December 2024 | A-18-22-07002

Summary Report of Prior Office of Inspector General Cyber Threat Hunt Audits of Eight HHS Operating Division Networks

Why OIG Did This Audit

- Government information systems, especially those managed by the Department of Health and Human Service's (HHS), are under constant threat from cyberattacks.
- Between 2018 and 2020, OIG assessed eight HHS operating divisions (OpDivs) computer networks for: active threats, evidence of undetected cyber breaches, effective cybersecurity defenses, and the ability to detect breaches and respond appropriately.

What OIG Found

Overall, the eight OpDivs lacked adequate protections to mitigate certain cyberattacks.

- We identified 19 threats that had been active on OpDivs' servers and workstations during our audits. We immediately communicated the discoveries to the OpDivs as part of our audit process.
- We identified a total of 138 vulnerabilities related to 19 National Institute of Standards and Technology Special Publication 800-53, Revision 4, controls that were not effectively implemented.
- We did not identify any past cyber breaches of the OpDivs' servers and workstations.

What OIG Recommends

We made three recommendations to the HHS Office of the Chief Information Officer (OCIO), including that it revise and enforce HHS policy to effectively mitigate the risk of compromise.

The OCIO concurred with two of our recommendations and detailed steps it has taken and plans to take to address them. The OCIO did not concur with one recommendation.