Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

SUMMARY REPORT FOR FISCAL YEAR 2016 OIG PENETRATION TESTING OF FOUR HHS OPERATING DIVISION NETWORKS

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

Gloria L. Jarmon
Deputy Inspector General
for Audit Services

December 2017
A-18-17-08500

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The 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. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC
at https://oig.hhs.gov

Section 8M of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG Web site.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

Report in Brief
Date: December 2017
CIN: A-18-17-08500

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

Summary Report for Fiscal Year 2016 OIG Penetration Testing of Four HHS Operating Division Networks

Why OIG Did This Review

We conducted a series of OIG audits at four HHS Operating Divisions (OPDIVs) using network and web application penetration testing to determine how well HHS systems were protected when subject to cyberattacks.

Our objectives were to determine whether security controls were effective in preventing certain cyberattacks, the likely level of sophistication an attacker needs to compromise systems or data, and HHS OPDIVs' ability to detect attacks and respond appropriately.

How OIG Did This Review

During fiscal year 2016, we conducted tests at four HHS OPDIVs. We contracted with Defense Point Security (DPS) to provide knowledgeable subject matter experts to conduct the penetration testing on behalf of OIG. We closely oversaw the work performed by DPS, and testing was performed in accordance with agreed-upon Rules of Engagement between OIG and the OPDIVs.

What OIG Found

On the basis of the systems we tested, we determined that security controls across the four HHS OPDIVs needed improvement to more effectively detect and prevent certain cyberattacks. During testing, we identified configuration management and access control vulnerabilities.

We shared with senior-level information technology personnel the common root causes for the vulnerabilities we identified. We provided actionable information regarding HHS's cybersecurity posture, information on common vulnerabilities across OPDIVs, recommendations and strategies to mitigate exploited weaknesses, key indicators to better identify signs of attack or compromise, and lessons learned during testing.

We would like to thank HHS and its OPDIVs for the cooperation we received throughout the penetration testing.

What OIG Observed and HHS's Comments

We provided to HHS a restricted rollup report of the four OPDIVs. The report included six observations, and HHS was asked to respond with proposed corrective actions.

In written comments on our draft summary report, HHS in general concurred with all six of our observations in the draft report. The four HHS OPDIVs that were part of the penetration testing generally concurred with our summary findings and conveyed that the vulnerabilities identified were corrected or were in the process of being corrected. We did not validate the OPDIVs' corrective actions.