OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Report

The Social Security Administration's Vulnerability Management Program

CONTAINS REDACTED INFORMATION

A-14-18-50585 | October 2019

OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: October 24, 2019 Refer To:

To: The Commissioner

From: Inspector General

Subject: The Social Security Administration’s Vulnerability Management Program (A-14-18-50585)

CONTAINS REDACTED INFORMATION

The attached final report presents the results of the Office of Audit’s review. The objective was to determine whether the Social Security Administration had effectively addressed known systems vulnerabilities.

If you wish to discuss the final report, please call me or have your staff contact Rona Lawson, Assistant Inspector General for Audit, at 410-965-9700.

Gail S. Ennis

Gail S. Ennis

Attachment

CONTAINS REDACTED INFORMATION

The Social Security Administration's Vulnerability Management Program A-14-18-50585

October 2019 **Office of Audit Report Summary**

Objective

To determine whether the Social Security Administration (SSA) had effectively addressed known systems vulnerabilities.

Background

In computer security, a vulnerability is a weakness that can be exploited (for example, by an attacker) to perform unauthorized actions in a computer system.

Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. Auditors have identified vulnerability and patch management as components of a significant deficiency in SSA's information technology controls.

We evaluated the vulnerability management process on all the devices connected to the Agency's network. To accomplish our objective, we selected scan results to determine whether SSA remediated vulnerabilities timely.

Findings

SSA needs to more effectively address known systems vulnerabilities.

Although timely vulnerability management poses challenges, SSA must overcome these challenges to protect its systems and its ability to serve the public.

Recommendations

SSA agreed with our recommendations.

CONTAINS REDACTED INFORMATION

TABLE OF CONTENTS

ABBREVIATIONS

DHS	Department of Homeland Security
FY	Fiscal Year
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
SSA	Social Security Administration

OBJECTIVE

Our objective was to determine whether the Social Security Administration (SSA) had effectively addressed known systems vulnerabilities.

BACKGROUND

The security of Federal information technology systems and data is vital to public confidence as well as national security, prosperity, and well-being. The risks to information technology systems that support the Government are increasing, including insider threats from employees acting with intent or unwitting employees, escalating and emerging worldwide threats, and/or the emergence of new and more destructive attacks. In Fiscal Year (FY) 2018, Federal agencies reported over 31,000 information security incidents.[1]

In computer security, a vulnerability is a weakness that can be exploited (for example, by an attacker) to perform unauthorized actions in a computer system. Known, but unmitigated, vulnerabilities are among the highest cyber-security risks agencies face. According to the Department of Homeland Security (DHS), the average time between a vulnerability's discovery and exploitation is decreasing as today's adversaries are more skilled, persistent, and able to exploit known vulnerabilities.[2]

Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. This includes patch management,[3] an important element in mitigating the risks associated with known vulnerabilities and maintaining the confidentiality, integrity, and availability of information systems. Vulnerabilities are classified by their severity, defined by the National Institute of Standards and Technology (NIST).[4] Auditors have identified

[1] Government Accountability Office*, Agencies and [the Office of Management and Budget] Need to Strengthen Policies and Practices, No. GAO-19-545,* p. 6 (2019).

[2] DHS, *Vulnerability Remediation Requirements for Internet-Accessible Systems, Binding Operational Directive 19-02,* p. 1 (April 29, 2019).

[3] Patches correct security and functionality problems in software. NIST, *Guide to Enterprise Patch Management Technologies, SP 800-40 Rev 3*, p. iii (July 2013).

[4] NIST, *National Vulnerability Database: Vulnerability Metrics*, nvd nist.gov (last visited August 6, 2019).

vulnerability and patch management as components of a significant deficiency in SSA's information systems controls.[5] We also reviewed SSA's patch management process in 2014.[6]

