Report in Brief
Date: March 2024
Report No. A-18-22-08020

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL

Administration for Children and Families Data Hosted in Certain Cloud Information Systems May Be at a High Risk of Compromise

Why OIG Did This Audit

This audit is one in a series of audits that will examine whether HHS and its Operating Divisions have implemented effective cybersecurity controls for cloud information systems in accordance with Federal security requirements and guidelines.

Our objectives were to determine whether the Administration for Children and Families (ACF) (1) accurately identified and inventoried its cloud computing components and (2) implemented security controls in accordance with Federal requirements and guidelines.

How OIG Did This Audit

We reviewed ACF's cloud inventory and its policies and procedures. We also analyzed the configuration settings of ACF vulnerability scanners. We performed external, internal, and web application penetration testing of selected cloud information systems from April through May 2022. We also conducted two simulated phishing campaigns that included a limited number of ACF personnel during this period. We contracted with Breakpoint Labs, LLC (BPL), to conduct the penetration test on OIG's behalf. We closely oversaw the work performed by BPL, and the assessment was performed in accordance with agreed upon Rules of Engagement.

What OIG Found

ACF did not accurately identify and inventory all of its cloud computing assets. Also, although ACF had implemented some security controls to protect its cloud information systems, it did not effectively implement several other security controls to protect its cloud information systems in accordance with Federal requirements and guidelines. This occurred because ACF did not establish policies and procedures to inventory and monitor cloud information system components. Also, ACF did not perform adequate cloud and web application technical testing techniques against its systems to proactively identify the vulnerabilities we discovered. As a result, ACF data hosted in certain systems may potentially be at a high risk of compromise.

What OIG Recommends and ACF Comments

We made a series of recommendations to ACF to improve its security controls over cloud information systems, including that it update and maintain a complete and accurate inventory, remediate the 19 security control findings identified in our report, and leverage cloud security assessment tools to identify misconfigurations and weak cybersecurity controls in its cloud infrastructure.

In written comments on our draft report, ACF concurred with our recommendations and described the actions it has taken or plans to take to address them, including (1) tracking its inventory in a new Governance, Risk, and Compliance system; (2) crafting steps for staff to effectively implement cloud security baselines; and (3) leveraging HHS Department-level penetration testing services to give ACF real-time visibility into exploitable vulnerabilities across a variety of assets. Although we have not yet confirmed whether ACF effectively implemented our recommendations, we are encouraged by ACF's response and we look forward to receiving and reviewing the supporting documentation through our audit resolution process.

The full report can be found on the OIG website.