Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Summary

Ransomware Prevention and Response

142309 September 2023

Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: September 25, 2023 **Refer to:** 142309

To: Kilolo Kijakazi
Acting Commissioner

From: Gail S. Ennis
Inspector General

Subject: Ransomware Prevention and Response

The attached final report summarizes Ernst & Young LLP's (Ernst & Young) review of the Social Security Administration's (SSA) ransomware prevention and response strategy.

Under a contract the Office of Audit monitored, Ernst & Young, an independent certified public accounting firm, reviewed SSA's ransomware prevention and response program. Ernst & Young met with SSA staff and management frequently and reviewed evidence SSA provided.

Ernst & Young's audit results contain information that, if not protected, could result in adverse effects to the Agency's information systems. In accordance with government auditing standards, we have separately transmitted to SSA management Ernst & Young's detailed findings and recommendations and excluded from this summary 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.

If you wish to discuss the final report, please contact Michelle L. Anderson, Assistant Inspector General for Audit.

Attachment

TABLE OF CONTENTS

ABBREVIATIONS

CISA	Cybersecurity and Infrastructure Security Agency
FISMA	*Federal Information Security Modernization Act of 2014*
GAO	Government Accountability Office
MS-ISAC	Multi-State Information Sharing and Analysis Center
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
SSA	Social Security Administration

OBJECTIVE

The objective was to assess the Social Security Administration's (SSA) overall ransomware prevention and response strategy.

BACKGROUND

Ransomware is a type of malicious attack where individuals encrypt an organization's data and information and demand payment to restore, or not disclose, the information to authorities, competitors, or the public. Ransomware incidents can impact business processes and leave organizations without the data they need to operate and deliver mission-critical services.

Ransomware incidents have become more destructive in nature and scope. According to Verizon's 2022 Data Breach Investigation Report, 40 percent of ransomware attacks gained access to the victim's network by using stolen credentials and 35 percent by using phishing emails.[1] Once in the network, malicious actors target critical data and propagate ransomware across entire networks. These actors also increasingly use such tactics as deleting system backups, so it is more difficult or infeasible for affected organizations to restore and recover data. Further, ransomware attacks differ from other cybersecurity events where access may be surreptitiously gained to information such as intellectual property, credit card data, or personally identifiable information, which is then later exfiltrated for monetization. Instead, ransomware threatens an immediate impact on business operations.

The economic and reputational impacts of ransomware incidents, from the initial disruption and, at times, through the extended recovery, have also proven a challenge for organizations. During a ransomware event, organizations may have little time to mitigate or remediate impact, restore systems, or communicate via necessary business, partner, and public-relations channels. Therefore, organizations must be prepared by educating users of cyber-systems, response teams, and business decisionmakers about the importance of—and processes and procedures for—preventing and handling compromises before they occur.

[1] NIST, *Guide to Malware Incident Prevention and handling for Desktops and Laptops*, 800-83 Revision 1, Appendix A, p.33 (November 2006). Phishing: Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

In 2020, the Cybersecurity and Infrastructure Security Agency (CISA) and Multi-State Information Sharing and Analysis Center (MS-ISAC) released a joint *Ransomware Guide*.[2] The Guide is a customer-centered, one-stop resource with best practices and ways to prevent, protect, and/or respond to a ransomware attack. CISA and MS-ISAC distributed the Guide to inform and enhance network defense and reduce exposure to a ransomware attack. In May 2023, the *Ransomware Guide* was updated and renamed the CISA *#StopRansomware Guide*. While Ernst & Young did not use the *CISA #StopRansomware Guide* as criteria during this audit, it refers to the Guide in its recommendations as the Guide is the current leading practice for Ransomware prevention and response strategy. Further, in February of 2022 the National Institute of Standards and Technology (NIST) issued guidance that mapped security objectives to security capabilities specific to ransomware events.[3]

SCOPE AND METHODOLOGY

Ernst & Young conducted this performance audit in accordance with generally accepted government auditing standards.[4] Ernst & Young performed the procedures outlined in our Statement of Work's Planned Scope and Methodology:[5]

- assessed SSA's ransomware risk management plan and strategy, including such security management tasks as reviewing the Agency's governance and oversight structure; assessing ransomware risk, business impact, and strategy; reviewing any plans or actions to address identified risks and Federal ransomware guidance; and assessing any crisis management actionable plans/strategy for responding to ransomware attacks;
- assessed and tested SSA's ransomware detective and preventive controls using the *Ransomware Guide* and assessed SSA's use of threat intelligence, phishing exercises, firewall rules and its network segmentation, and security awareness and training; and
- determined whether SSA has secure and segregated backups and assessed SSA's contingency planning and recovery strategy and capability.

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

[2] CISA and MS-ISAC, *Ransomware Guide* (September 2020).

[3] NIST Interagency or Internal Report 8374, *Ransomware Risk Management: A Cybersecurity Framework Profile* (February 2022).

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

[5] Contract Number: GS-00F-290CA, Task Order Number 28321323FDX030009.

RESULTS OF REVIEW

Ernst & Young concluded SSA's Ransomware Prevention and Response Strategy did not effectively implement procedures and practices to address CISA and NIST guidance.[6] For example, Ernst & Young found SSA had not:

1. fully defined roles and responsibilities in its Cyber Incident Response and Recovery Plan, related to the unique circumstances of a ransomware attack;
2. updated the Plan regularly, as required by the *Ransomware Guide* and Ransomware Playbook according to the *CISA #StopRansomware Guide*; and
3. documented corrective action plans based on findings in the Agency's biannual tabletop exercise.