Vulnerability Management Requirements

The *Federal Information Security Modernization Act of 2014* requires that each agency develop, document, and implement a program to secure its information and information systems.[7] According to DHS, effective information security programs include timely remediation of vulnerabilities.[8] DHS sends SSA weekly Cyber Hygiene reports to help secure Internet-facing systems from weak configuration and known vulnerabilities. The Cyber Hygiene reports we reviewed for this audit did not identify any critical or high-risk vulnerabilities[9] on SSA's Internet-facing systems. In 2015, DHS began requiring that agencies mitigate critical vulnerabilities identified in the weekly Cyber Hygiene reports within 30 days.[10] However, in April 2019, DHS issued new guidance that requires mitigation of critical vulnerabilities within 15 days and high-risk vulnerabilities within 30 days.[11] Further, NIST indicates that organizations should correct information system vulnerabilities and install security-relevant updates within an organizationally defined time period.[12]

[5] Annual financial statement and *Federal Information Security Modernization Act of 2014* audits have consistently identified significant deficiencies in information systems controls. See SSA, *Agency Financial Report, Fiscal Year 2017*, pp. 98 and 99 (2017); SSA, *Agency Financial Report, Fiscal Year 2016*, pp. 108 and 109 (2016); SSA, *Agency Financial Report, Fiscal Year 2015*, p. 108 (2015). For FY 2018, Grant Thornton identified patch management and network security deficiencies that were included in the Network Security Controls portion of the significant deficiency. SSA, *Agency Financial Report, Fiscal Year 2018*, p. 109 (2018).

[6] SSA, OIG, *Effectiveness of the Social Security Administration's Server Patch Management Process, A-14-14-14043* (September 2014). In response to this review, the Agency stated it "… should acquire additional resources to mature its process to include more prompt updates to all software on all devices to remediate all vulnerabilities." SSA, Office of Systems, Office of Information Security, updated response to the recommendation in this report provided in September 2016.

[7] *Federal Information Security Modernization Act of 2014,* Pub. L. No. 113-283, § 3554(b), 128 Stat. 3073, p. 3079 (2014).

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

[9] The vulnerability rating classifications are used in the Common Vulnerability Scoring System, designed to provide a universally open and standardized method for rating information technology vulnerabilities. A numerical score, determined by a variety of factors, is derived and the severity rating (low, medium, high, critical) corresponds to these numerical scores. See NIST, *National Vulnerability Database: Vulnerability Metrics*, nvd nist.gov (last visited August 6, 2019).

[10] DHS, *Critical Vulnerability Mitigation Requirements for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems Binding Operational Directive* 15-01, p. 3 (May 21, 2015).

[11] DHS, *Vulnerability Remediation Requirements for Internet-Accessible Systems, Binding Operational Directive,* 19-02, p. 3 (April 29, 2019).

[12] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations, SP 800-53 Rev. 4*, p. F-216 (April 2013).

SSA's Vulnerability Scanning

[redacted]

Scope and Methodology

We reviewed select fields from SSA's vulnerability scan results for [redacted]. We analyzed the occurrences of critical and high-rated plugin[13] identifications known to be exploitable. Plugins indicate whether specific vulnerabilities are present. For our analysis, we considered a plugin identification to be one vulnerability. However, a plugin may include more than one vulnerability, and each vulnerability may have a different severity rating based on the Common Vulnerability Scoring System standard SSA uses. The Common Vulnerability Scoring System produces numerical severity scores for vulnerabilities that can be translated as low, medium, high, or critical to help organizations properly assess and prioritize their vulnerability management processes.[14] Because plugins can include more than one vulnerability, the severity rating the scanning tool provides may differ from SSA's assessment of severity. We also analyzed the scan results to identify unauthorized software installed on Agency devices. See Appendix A for additional information about our scope and methodology.

RESULTS OF REVIEW

SSA needs to more effectively address known systems vulnerabilities. [redacted]

[redacted]

[13] In the context of a vulnerability scanner, a plugin is a program that detects new vulnerabilities. It contains vulnerability information, a set of remediation actions, and a way of testing for a security issue. Tenable, *Plugins*, tenable.com (last visited July 15, 2019).

[14] See Footnote 9.

Critical and High-risk Vulnerabilities

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]			
	[redacted]		[redacted]	
	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

Unauthorized Software

Unauthorized software may be unmanaged and introduce vulnerabilities that attackers can use to compromise systems. SSA documented its managed, authorized software and established a process for users to request exceptions if business needs require the use of other software. If the Agency considers the security risk acceptable and approves an exception, the requestor must manage the software, keeping it patched and updated.

