Ernst & Young conducted technical diagnostic testing on a selection of technology platforms and conducted internal, external, wireless, and web application penetration testing.

To assess SSA's program effectiveness under FISMA, Ernst & Young used the IG FISMA Metrics Evaluator's Guide and SSA's self-assessed maturity levels to develop its procedures.[10] Ernst & Young also mapped SSA's key information security controls to the metrics in the FY 2024 FISMA domains.

For each IG FISMA Reporting Metric, Ernst & Young tested the control design by interviewing managers and inspecting management policies and procedures. For controls Ernst & Young determined SSA defined adequately, Ernst & Young 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 IG Assessment maturity levels for the FISMA metrics, domains, functions, and overall security program. Ernst & Young 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.

[10] OMB, CIGIE, *FY 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Metrics Evaluator's Guide,* (April 30, 2024).

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*,[11] 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.

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,[12] 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 2024 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 for FY 2024.

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

[12] Government Accountability Office, *Government Auditing Standards, 2018 Revision Technical Update*, GAO-21-568G, Ch. 9.66, pp. 209 and 210 (April 2021).

Table 3: Assessed Maturity-level Determinations

Function/Domain	SSA's Self-assessment[13]		Ernst & Young's Assessment		
	Core Metric Average	Supplemental Metric Average	Core Metric Average	Supplemental Metric Average	Maturity
IDENTIFY	***	***	**2.00**	**2.00**	**Level 2**
Risk Management	2.40	2.50	2.00	2.00	Level 2
Supply Chain Risk Management	2.00	3.00	2.00	2.00	Level 2
PROTECT	***	***	**3.13**	**3.00**	**Level 3**
Configuration Management	2.00	3.00	2.00	2.33	Level 3
Identity and Access Management	3.33	4.00	3.00	4.00	Level 3
Data Protection and Privacy	3.50	3.00	4.00	2.50	Level 4
Security Training	5.00	4.00	4.00	4.00	Level 4
DETECT	***	***	**2.50**	**2.00**	**Level 2**
Information Security Continuous Monitoring	2.50	2.00	2.50	2.00	Level 2
RESPOND	***	***	**4.00**	**4.33**	**Level 4**
Incident Response	4.00	4.33	4.00	4.33	Level 4
RECOVER	***	***	**2.50**	**3.00**	**Level 3**
Contingency Planning	3.00	3.00	2.50	3.00	Level 3
Overall Security Program Effectiveness	***	***	**2.83**	**2.87**	**Not Effective**

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

Examples of Ernst & Young's Findings

Following are examples of the deficiencies Ernst & Young identified.[14]

Identify

- SSA was not fully performing its defined cyber-security functions and responsibilities.
- SSA had not fully 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.

[13] SSA did not provide self-assessment for domains, functions, or the Overall Effectiveness determination.

[14] Because of their sensitive nature, we shared Ernst & Young's findings with SSA in a separate document.

- 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 or security-authorization activities for some systems.
- 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.

Respond

- SSA had not fully implemented error-logging requirements.
- SSA’s Incident Response playbook was outdated in some areas.

Recover

- SSA had not performed testing exercises for contingency planning for all systems.

Ernst & Young’s Recommendations to the Agency

In addition to the recommendations provided in the performance audit report, 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 as well as 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 2021.

Table 4: Summary Results by Function—FYs 2021 Through 2024

FUNCTION/Domain	FY 2021	FY 2022	FY 2023	FY 2024
IDENTIFY	**Level 2**	**Level 2**	**Level 2**	**Level 2**
Risk Management	Level 2	Level 2	Level 2	Level 2
Supply Chain Risk Management	Level 2	Level 2	Level 2	Level 2
PROTECT	**Level 3**	**Level 3**	**Level 3**	**Level 3**
Configuration Management	Level 2	Level 2	Level 3 ▲	Level 3
Identity and Access Management	Level 3	Level 3	Level 3	Level 3
Data Protection and Privacy	Level 2	Level 4 ▲	Level 4	Level 4
Security Training	Level 3	Level 4 ▲	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 3**	**Level 3**	**Level 3**	**Level 3**
Contingency Planning	Level 3	Level 3	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.

