LIMITED DISTRIBUTION

Security of the Social Security Administration's Public Web Applications A-14-17-50152

SOCIAL SECURITY ADMINISTRATION OIG

April 2017 **Office of Audit Report Summary**

Objective

To determine the effectiveness of the Social Security Administration's (SSA) efforts to identify, assess, and remediate vulnerabilities in the Agency's publicly accessible Web applications.

Background

SSA manages a number of Web applications to transact business with the public, government agencies, and others. Because hackers attempt to exploit vulnerabilities to gain unauthorized access to networks, it is imperative that SSA identify any vulnerabilities in its publicly accessible Web applications and remediate them timely to protect the Agency's sensitive information.

As part of a Council of the Inspectors General on Integrity and Efficiency (CIGIE) Information Technology Subcommittee's crosscutting project, SSA's Office of the Inspector General (OIG) joined other OIGs to conduct a Government-wide review of publicly accessible Web applications and associated security controls. Each OIG that participated in the project assessed its own agency's Web application program, allowing CIGIE to then develop Government-wide recommendations and best practices to secure and manage Web applications.

Findings

Opportunities existed for SSA to strengthen its controls over identifying, assessing, and remediating vulnerabilities in its publicly accessible Web applications.

We reviewed the results of SSA and the Department of Homeland Security's (DHS) scans—as well as a contractor-performed scan—for 1 week in June 2016. Collectively, those scans identified 39 vulnerabilities in SSA's publicly accessible systems. Although SSA was tracking remediation efforts for vulnerabilities it identified in its own scans, the Agency was not effectively tracking vulnerabilities that DHS or the contractor identified. In November 2016, SSA began tracking all vulnerabilities identified in one application that triggers automatic notification to the appropriate systems owner.

In January 2017, SSA reported it had remediated six vulnerabilities. In addition, SSA accepted the risk, and did not remediate, four vulnerabilities. The Agency concluded the remaining 29 were false positives and did not represent true vulnerabilities. According to DHS, if an agency believes a reported vulnerability is in error, it can submit a false positive assertion. DHS will review the evidence and conduct its own analysis.

Because DHS analyzes the results of its scans to evaluate the state of the nation's cybersecurity posture, it is important that agencies report false positives to ensure DHS has accurate data. SSA reported it contacted DHS about the false positives in January 2017.

Recommendation

We recommend that SSA ensure all vulnerabilities identified through scanning activities are assessed, tracked, and remediated or otherwise resolved timely.

SSA agreed with our recommendation.