Security of the Social Security Administration's Disability Case Processing System
A-14-20-50896

November 2020 **Report Summary**

Objective

Under a contract we monitored, Grant Thornton LLP (Grant Thornton), an independent certified public accounting firm, conducted an audit to determine the effectiveness of selected information security controls for the Social Security Administration's (SSA) Disability Case Processing System (DCPS). Testing also provided support for Grant Thornton's overall Fiscal Year 2020 *Federal Information Security Modernization Act of 2014* (FISMA) performance audit.[1]

Background

SSA developed DCPS, a cloud-based application, to replace five legacy case processing systems used by State disability determination services (DDS). Historically, each of the 52 DDSs maintained their own case processing system. SSA stated, "DCPS will replace the outdated legacy systems with a modern, scalable and secure application capable of providing the flexibility and high performance that the DDSs and Federal sites need to process disability claims timely and efficiently."[2] As of September 2020, 45 of the 52 DDSs were using DCPS in some capacity to process disability claims, and 6 DDSs have transitioned exclusively to DCPS for processing of new cases.

Grant Thornton's Scope and Methodology

Grant Thornton performed testing over the DCPS application and cloud infrastructure in the following areas.

- Security Management;
- Access Controls;
- Audit Logging and Monitoring;
- Change and Configuration Management;
- Disaster Recovery;
- Incident Response; and
- Cloud Computing Controls.

---

[1] Grant Thornton's audit report contains information that, if not protected, could result in adverse effects to the Agency's information systems. In accordance with government auditing standards, we have transmitted Grant Thornton's report to SSA executives and excluded from this publicly available summary certain sensitive information because of the potential damage that could result if the information is misused. We have determined the omitted information does not distort the audit results described in this summary nor conceal improper or illegal practices. Government Accountability Office, *Government Auditing Standards*, GAO-18-568G, pp. 208 through 210, paras. 9.61 through 9.67, (July 2018).

[2] SSA, Disability Case Processing System (DCPS): About DCPS, SSA DCPS Intranet site (last visited May 1, 2020).

The firm reviewed security controls responsibilities between the cloud service provider, SSA cloud infrastructure team, DCPS development and maintenance team, and individual DDS sites and tested appropriate SSA controls at each level of the hierarchy. Grant Thornton performed its security testing within the "Acceptance Testing Environment,"[3] which mimics[4] the live version in production.

Grant Thornton focused its audit approach on Federal information security guidance developed by the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) as well as the Federal Risk and Authorization Management Program (FedRAMP), developed by General Services Administration's FedRAMP Project Management Office. NIST Special Publications provide guidelines that are considered essential to the development and implementation of agencies' security programs.

Grant Thornton conducted its audit at SSA Headquarters in Baltimore, Maryland, from October 2019 through March 2020. Additionally, Grant Thornton performed testing on site at one State DDS from February 4 through February 6, 2020.

Office of the Inspector General's Evaluation of Grant Thornton's Performance

We monitored Grant Thornton's performance by

- reviewing Grant Thornton's audit approach and planning;
- evaluating Grant Thornton's auditors' qualifications and independence;
- monitoring the audit progress;
- examining Grant Thornton's working papers;
- reviewing Grant Thornton's report to ensure it complies with *Government Auditing Standards*;
- coordinating the issuance of the audit report; and
- performing other procedures as deemed necessary.

Grant Thornton is responsible for the attached auditor's report and the conclusions expressed therein. The Office of the Inspector General was responsible for technical and administrative oversight regarding Grant Thornton's performance under the contract terms. We did not conduct oversight of Grant Thornton's audit in accordance with generally accepted government auditing standards. Our oversight activities were not intended to enable us to express, and, accordingly, we do not express, an opinion about the effectiveness of SSA's information security policies, procedures, and practices. However, our monitoring review, as qualified above, disclosed no instances where Grant Thornton did not comply with applicable auditing standards.

[3] The final environment in the change management process before software changes are moved to production. This environment allows users to interact with a production-like setup to determine whether changes have been developed appropriately before that change is implemented into production.

[4] This allowed Grant Thornton to perform testing without interfering with real or live claims processing.

Results of Grant Thornton's Review

Although SSA established information security controls for DCPS, as required by FISMA, OMB policy and guidelines, FedRAMP requirements, and NIST guidelines, Grant Thornton identified a number of deficiencies, in design and operating effectiveness, in information security controls specific to the DCPS application. Following are examples of some of the deficiencies Grant Thornton identified.

Access Controls

- Specific aspects of an access control were not required or performed
- Sampled users were not reviewed as part of SSA's agencywide process.
- In certain instances, the Agency was unable to provide evidence that staff followed defined controls.

Audit Logging and Monitoring

- The DCPS Audit Plan had not been updated in accordance with plan requirements. Additionally, SSA did not share audit logs with all responsible parties.

Separation of Duties

- SSA had not clearly defined or documented how separation of duties was enforced for a specific process.

Risk Management

- Documentation related to DCPS security had not been reviewed and updated in accordance with Agency policy. Additionally, Grant Thornton identified aspects of documentation that were incomplete, inaccurate, or inconsistent.

Additionally, Grant Thornton identified weaknesses during its testing of Application Security, Cloud Infrastructure Security, and Contingency Planning.

Grant Thornton's Conclusions

Based on the procedures performed, Grant Thornton noted information security controls for DCPS were, at times, not designed or operating effectively. While policies and procedures were in place, Grant Thornton noted instances where they were not consistent with the current controls in place as well as 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.

Grant Thornton's Recommendations to SSA

As SSA continues transitioning from legacy case processing systems to DCPS, Grant Thornton recommended SSA develop specific policy and procedures outlining control requirements, activities, and processes for DCPS so controls are designed and implemented consistently. Additionally, as SSA continues modernizing its systems, management should continue improving the cyber-security posture to minimize risk to Agency data. Grant Thornton provided SSA with 11 recommendations to address the specific issues identified during the audit.

Agency Comments

SSA management generally agreed with Grant Thornton's findings. Grant Thornton determined management's response does not impact the audit's results, findings, and conclusion.