The results are not directly comparable across all years because the maturity-level determinations are not based on the same number of metrics. The results for FY 2020 included 59 metrics, FY 2021 results included 57 metrics, FY 2022 results included only 20 core metrics, FY 2023 results included 20 core and 20 supplemental metrics, and FY 2024 results include 20 core and 17 supplemental metrics.

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 2023. Also, as in FY 2023, Ernst & Young concluded SSA's overall information security program in FY 2024 was "Not Effective" because the FY 2024 IG FISMA Reporting Metrics guidance considers Level 4, *Managed and Measurable*, or higher to be an effective level of security.

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 and responded under separate cover. See Appendix C for the full text of the Agency's response to this Summary Report.

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]

Objective and 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) 2023-2024 IG FISMA Reporting Metrics as of July 31, 2024.[2]

Ernst & Young assessed the IG FISMA Reporting Metrics at SSA and based on the aggregation of their testing results. In FY 2024, Ernst & Young tested SSA's information security controls at 2 regional offices, 3 disability determination services, and 11 systems at SSA Headquarters. Ernst & Young also mapped the current-year Notices of Findings and Recommendations to prior years' findings.

Methodology

Ernst & Young mapped SSA's key information security controls to the metrics in the FY 2024 FISMA domains. For each metric question, Ernst & Young tested the control's design by meeting with managers and inspecting management policies and procedures. For controls Ernst & Young determined SSA defined adequately, it tested controls to determine whether they were effectively and consistently implemented. Depending on the control, Ernst & Young performed procedures for the 11 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 SP 800-53 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, 3075-3082 (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).

[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 security program at SSA.
- Review 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 SSA management's behalf that had a similar scope to the FY 2024 IG FISMA Reporting Metrics and incorporate the results as part of the FY 2024 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 conducted 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 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.

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

Criteria

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

1. Department of Homeland Security (DHS) Binding Operational Directive 18-02, *Securing High Value Assets* (May 07, 2018).

2. DHS Binding Operational Directive 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems* (April 29, 2019).

3. DHS Binding Operational Directive 22-01, *Reducing Significant Risk of Known Exploited Vulnerabilities* (November 03, 2021).

4. *Executive Order on Improving the Nation's Cybersecurity* (EO 14028) (May 12, 2021).

5. *IG FISMA Metrics Evaluation Guide* (2024 Publication).

6. *Federal Information Security Modernization Act of 2014* (December 2014).

7. Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004).

8. Federal Information Processing Standards 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006).

9. NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* (May 2010).

10. 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).

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

12. NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide* (August 2012).

13. NIST IR 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)* (October 2020).

14. NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (September 2011).

15. Office of Management and Budget (OMB) M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007).

16. OMB M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program* (December 10, 2018).

17. OMB M-19-17, *Enabling Mission Delivery Through Improved Identity, Credential, and Access Management* (May 21, 2019).

18. OMB M-16-17, OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 15, 2016).

19. OMB M-21-30, *Protecting Critical Software Through Enhanced Security Measures* (August 10, 2021).

20. OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021)

21. OMB M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (October 08, 2021).

22. OMB M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements* (December 4, 2023).

23. OMB M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements* (December 6, 2021).

24. 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 the evidence obtained provides a reasonable basis for its findings and conclusions based on the audit objective.

Appendix B – Fiscal Year 2024 Maturity Model Scoring

The Fiscal Year 2023-2024 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.

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 Special Publication 800-53*, Rev. 5, Appendix A, p. 415.

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 Core 2 Supplemental	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." *National Institute of Standards and Technology Special Publication 800-53*, Rev 5, Appendix A, p. 420.

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	0	0	0

[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).