SSA's security tool generates a list of all software installed on the Agency's network. SSA manually classifies and removes known, authorized software from the list. The Agency will either remediate remaining software or work with end users to obtain exceptions where appropriate.

[redacted]

CONTAINS REDACTED INFORMATION

[redacted]

[redacted]

CONCLUSIONS

SSA needs to more effectively address known systems vulnerabilities. [redacted]

[redacted]

[redacted]

[redacted]

RECOMMENDATIONS

We recommend that SSA:

[redacted]

[redacted]

AGENCY COMMENTS

SSA agreed with our recommendations. The Agency's comments are included in Appendix B.

Rona Lawson

Rona Lawson
Assistant Inspector General for Audit

CONTAINS REDACTED INFORMATION

APPENDICES

Appendix A – Scope and Methodology

Our objective was to determine whether the Social Security Administration (SSA) had effectively addressed known systems vulnerabilities. To accomplish our objective, we:

- Reviewed applicable Federal laws[1] and related guidance for vulnerability management, including the following.
    - Department of Homeland Security, *Binding Operational Directive BOD-19-02*, April 29, 2019.
    - Office of Management and Budget Memorandum, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*, October 30, 2015.
- Reviewed SSA's policies and procedures pertaining to the Agency's Vulnerability Management Program, including the following.
    - SSA Information Security Policy.
    - SSA Vulnerability Management Policy and Procedures.
- Reviewed various National Institute of Standards and Technology publications.
- Interviewed SSA staff from the Office of Information Security.
- Obtained and reviewed documentation including the following.
    - [redacted]
    - [redacted]

[redacted]

[1] *Federal Information Security Modernization Act of 2014*, Pub. L. No. 113-283, 128 Stat. 3073 (2014).

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

We conducted our audit at SSA Headquarters in Baltimore, Maryland, [redacted] [redacted] The principal entity reviewed was the Office of Information Security under the Office of the Deputy Commissioner for Systems. We determined the data used were sufficiently reliable given the audit objective and intended use of the data. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix B – AGENCY COMMENTS

SOCIAL SECURITY

MEMORANDUM

Date: October 10, 2019 Refer To: S1J-3

To: Gail S. Ennis
Inspector General

Stephanie Hall

From: Stephanie Hall
Deputy Chief of Staff

Subject: Office of the Inspector General Draft Report, "The Social Security Administration’s Vulnerability Management Program" (A-14-18-50585) -- INFORMATION

Thank you for the opportunity to review the draft report; we agree with both recommendations. [redacted]

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

Mission

By conducting independent and objective audits, evaluations, and investigations, the Office of the Inspector General (OIG) inspires public confidence in the integrity and security of the Social Security Administration's (SSA) programs and operations and protects them against fraud, waste, and abuse. We provide timely, useful, and reliable information and advice to Administration officials, Congress, and the public.

Connect with Us

The OIG Website (https://oig.ssa.gov/) gives you access to a wealth of information about OIG. On our Website, you can report fraud as well as find the following.

- OIG news
- audit reports
- investigative summaries
- Semiannual Reports to Congress
- fraud advisories
- press releases
- congressional testimony
- an interactive blog, "Beyond The Numbers" where we welcome your comments

In addition, we provide these avenues of communication through our social media channels.

Watch us on YouTube

Like us on Facebook

Follow us on Twitter

Subscribe to our RSS feeds or email updates

Obtain Copies of Audit Reports

To obtain copies of our reports, visit our Website at https://oig.ssa.gov/audits-and-investigations/audit-reports/all. For notification of newly released reports, sign up for e-updates at https://oig.ssa.gov/e-updates.

Report Fraud, Waste, and Abuse

To report fraud, waste, and abuse, contact the Office of the Inspector General via

Website: https://oig.ssa.gov/report-fraud-waste-or-abuse

Mail: Social Security Fraud Hotline
P.O. Box 17785
Baltimore, Maryland 21235

FAX: 410-597-0118

Telephone: 1-800-269-0271 from 10:00 a.m. to 4:00 p.m. Eastern Standard Time

TTY: 1-866-501-2101 for the deaf or hard of hearing