Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Summary

The Social Security Administration's Information Security Program and Practices for Fiscal Year 2025

142501 September 2025

Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: September 30, 2025 **Refer to:** 142501

To: Frank Bisignano
Commissioner

From: Michelle L. Anderson
Acting Inspector General

Subject: The Social Security Administration's Information Security Program and Practices for Fiscal Year 2025

The attached final report summarizes Ernst & Young LLP's (Ernst & Young) Fiscal Year (FY) 2025 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 2025. Ernst & Young met with SSA staff and management frequently and reviewed evidence the Agency provided. As required, on July 31, 2025, we submitted to the Office of Management and Budget Ernst & Young's responses to the FY 2025 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 2025 142501

September 2025 **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 2025 Inspector General FISMA reporting metrics as of July 31, 2025.

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 Fiscal Year 2025 Financial Statements.

Results

Based on the Inspector General FISMA reporting metrics, 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 five of the six functions: Govern, 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, cybersecurity program.

1. Continue refining the enterprise architecture system inventory as well as software, hardware, data, and metadata inventories.
2. Continue implementing the cybersecurity risk management strategy to obtain a comprehensive assessment of risks to the Agency and follow a standardized process to accept and monitor these risks.
3. Implement ongoing authorization to ensure it continuously assesses Agency-wide systems.
4. Continue improving the process for integrating and formalizing risk-based decisions into cybersecurity 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 its information security controls are appropriately designed and operating effectively.

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
Ernst & Young	Ernst & Young, LLP
FISMA	*Federal Information Security Modernization Act of 2014*
FY	Fiscal Year
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) 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) 2025 Inspector General (IG) FISMA reporting metrics as of July 31, 2025.[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 whether they are effective.[5] We engaged Ernst & Young LLP (Ernst & Young) to conduct this performance audit in conjunction with the audit of SSA's FY 2025 Financial Statements. Ernst & Young used the IG FISMA Reporting Metrics to evaluate 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 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0* (April 3, 2025).

[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).

Cybersecurity Framework Functions and Related Inspector General Metric Domains

Representatives from OMB and CIGIE developed the IG FISMA Reporting Metrics with review and feedback from 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 *Cybersecurity Framework 2.0* areas.[6] Table 1 includes the in-scope reporting metric domains for the performance audit.

Table 1: Aligning the Cybersecurity Framework with the FY 2025 IG FISMA Reporting Metric Domains[7]

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

Fiscal Year 2025 Metrics

For FY 2025, the IG FISMA Reporting Metrics included 20 core metrics for annual evaluation. These metrics represent a combination of Administration priorities and other high-value controls.[8] The FY 2025 IG metrics also included five supplemental metrics for evaluation. Supplemental metrics represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.[9]

[6] OMB & CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0*, p. 6 (April 3, 2025).

[7] OMB & CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0,* p. 5 (April 3, 2025).

[8] OMB & CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0,* p. 4 (April 3, 2025).

[9] OMB & CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0,* p. 8 (April 3, 2025).

The new Govern function included three of the five supplemental metrics in the new Cybersecurity Governance domain.[10] The additional function and domain underscored the critical role of governance in managing cybersecurity risks and incorporating cybersecurity into an organization's broader enterprise risk management strategy.[11] The remaining two supplemental metrics addressed the security posture of assets and inventories of data and metadata.[12]

The IG metrics comprise the 10 FISMA domains, descriptions of the 5 maturity levels for each 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. For FY 2025, CyberScope calculated overall and function 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, function, and domain-level effectiveness.

[10] OMB & CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0*, pp. 6 and 7 (April 3, 2025).

[11] OMB & CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0,* p. 6 (April 3, 2025).

[12] OMB & CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0,* p. 7 (April 3, 2025).

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*.[13]

ERNST & YOUNG'S SCOPE AND METHODOLOGY

In FY 2025, Ernst & Young assessed SSA's program effectiveness, based on OMB and DHS guidance for FISMA. Ernst & Young tested SSA's information security controls at three regional offices and selected 22 systems at SSA Headquarters that represented the broader information technology environment implemented at the Agency. Further, Ernst & Young conducted technical diagnostic testing on a selection of technology platforms and conducted internal, external, wireless, and cloud-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.[14] Ernst & Young also mapped SSA's key information security controls to the metrics in the FY 2025 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.

[13] OMB & CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, pp. 9 and 10 (April 3, 2025).

[14] OMB & CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Metrics Evaluator's Guide, Version 1.0* (May 5, 2025).

OFFICE OF THE INSPECTOR GENERAL'S EVALUATION OF ERNST & YOUNG'S PERFORMANCE

The OIG provides technical and administrative oversight regarding Ernst & Young's performance under the contract terms. To fulfill our responsibilities under the *Inspector General Act of 1978*,[15] 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 adversely affect the Agency's information systems. In accordance with government auditing standards,[16] 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 2025 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 five of the six functions: Govern, Identify, Protect, Detect, and Recover. Table 3 summarizes Ernst & Young's conclusions for FY 2025.

