Report in Brief
Date: February 2023
Report No. A-18-20-08200

U.S. Department of Health & Human Services
Office of Inspector General

The Health Resources and Services Administration Should Improve Preventive and Detective Controls To More Effectively Mitigate the Risk of Compromise

Why OIG Did This Audit

We conducted a cyber threat hunt assessment of the Health Resources and Services Administration's (HRSA's) information systems to independently assess the effectiveness of HRSA's cybersecurity defenses, conducted an intrusion analysis, and reviewed its incident response capabilities.

Our objectives were to determine whether: (1) HRSA's cybersecurity defenses were effective, (2) there was an active threat on the HRSA network or whether there had been a past cyber breach, and (3) HRSA was able to detect breaches and respond appropriately.

How OIG Did This Audit

We performed the cyber threat hunt of HRSA's endpoints between June and July 2020. We conducted the assessment on approximately 3,858 endpoints that HRSA manages. We contracted with Accenture Federal Services (AFS) to provide subject matter experts to conduct the cyber threat hunt on OIG's behalf. We closely oversaw the work performed by AFS, and the assessment was performed in accordance with generally accepted government auditing standards and agreed-upon Rules of Engagement among OIG, AFS, and HRSA.

What OIG Found

Although HRSA had implemented some security controls for detecting and preventing threats on its network, HRSA's cybersecurity controls needed improvements to better detect and prevent cyber threats on its network. We found multiple security controls at HRSA that were not operating effectively, including controls related to malicious code protection and protection against unauthorized installation of software by users. Although we did not identify evidence of a past breach, we found three active threats on the HRSA network. We promptly shared these significant findings with HRSA during our audit period. Lastly, we concluded that HRSA was able to detect certain breaches and respond appropriately. We based this conclusion on the fact that HRSA was already in the process of investigating two of the three active threats that we had identified before we notified it of our findings.

The security control failures that we identified occurred because HRSA had not updated security configurations to align with the most current National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security controls and had not implemented procedures to assess and monitor the NIST controls on its endpoints. As a result of HRSA not correctly implementing these controls, these threats could increase the endpoint or network attack surfaces, or bypass current organizational security policies and controls. The likelihood of successful cyberattacks and unauthorized access to sensitive data is greater in environments where these types of security controls are not enforced.

What OIG Recommends and HRSA Comments

We recommend that HRSA: (1) remediate the nine security control findings we identified, (2) update security configurations to align with the most current NIST SP 800-53 security controls, and (3) implement policies and procedures to periodically identify and assess whether security controls are in place and operating effectively in accordance with the most current NIST SP 800-53 and remediate weak controls timely.

In written comments on our draft report, HRSA concurred with our findings and recommendations and described the actions it has taken or plans to take to address them.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/182008200.asp.