Report in Brief
Date: July 2024
Report No. A-18-22-08018

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

Why OIG Did This Audit

This audit is one in a series of audits that will examine whether HHS and its operating divisions (OpDivs) have implemented effective cybersecurity controls for cloud information systems owned, operated, or maintained by HHS or its contractors in accordance with Federal security requirements and guidelines.

Our objectives were to determine whether the HHS Office of the Secretary (HHS OS) (1) accurately identified and inventoried its cloud information systems and components and (2) implemented security controls in accordance with Federal requirements and guidelines.

How OIG Did This Audit

We reviewed HHS OS's cloud information system inventory and its policies and procedures. We also analyzed the configuration settings of HHS OS's cloud environment using both a network vulnerability scanner and a cloud security assessment tool. Also, we performed penetration testing of selected cloud information systems in June and July 2022. We also conducted two email phishing campaigns that included a limited number of HHS OS personnel and cloud component users during this period. We contracted with Breakpoint Labs, LLC (BPL), to conduct the penetration test of HHS OS. We closely oversaw the work performed by BPL, and the assessment was performed in accordance with the agreed-upon Rules of Engagement document.

HHS Office of the Secretary Needs to Improve Key Security Controls to Better Protect Certain Cloud Information Systems

What OIG Found

HHS OS accurately identified the components within the cloud systems we were able to assess. However, HHS OS did not accurately identify and inventory all of its cloud systems in accordance with HHS security requirements. Also, although HHS OS implemented some security controls to protect its cloud systems, several key security controls were not effectively implemented in accordance with Federal requirements and guidelines. This occurred because certain HHS OS system owners and System Security Officers did not identify some of their information systems as cloud systems in accordance with HHS requirements. Also, HHS OS System Security Officers–most often assigned by business or system owners–do not always have the skill sets or experience necessary to adequately perform the roles and responsibilities for the job function as defined by NIST. Although System Security Officer roles and responsibilities are defined in HHS security policies, there is no standardized process for ensuring qualified System Security Officers are selected. This adversely effects HHS OS's ability to ensure security controls are effectively implemented. As a result, HHS OS data stored in the cloud systems we examined may potentially be at a risk of compromise.

What OIG Recommends and HHS Office of the Secretary Comments

We made a series of recommendations for HHS OS to improve key security controls over cloud information systems, including that it implement a strategy that includes leveraging cloud security assessment tools that identify misconfigurations and other control weaknesses in its cloud services, and develop and implement a policy and process to ensure qualified staff areassigned as System Security Officers for its cloud systems.

In written comments on our draft report, HHS OS concurred with our recommendations and indicated that it would implement them.

The full report can be found on the OIG website.