[15] 5 U.S.C. Ch. 4.

[16] 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	Ernst & Young's Assessment		
	Core Metric Average	Supplemental Metric Average	Maturity
Govern	2.00	2.33	Level 2
Identify	2.00	1.00	Level 2
Protect	3.00	N/A	Level 3
Detect	2.50	3.00	Level 3
Respond	4.00	N/A	Level 4
Recover	2.00	N/A	Level 2
Overall Security Program	**2.58**	**2.11**	**Level 3**

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 by function.[17]

Govern

- SSA needed to improve its cybersecurity risk management program to address specific guidance.
- SSA's supply chain risk-management policies did not fully address requirements.

Identify

- SSA had not fully implemented all aspects of its risk-monitoring tool.
- SSA needed to fully implement its policies and processes for maintaining a complete and accurate inventory of information systems, hardware, and software.
- SSA did not maintain a comprehensive and accurate inventory of data and corresponding metadata.
- SSA had not fully implemented its defined security architecture.
- SSA had not completed privacy impact assessments for two systems.

Protect

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

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

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.
- Although SSA defined performance measures for its continuous-monitoring program, it needed to improve monitoring to track effectiveness.

Respond

- SSA had not fully implemented event logging requirements.

Recover

- SSA did not complete contingency exercises for all systems.
- SSA needed to update and improve its business impact analyses.

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, cybersecurity program.

1. Continue refining the enterprise architecture system inventory as well as software, hardware, data, and metadata inventories.
2. Continue implementing the cybersecurity risk management strategy to obtain a comprehensive assessment of risks to the Agency and follow a standardized process to accept and monitor these risks.
3. Implement ongoing authorization to ensure it continuously assesses Agency-wide systems.
4. Continue improving the process for integrating and formalizing risk-based decisions into cybersecurity 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 2025

FUNCTION/Domain	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025
GOVERN	**N/A**	**N/A**	**N/A**	**N/A**	**Level 2**
Cybersecurity Governance	N/A	N/A	N/A	N/A	Level 2
Cybersecurity Supply Chain Risk Management[18]	Level 2	Level 2	Level 2	Level 2	Level 2
IDENTIFY	**Level 2**	**Level 2**	**Level 2**	**Level 2**	**Level 2**
Risk and Asset Management[19]	Level 2	Level 2	Level 2	Level 2	Level 2
PROTECT	**Level 3**	**Level 3**	**Level 3**	**Level 3**	**Level 3**
Configuration Management	Level 2	Level 2	Level 3 ▲	Level 3	Level 2▼
Identity and Access Management	Level 3	Level 3	Level 3	Level 3	Level 3
Data Protection and Privacy	Level 2	Level 4 ▲	Level 4	Level 4	Level 4
Security Training	Level 3	Level 4 ▲	Level 4	Level 4	Level 3▼
DETECT	**Level 2**	**Level 2**	**Level 2**	**Level 2**	**Level 3▲**
Information Security Continuous Monitoring	Level 2	Level 2	Level 2	Level 2	Level 3▲
RESPOND	**Level 4**	**Level 4**	**Level 4**	**Level 4**	**Level 4**
Incident Response	Level 4	Level 4	Level 4	Level 4	Level 4
RECOVER	**Level 3**	**Level 3**	**Level 3**	**Level 3**	Level 2▼
Contingency Planning	Level 3	Level 3	Level 3	Level 3	Level 2▼
Overall Security Program	***N/A***	***N/A***	***N/A***	***N/A***	***Level 3***[20]
Overall Security Program Effectiveness	***Not Effective***	***Not Effective***	***Not Effective***	***Not Effective***	***Not Effective***

▲ Indicates a higher maturity rating than the prior FY.

▼ Indicates a lower maturity rating than 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. Between FYs 2021 and 2025, the number of metrics ranged from 25 to 57.

For FY 2025, Ernst & Young rated three domains lower and one domain higher than the prior year. As a result, the firm rated one function lower and one function higher. Ernst & Young rated SSA's overall security program at Level 3, *Consistently Implemented*. As in previous years, the program was "Not Effective" in FY 2025 because the FY 2025 IG FISMA Reporting Metrics guidance considers Level 4, *Managed and Measurable*, or higher to be an effective level of security.

[18] Supply Chain Risk Management was a domain under the Idenitfy function before FY 2025.

[19] The Risk Management domain was changed to Risk and Asset Management in FY 2025.

[20] FY 2025 was the first year CyberScope required a maturity rating for the overall security program.

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. SSA must improve its risk management processes and ensure its information security controls are appropriately designed and operating effectively.

AGENCY COMMENTS

SSA agreed with Ernst & Young's recommendations. 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) 2025 IG FISMA Reporting Metrics as of July 31, 2025.[2]

Ernst & Young assessed the IG FISMA Reporting Metrics at SSA and based its conclusions on the aggregation of its testing results. In FY 2025, Ernst & Young tested SSA's information security controls at 3 regional offices and 22 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 2025 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 22 in-scope systems, random sampling, or inspection of system settings. For specific controls identified for testing, Ernst & Young considered suggested controls outlined in the cybersecurity 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 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v 2.0* (April 3, 2025).

