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*

CONTAINS REDACTED INFORMATION

# 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 |

## 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]

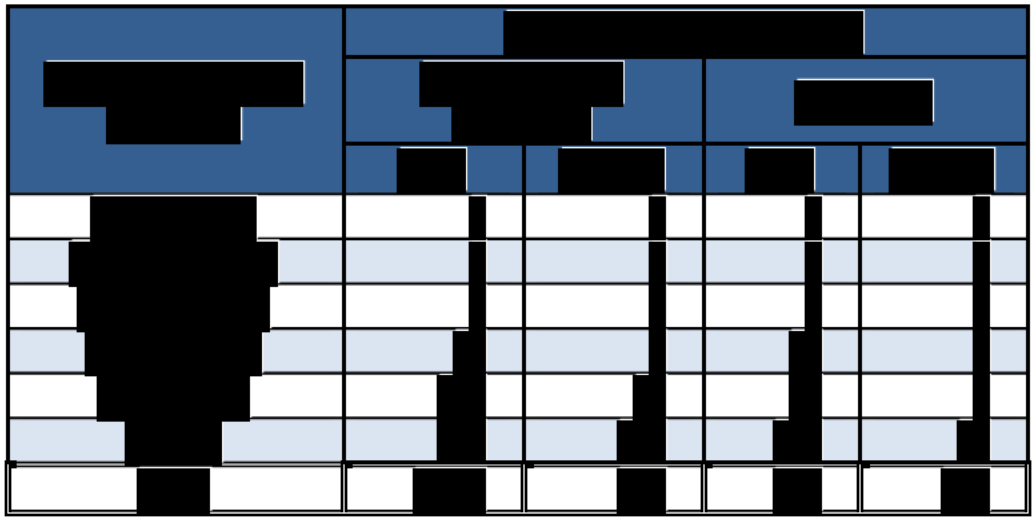
[13] In the context of a vulnerability scanner, a plugin is a program that detects new vulnerabilities. It contains vulnerability information, a set of remediation actions, and a way of testing for a security issue. Tenable, *Plugins*, tenable.com (last visited July 15, 2019).

[14] See Footnote 9.

## Critical and High-risk Vulnerabilities

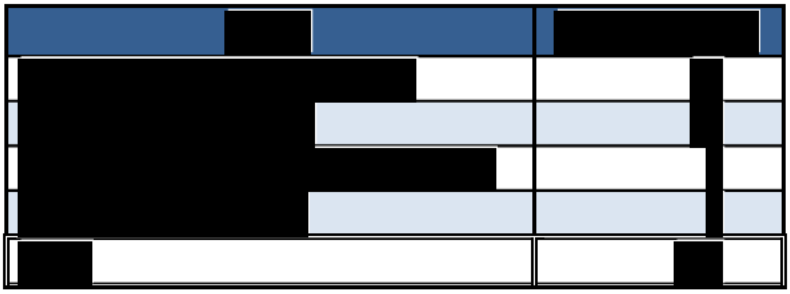
[redacted]

[redacted]



[redacted]

[redacted]



[redacted]

---

[redacted]

[redacted]

## 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]

[redacted]

[redacted]

## CONCLUSIONS

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

[redacted]

[redacted]

[redacted]

CONTAINS REDACTED INFORMATION

## RECOMMENDATIONS

We recommend that SSA:

[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

# Appendix A – Scope and Methodology

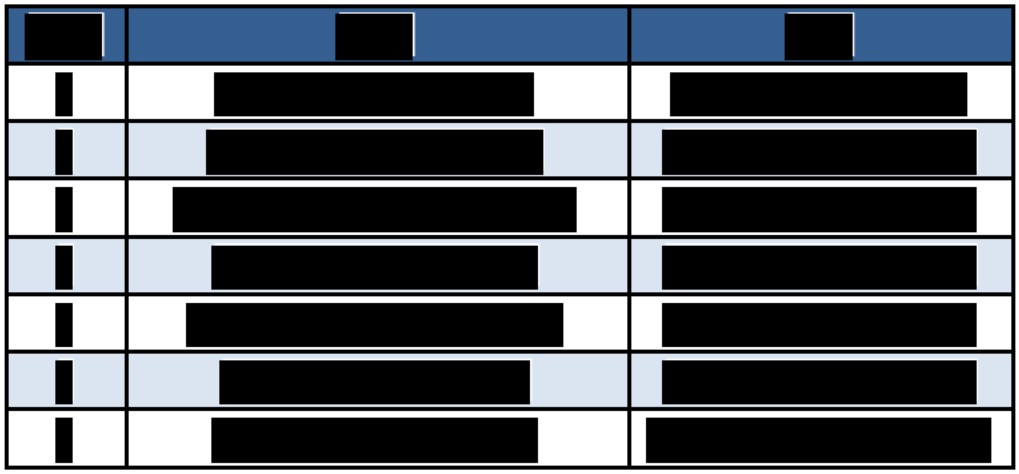
Our objective was to determine whether the Social Security Administration (SSA) had effectively addressed known systems vulnerabilities. To accomplish our objective, we:

- 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]

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

[redacted]



[redacted]

We conducted our audit at SSA Headquarters in Baltimore, Maryland, [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.

**CONTAINS REDACTED INFORMATION**

# 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.