CONTAINS RESTRICTED INFORMATION

Grant Thornton

The Social Security Administration's Controls over Malware Introduced by Email Phishing
A-14-18-50710

December 2019 **Report Summary**

Objective

The objective was to determine the effectiveness of Social Security Administration's (SSA) incident response and continuous monitoring programs in identifying, logging, analyzing, blocking, containing, and reporting command-and-control payload delivery attempts.

Background

In conjunction with the SSA Financial Statement Audit and *Federal Information Security Modernization Act of 2014* Performance Audit, the SSA Office of Inspector General has engaged Grant Thornton to conduct two performance audits for testing controls over reporting malicious activity, data exfiltration attempts, and command-and-control payload. Responding to computer security incidents has become an important component of information technology programs. Cyber-attacks have become more numerous, diverse, damaging and disruptive. New types of security-related incidents emerge frequently. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring information technology services.

Findings

SSA established policies, procedures and technical controls to identify, log, analyze, block, contain, and report on command-and-control payload delivery and other data exfiltration attempts as required by FISMA, Office of Management and Budget policy and guidelines, and National Institute of Standards and Technology standards and guidelines. However, we identified a number of control weaknesses related to preventing and detecting malicious activity.

Recommendations

SSA has continued implementing solutions to identify and respond to threats and malicious activity on the SSA enterprise network that could result from an email phishing attack. SSA should continue implementing additional corrective actions that address the root causes of findings documented in this report as well as similar previous reports and assessments provided to the Agency.

Based on the audit procedures performed, we noted that controls related to our audit objective were not designed or operating effectively. While policies and procedures were in place, we noted instances where controls were not designed or implemented 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-critical assets adequately. Additionally, some deficiencies could negatively affect the confidentiality, integrity, and availability of the Agency's systems and personally identifiable information.

SSA officials agreed with the recommendations and are taking immediate action to address the audit findings. Please see Agency's response in Appendix A. Management's response does not impact the results, findings, and conclusion of our audit.