Additionally, Ernst & Young issued findings to SSA as part of the FY2023 *Federal Information Security Modernization Act of 2014* (FISMA)[7] performance audit that related to the Ransomware audit objective. These findings and recommendations were provided to management as part of the FISMA audit through an issued Notice for Finding and Recommendations.

RECOMMENDATIONS

Ernst & Young provided six recommendations to address the identified findings related to SSA's Ransomware Prevention and Response Strategy. Ernst & Young transmitted the recommendations to SSA management under separate cover.

[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.

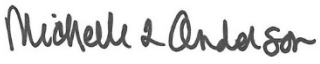
[7] *Federal Information Security Management Act of 2014*, Pub. L. No. 113-283, § 2, 128 Stat. 3073, 3075-3078 (2014).

THE OFFICE OF THE INSPECTOR GENERAL'S COMMENTS

SSA maintains sensitive information about each person who has been issued a Social Security number. The Agency should ensure its Ransomware Prevention and Response Strategy follows all federal guidelines to protect the Agency's sensitive data.

AGENCY COMMENTS

SSA responded to Ernst & Young's recommendations under separate cover. See Appendix B for the full text of the Agency's response to the audit summary.



Michelle L. Anderson
Assistant Inspector General for Audit

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

Scope

The purpose of the Ransomware Response and Prevention performance audit was to assess the Social Security Administration's (SSA) overall ransomware prevention and response controls and strategy based on audit standards and criteria including, but not limited to:

- Federal Risk and Authorization Management Program:
  - *Security Assessment Framework*, Version 2.1 (December 2015);
  - *High, Moderate, Low, Baseline security Plan* template (June 2023);
  - *Continuous Monitoring Performance Management Guide*, Version 3.0 (August 2023).
- Government Accountability Office's (GAO), *Federal Information System Controls Audit Manual* (February 2009).
- GAO, *Government Auditing Standards*, GAO-21-368G, Chapters 8 and 9 (April 2021).
- FY 2023 – 2024 Inspector General *Federal Information Security Modernization Act of 2014* Fiscal Year Reporting Metrics.[1]
- Cybersecurity & Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC), *Ransomware Guide* (2020.)
- National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 5.
- NIST, *Ransomware Risk Management: A Cybersecurity Framework Profile*, NIST Interagency or Internal Report 8374 (February 2022).
- 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).
- SSA guidance and policies.

Methodology

Ernst & Young evaluated SSA's ransomware prevention and response strategy in accordance with specified objectives mapped to the NIST Cybersecurity Framework:[2]

- **Identify**
  - **Security Management (Governance) Ransomware Role and Responsibilities**: Determine the roles and responsibilities for SSA Office of Information Security, Chief Information Officer, Office of Operations, and/or other components as applicable.

- **Security Management (Governance) Ransomware Risk Assessment Processes**: Assess Risk Assessment, Business Impact Assessment, and/or Other Strategy, Evaluations, and Supporting Documentation.

- **Protect**
  - **Test of Ransomware Detective and Preventive Controls**: Determine the effectiveness of SSA Ransomware Detective and Preventive Controls.
  - **Security Awareness and Training**: Determine the effectiveness of SSA Security Awareness and Training Controls related to Ransomware.
- **Detect/Respond/Recover**
  - **Contingency Planning and Recovery Strategy and Capability**: Determine the effectiveness of SSA Contingency Planning and Recovery Strategy and Capability related to Ransomware.
  - **Secure and Segregated Backups**: Determine the effectiveness of SSA Secure and Segregated Backup Controls related to Ransomware.

To accomplish its objectives, Ernst & Young performed the procedures outlined in our Statement of Work's Planned Scope and Methodology section.[3] This included using Federal guidance to:

- assess SSA's ransomware risk management plan and strategy, including such security management tasks as reviewing the Agency's governance and oversight structure; assessing ransomware risk, business impact, and strategy; reviewing any plans or actions to address identified risks and Federal ransomware guidance; and assessing any crisis management actionable plans/strategy for responding to ransomware attacks;
- assess and test SSA's ransomware detective and preventive controls using the *Ransomware Guide* and assess SSA's use of threat intelligence, phishing exercises, firewall rules and its network segmentation, and security awareness and training; and
- determine whether SSA had secure and segregated backups and assess SSA's contingency planning and recovery strategy and capability.

To the extent possible, Ernst & Young leveraged the audit work it performed for *The Social Security Administration's Information Security Program and Practices for Fiscal Year 2023* (142306); *The Social Security Administration's Financial Reporting for Fiscal Year 2023* (152308); *Security of the Earnings Record Maintenance Cloud System* (142310); and *Security of the Web Identification, Authentication, and Access Control System* (142311).

[1] Office of Management and Budget, Office of the Federal Chief Information Officer, *FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.*

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

[3] Contract Number: GS-00F-290CA, Task Order Number 28321323FDX030009, Section 5.3.

Ernst & Young stated it 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 our audit objectives. Ernst & Young believes that the evidence obtained provides a reasonable basis for our findings and conclusions based on its audit objectives.

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 Summary Report, "The Social Security Administration's FY 2023 Ransomware Prevention and Response Performance" (142309)—INFORMATION

Thank you for the opportunity to review the draft report. Protecting our networks and the information we use to administer our programs are critical priorities for us. We continuously improve our cybersecurity controls. We are pleased that we were recognized as one of the most improved agencies on the recent Federal Information Technology Acquisition Reform Act cybersecurity scorecard.

Please let me know if I can be of further assistance. You may direct staff inquiries to Trae Sommer at (410) 965-9102.

Attachment

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:

Twitter: @TheSSAOIG

Facebook: OIGSSA

YouTube: TheSSAOIG

Subscribe to email updates on our website.