Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

Audit Summary

Security of the Earnings Record Maintenance System - Cloud

142310 September 2023

Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: September 25, 2023 **Refer to:** 142310

To: Kilolo Kijakazi
Acting Commissioner

From: Gail S. Ennis Gail S. Ennis
Inspector General

Subject: Security of the Earnings Record Maintenance System - Cloud

The attached final report summarizes Ernst & Young LLP's (Ernst & Young) review of the security of the Social Security Administration's (SSA) Earnings Record Maintenance System - Cloud.

Under a contract the Office of Audit monitored, Ernst & Young, an independent certified public accounting firm, who reviewed the security of SSA's Earnings Record Maintenance System – Cloud. Ernst & Young interviewed SSA staff and management and reviewed evidence the Agency provided.

Ernst & Young's audit results contain information that, if not protected, could be used to adversely affect SSA's information systems. In accordance with government auditing standards, we have transmitted Ernst & Young's detailed findings and recommendations to SSA management and excluded from this summary 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 Michelle L. Anderson, Assistant Inspector General for Audit.

Attachment

TABLE OF CONTENTS

ABBREVIATIONS

ERMS-C	Earning Record Maintenance System – Cloud
Framework	NIST Cybersecurity Framework
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
SSA	Social Security Administration

OBJECTIVE

The objective was to determine the effectiveness of information security controls of the Earnings Record Maintenance System – Cloud (ERMS-C) information technology security environment.

BACKGROUND

ERMS-C accounts for the cloud assets that support the ERMS business processes.
The ERMS-C business processes comprise the integrated sub-systems that maintain and provide for individuals' and employers' use of major earnings files and data.
These sub-systems are categorized in four major system groups: Annual Wage Reporting, Electronic Wage Reporting, Earnings Corrections, and Earnings Queries.

The Office of Management and Budget requires that Federal agencies implement National Institute of Standards and Technology (NIST) security controls.[1] The guidance specifies security controls for organizations and information systems that each agency can tailor based on their specific risk posture, tolerance, and appetite.

NIST's Cybersecurity Framework (Framework) focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of an organization's risk-management processes.[2] The Framework consists of three parts:

1. The Framework Core is a set of cyber-security activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational profiles.

2. Implementation Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cyber-security risk, which will help in prioritizing and achieving cyber-security objectives.

3. Framework Profiles help an organization align and prioritize its cyber-security activities with its business/mission requirements, risk tolerances, and resources. The Framework Profiles are divided into five functions: Identify, Protect, Detect, Respond, and Recover.[3]

The Social Security Administration's (SSA) management is responsible for defining the policies, procedures, and processes supporting the implementation of the SSA's Information Security Program including for the ERMS-C environment.

[1] Office of Management and Budget, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, *M-19-17* (2019).

[2] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1, p. v (April 2018).

[3] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1, ch. 1.1, pp. 3-4 (April 2018).

Scope and Methodology

Ernst & Young conducted this performance audit in accordance with generally accepted government auditing standards.[4] Ernst & Young evaluated the ERMS-C implementation of SSA's Information Security Program in accordance with specified areas outlined in our Statement of Work's Planned Scope and Methodology.[5] These specified areas were mapped to the Framework:

- conducted system walkthroughs with SSA personnel to understand the ERMS-C control environment and identified relevant policies, procedures, and processes;
- observed controls as they occurred and inspected evidence to support the controls' implementation; and
- performed detailed technical security controls testing with SSA's Information System staff knowledge and consent.

See Appendix A for details of Ernst & Young's scope and methodology.

Results of Review

Ernst & Young concluded SSA's ERMS-C information technology security environment was not effectively designed or, in some instances, had not fully implemented procedures and practices to address the requirements outlined in the SSA's Information Security Program and related NIST guidance.[6] Ernst & Young noted SSA ERMS-C had not defined procedures to:

1. capture security requirements associated with interfaces; and
2. review third-party risks to the system to evaluate findings and vulnerabilities.

Ernst & Young also noted, in some instances, SSA had not:

1. consistently updated system security plan documentation to reflect current required system security plan information;
2. updated system security plan documentation to identify control implementation requirements for all required controls;
3. define timeframe for remediation of Open Web Application Security Project (OWASP) vulnerabilities;
4. maintained evidence to support the performance of audit log review processes; and

[4] Government Accountability Office, *Government Auditing Standards, GAO-21-368G* (April 2021).

[5] Contract Number GS-00F-290CA, Ernst & Young LLP-SSA Office of Acquisition and Grants, Task Order Number 28321323FDX030009, Attachment 1, sec. 6, pp. 65-72, October 31, 2022.

[6] Ernst & Young's audit results contain information that, if not protected, could be used to adversely affect SSA's information systems. In accordance with government auditing standards, we have transmitted Ernst & Young's detailed findings and recommendations to SSA management and excluded from this report certain sensitive information because of the potential damage if the information is misused. We have determined the omitted information neither distorts the audit results described in this report nor conceals improper or illegal practices.

5. defined roles and responsibilities for disaster recovery responses.

RECOMMENDATIONS

Ernst & Young provided seven recommendations to address the identified security-related findings related to ERMS-C. Ernst & Young transmitted the recommendations to SSA management separately.

OFFICE OF THE INSPECTOR GENERAL'S COMMENTS

SSA houses, in its Master Earnings File, sensitive information about each person who has been issued a Social Security number. SSA should ensure ERMS-C has an effective information technology security environment to protect the sensitive data it contains.