[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 the following.

- Reviewing applicable Federal laws, regulations, and guidance.
- Gaining an understanding of the security program at SSA.
- Reviewing SSA's self-assessment for each FISMA reporting metric.
- Assessing the status of SSA's security program against its cybersecurity program policies, other standards and guidance issued by SSA management, and reporting metrics.
- Inspecting and analyzing 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.
- Inspecting internal assessments performed on SSA management's behalf that had a similar scope to the *FY 2025 IG FISMA Reporting Metrics* and incorporating the results as part of the FY 2025 IG FISMA assessment.
- Inspecting 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 the 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 its findings and conclusions based on the 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* (2025 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 3, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile* (April 2025).
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-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (January 26, 2022).

23. OMB M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements* (January 15, 2025)

Appendix B – Fiscal Year 2025 Maturity Model Scoring

The Fiscal Year 2025 Inspector General *Federal Information Security Modernization Act of 2014* reporting metrics continued using the maturity model approach for all security domains and were fully aligned with the National Institute of Standards and Technology Cybersecurity Framework 2.0 functions.[1] Tables B–1 through B–6 summarize Ernst & Young's maturity assessments of the functions, including each security domain, for the Social Security Administration (SSA). Table B–7 summarizes Ernst & Young's assessment of the Agency's overall information security program.

Table B–1: Assessment Summary of the Govern Function

FUNCTION: Govern				**DEFINED (LEVEL 2)**
Domain: Cybersecurity Governance				**Defined (Level 2)**
Governance plays a critical role in managing cybersecurity risks and incorporating cybersecurity into an organization's broader enterprise risk management strategy.				
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 Supplemental	1 Supplemental	0	0
Domain: Cybersecurity 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	0	0	0

[1] Office of Management and Budget, Council of the Inspectors General on Integrity and Efficiency, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0* (April 3, 2025).

Table B–2: Assessment Summary of the Identify Function

FUNCTION: IDENTIFY	DEFINED (LEVEL 2)
Domain: Risk and Asset 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)
1 Supplemental	5 Core	0	0	0

Table B–3: 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	0	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	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	0	1 Core	0	1 Core

FUNCTION: PROTECT	CONSISTENTLY IMPLEMENTED (LEVEL 3)
Domain: Security Training	**Consistently Implemented (Level 3)**

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	1 Core	0	0

Table B–4: Assessment Summary of the Detect Function

FUNCTION: DETECT	CONSISTENTLY IMPLEMENTED (LEVEL 3)
Domain: Information Security Continuous Monitoring	**Consistently Implemented (Level 3)**

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–5: 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	0	1 Core

Table B–6: Assessment Summary of the Recover Function

FUNCTION: RECOVER	DEFINED (LEVEL 2)
Domain: Contingency Planning	**Defined (Level 2)**
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	2 Core	0	0	0

Table B–7: Assessment Summary of SSA's Overall Information Security Program

Overall Information Security Program	Not Effective
GOVERN	Defined (Level 2)
IDENTIFY	Defined (Level 2)
PROTECT	Consistently Implemented (Level 3)
DETECT	Consistently Implemented (Level 3)
RESPOND	Managed and Measurable (Level 4)
RECOVER	Defined (Level 2)
Conclusion	**Consistently Implemented (Level 3)**

Ernst & Young determined SSA's cybersecurity program was "Not Effective." The firm based its determination on SSA not meeting Managed and Measurable maturity for five of the six functions: Govern, Identify, Protect, Detect, and Recover.

Although Ernst & Young rated three of the six functions at Level 2, *Defined*, the firm assessed the overall program at the Level 3, *Consistently Implemented*. The lack of consistent implementation at the Governance and Identify functions prevented SSA from appropriately managing and measuring risk, but not necessarily consistently implementing its program.

To determine whether individual domains and functions were effective, Ernst & Young reviewed core metric scores and the relevant risks identified by the evaluation of the supplemental metric areas or other risk factors identified during the audit period.

Appendix C – Agency Comments

SOCIAL SECURITY
Office of the Commissioner

MEMORANDUM

Date: September 19, 2025 Refer To: TQA-1

To: Michelle L. Anderson
Acting Inspector General

From: Chad Poist
Chief of Staff

Subject: Office of the Inspector General Draft Report, "The Social Security Administration's Information Security Program and Practices for Fiscal Year 2025" (142501L/142501) - INFORMATION

Thank you for the opportunity to review the draft report. We agree with the recommendations.

Please let me know if I can be of further assistance. You may direct staff inquiries to Amy Gao, Director of the Audit Liaison Staff, at (410) 966-1711.

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:

@TheSSAOIG

OIGSSA

TheSSAOIG

Subscribe to email updates on our website.