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 2 Supplemental	1 Supplemental	0	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 Core	1 Core 1 Supplemental	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)	Defined (Level 2)	Consistently Implemented (Level 3)	Managed and Measurable (Level 4)	Optimized (Level 5)
0	1 Supplemental	1 Core 1 Supplemental	0	1 Core
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 Supplemental	1 Core	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.				
		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 1 Supplemental

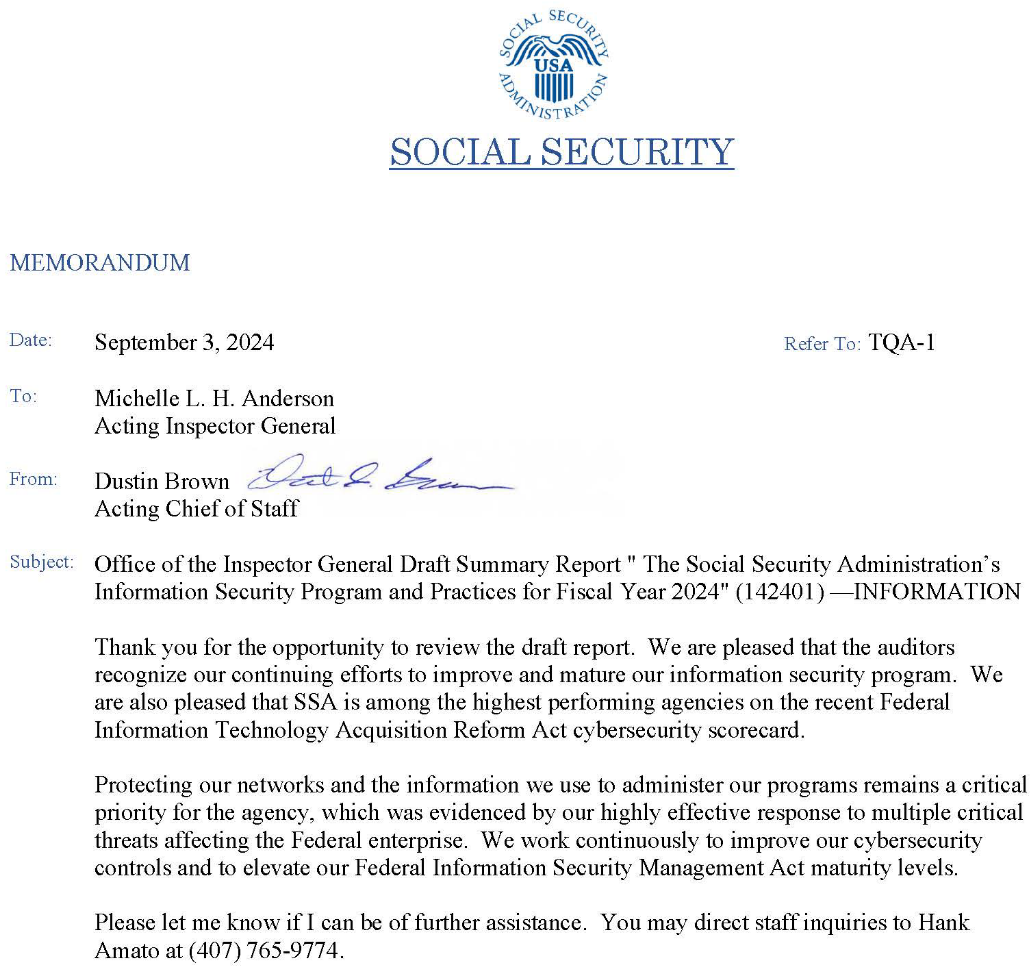
Table B–5: Assessment Summary of the Recover Function

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 Core	1 Core 2 Supplemental	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, 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 *Managed and Measurable* level as "effective" for FY 2024.	

Appendix C – AGENCY COMMENTS



SOCIAL SECURITY

MEMORANDUM

Date: September 3, 2024 Refer To: TQA-1

To: Michelle L. H. Anderson
Acting Inspector General

From: Dustin Brown
Acting Chief of Staff

Subject: Office of the Inspector General Draft Summary Report " The Social Security Administration's Information Security Program and Practices for Fiscal Year 2024" (142401) —INFORMATION

Thank you for the opportunity to review the draft report. We are pleased that the auditors recognize our continuing efforts to improve and mature our information security program. We are also pleased that SSA is among the highest performing 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 the agency, which was evidenced by our highly effective response to multiple critical threats affecting the Federal enterprise. 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 Hank Amato at (407) 765-9774.

OFFICE OF THE INSPECTOR GENERAL ★ SOCIAL SECURITY ADMINISTRATION ★

OIG

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:

𝕏 @TheSSAOIG

f OIGSSA

▶ TheSSAOIG

✉ Subscribe to email updates on our website.