AGENCY COMMENTS

SSA agreed with Ernst & Young's recommendations. See Appendix B for the full text of the Agency's response.

Michelle L Anderson

Michelle L. Anderson
Assistant Inspector General for Audit

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

Scope

The purpose of the Social Security Administration's (SSA) Earnings Records Maintenance System – Cloud (ERMS-C) Supplemental In-Depth Performance Audit is to determine the effectiveness of a selection of information security controls from ERMS-C. Ernst & Young did this by assessing SSA's policies, procedures, and processes in accordance with the *Federal Information Security Modernization Act of 2014*.[1] The information security controls selected for testing are in the following areas: Security Management, Access Controls, Audit Logging & Monitoring, Change and Configuration Management, Disaster Recovery, and Incident Response. SSA defines ERMS-C as follows:

> [ERMS-C] is a major SSA application comprised of a collection of integrated sub-systems that maintain and provided for the use of major earnings files and data from individuals and employers. [The] ERMS-C project accounts for the cloud assets supporting the ERMS business processes. Its configuration contains four of the five major system groups: Annual Wage Reporting, Electronic Wage Reporting, Earnings Queries, and Earnings Corrections.[2]

Methodology

To accomplish the objectives, Ernst & Young performed the procedures outlined in the Statement of Work's[3] Planned Scope and Methodology. Below is a list of criteria Ernst & Young used to conduct the ERMS-C performance audit:

- Government Accountability Office, *Federal Information System Controls Audit Manual*.
- Government Accountability Office, *Government Auditing Standards*, Chapters 8 and 9.
- Office of Management and Budget Circular A-130, *Managing Federal Information as a Strategic Resource*, Appendix I, *Responsibilities for Protecting and Managing Federal Information Resources*.
- National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 5.
- NIST, Federal Information Processing Standards Publications.
  - 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004);
  - 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006); and
  - 201-3, *Personal Identity Verification of Federal Employees and Contractors* (January 2022).

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

[2] SSA, *System Security Plan for Earnings Record Maintenance System - Cloud* (2023).

[3] Contract Number GS-00F-290CA, Ernst & Young LLP-SSA Office of Acquisition and Grants, Task Order Number 28321323FDX030009, Attachment 1, sec. 6, pp. 65-72, October 31, 2022.

- Federal Risk and Authorization Management Program *Security Assessment Framework; System Security Plan Baseline Template*; and *Continuous Monitoring Strategy & Guide*.
- SSA policies and procedures.

Ernst & Young evaluated the ERMS-C implementation of SSA's Information Security Program in accordance with specified areas mapped to the NIST Cybersecurity Framework:[4]

- **Identify:**
  - Business Environment: Determine whether interface, business process, and data controls had been defined.
  - Governance: Determine whether ERMS-C roles and responsibilities had been adequately defined.
- **Protect:**
  - Identity Management and Access Controls: Determine whether ERMS-C had implemented logical access controls, role-based access, segregation of duties, and privileged account management controls.
  - Information Protection Processes and Procedures: Determine whether ERMS-C had documented and implemented the system development life-cycle processes, change management, and version-control processes.
  - Protective Technologies: Determine whether ERMS-C (application-level) had implemented a vulnerability management plan, policy, and procedures.
- **Detect/Anomalies and Events:** Determine whether ERMS-C had defined appropriate auditable and, security events, and implemented an appropriate monitoring process.
- **Respond/Response Planning:** Determine whether ERMS-C had implemented incident response plans, policies, and procedures.
- **Recover/Recovery Planning:** Determine whether the disaster-recovery processes had been documented and implemented.

Ernst & Young considered controls outlined in the NIST security and privacy control baselines,[5] and tailored this guidance to assist in the control selection process. Additionally, Ernst & Young considered the NIST Cybersecurity Framework and Privacy Framework[6] to identify additional controls to test and meet the audit objective.

[4] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1 (April 2018).

[5] NIST, *Control Baselines for Information Systems and Organizations*, *800-53B* (October 2020, amended December 2020).

[6] NIST, *Security and Privacy Controls for Information Systems and Organizations*, *800-53 Revision 5* (September 2020); NIST, *Cybersecurity Framework/Privacy Framework to NIST Special Publication 800-53, Revision 5 Mapping* (July 2023).

Ernst & Young conducted system walkthroughs with SSA personnel to understand the ERMS-C control environment and identified relevant policies, procedures, and processes. In addition, Ernst & Young observed controls as they occurred and inspected evidence to support the implementation of the control. To the extent possible, Ernst & Young leveraged the audit work performed for *The Social Security Administration's Information Security Program and Practices for Fiscal Year 2023* (142306) and *The Social Security Administration's Financial Reporting for Fiscal Year 2023* (152308).

Finally, Ernst & Young performed detailed technical security controls testing with the knowledge and consent of staff in SSA's Office of Information Systems. For this testing, the team collaborated with SSA's Office of the Inspector General and designated SSA points of contact to agree on the Rules of Engagement that defined the nature, timing, and extent of the technical security work, such as diagnostic or technical security testing outside of the controls work. Ernst & Young used NIST Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment,* guidance as the foundation to define the attributes of the technical security testing. This testing focused on the following domains for the ERMS-C and its subsystems to include the following:

- Network architecture of external facing systems,
- Assessment of internal Internet Protocol addresses for exposure,
- Web application firewall enablement,
- Audit logging and monitoring, and
- Security of exposed assets.

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 – Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: September 21, 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, "Security of the Earnings Record Maintenance System-Cloud" (142310L) — 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 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](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.