The Social Security Administration's Controls over Malicious Software and Data Exfiltration
A-14-18-50709

December 2019 **Report Summary**

Objective

Our objective was to determine the effectiveness of the Social Security Administration's (SSA) incident response and continuous monitoring programs in identifying, logging, analyzing, blocking, containing, and reporting malicious activity and data exfiltration attempts.

Background

In conjunction with the SSA Financial Statement Audit and *Federal Information Security Modernization Act of 2014* Performance Audit, the OIG engaged Grant Thornton to conduct two performance audits for testing controls over reporting malicious activity, data exfiltration attempts, and command-and-control payloads. SSA maintains an Information Security Policy that outlines approved network use. Violation of this policy would be considered a security incident and may indicate malicious activity. Malicious activity can be presented in many forms including phishing emails; downloaded malware; and data exfiltration over the Web, by email, or by removable media. SSA used incident response and reporting processes to detect, investigate, and respond to potential malicious activity in order to reduce risks to the confidentiality, availability, or integrity of Agency data and information.

Findings

Although SSA established policies, procedures and technical controls to identify and respond to malicious software and data exfiltration across the Agency, as required by the *Federal Information Security Modernization Act of 2014*, Office of Management and Budget policy, and National Institute of Standards and Technology standards and guidelines, we identified a number of control weaknesses related to Preventing Malicious Activity, Detecting Malicious Activity, and Responding to Malicious Activity.

During our testing, we held an incident response tabletop exercise with Agency personnel to discuss opportunities to improve SSA's incident response and continuous monitoring programs. Continuing to perform simulated testing exercises could assist SSA to refine specific process weaknesses identified in our testing exercises and stay current as threats evolve.

Recommendations

Based on the procedures performed, we noted that certain controls related to our audit objective were not designed or operating effectively. While policies, procedures, and practices were in place, we noted instances where controls were not designed or operating as intended, which could lead to security weaknesses on the Agency network and/or devices resulting in the loss of sensitive data. Without appropriate security, SSA may not be able to protect its mission assets adequately. Additionally, some deficiencies we identified could negatively affect the confidentiality, integrity, and availability of the Agency's systems and personally identifiable information.

Although SSA officials generally agreed with the individual findings, there was disagreement with two of our nine recommendations. Please see the Agency's response in Appendix A. Management's response does not impact the results, findings, and conclusion of our audit.