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.