Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

HHS OFFICE OF THE SECRETARY SHOULD IMPROVE PREVENTATIVE AND DETECTIVE CONTROLS TO MORE EFFECTIVELY MITIGATE THE RISK OF COMPROMISE

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Amy J. Frontz
Deputy Inspector General
for Audit Services

April 2020
A-18-18-08600

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG) is to provide objective oversight to promote the economy, efficiency, effectiveness, and integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of the people they serve. Established by Public Law No. 95-452, as amended, OIG carries out its mission through audits, investigations, and evaluations conducted by the following operating components:

Office of Audit Services. OAS provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. The audits examine the performance of HHS programs, funding recipients, and contractors in carrying out their respective responsibilities and provide independent assessments of HHS programs and operations to reduce waste, abuse, and mismanagement.

Office of Evaluation and Inspections. OEI's national evaluations provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. To promote impact, OEI reports also provide practical recommendations for improving program operations.

Office of Investigations. OI's criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs and operations often lead to criminal convictions, administrative sanctions, and civil monetary penalties. OI's nationwide network of investigators collaborates with the Department of Justice and other Federal, State, and local law enforcement authorities. OI works with public health entities to minimize adverse patient impacts following enforcement operations. OI also provides security and protection for the Secretary and other senior HHS officials.

Office of Counsel to the Inspector General. OCIG provides legal advice to OIG on HHS programs and OIG's internal operations. The law office also imposes exclusions and civil monetary penalties, monitors Corporate Integrity Agreements, and represents HHS's interests in False Claims Act cases. In addition, OCIG publishes advisory opinions, compliance program guidance documents, fraud alerts, and other resources regarding compliance considerations, the anti-kickback statute, and other OIG enforcement authorities.

Report in Brief
Date: April 2020
Report No. A-18-18-08600

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

HHS Office of the Secretary Should Improve Preventative and Detective Controls to More Effectively Mitigate the Risk of Compromise

Why OIG Did This Audit

We conducted a compromise assessment of the HHS Office of the Secretary's (OS) information systems to independently assess the effectiveness of OS's cybersecurity defenses, as well as intrusion analysis and incident response capabilities.

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

How OIG Did This Audit

We performed the compromise assessment of OS's network, which included endpoints that they manage for certain smaller HHS Operating Divisions (OpDivs) and Staff Divisions. We performed the assessment from November 2018 through January 2019. We contracted with Defense Point Security (DPS) to provide subject matter experts to conduct the compromise assessment on behalf of OIG. We closely oversaw the work performed by DPS and the assessment was performed in accordance with generally accepted government auditing standards and agreed-upon Rules of Engagement between OIG, DPS, and OS.

What OIG Found

We identified seven previously undetected active threats on OS's network. We promptly shared significant findings with OS during the course of the audit and provided detailed documentation about our preliminary findings in advance of issuing our draft report.

As for our second audit objective, based on the assessment results, OS needs to improve its cybersecurity defenses. We identified 11 findings in the OS network, which fall under 3 security control categories: unauthorized software, user account and password management, and configuration management.

Regarding our third objective, OS needs to improve its threat mitigation procedures by more fully investigating breaches and conducting comprehensive root cause analysis. OS should also enhance its detection capabilities and technologies to better identify and eradicate advanced unknown adversary attacks.

What OIG Recommends and Office of the Secretary Comments

During the audit, OS provided sufficient evidence that 2 of the 11 findings we identified were remediated. Therefore, we recommend that OS remediate the nine remaining findings that were not remediated and improve their cybersecurity defenses as well as their detection capabilities as part of an enterprise strategy to better protect all OS systems and data.

In written comments to our draft report, OS concurred with 12 of 13 recommendations and described actions it has taken or plans to take to address our findings. OS did not concur with our recommendation to fully implement the Office of Management and Budget's (OMB) Memorandum M-17-25 stating that it was not applicable to OS or other OpDivs.

We believe our finding was valid. However, we changed the reference in the finding and modified the related recommendation to reflect the National Institute of Standards and Technology Special Publication 800-53, Revision 4 requirements.