Report in Brief
Date: March 2019
CIN: A-18-18-08500

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

Summary Report for Office of Inspector General Penetration Testing of Eight HHS Operating Division Networks

Why OIG Did This Review

We conducted a series of audits at eight 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 years 2016 and 2017, we conducted tests at eight 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 generally accepted government auditing standards and 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 eight HHS OPDIVs needed improvement to more effectively detect and prevent certain cyberattacks. During testing, we identified vulnerabilities in configuration management, access control, data input controls, and software patching.

We shared with senior-level HHS information technology management the common root causes for the vulnerabilities we identified, information regarding HHS's cybersecurity posture, and four broad recommendations that HHS should implement across its enterprise to more effectively address these vulnerabilities. We also provided separate reports with detailed results and specific recommendations to each OPDIV after testing was completed. We will be following up with each OPDIV on the progress of implementing our recommendations.

Based on the findings of this audit, we have initiated a new series of audits looking for indicators of compromise on HHS and OPDIV systems to determine whether an active threat exists on HHS networks or whether there has been a past breach by threat actors.

What OIG Recommends and HHS's Comments

We provided to HHS a restricted roll-up report of the results of our testing at the eight OPDIVs. The report included four broad recommendations that HHS should implement across its enterprise.

In written comments on our draft summary report, HHS management concurred with our recommendations and described actions it has taken or plans to take to ensure they are addressed. HHS also indicated that the OPDIVs have incorporated actions to address their individual vulnerabilities and that HHS will follow up with them to ensure that these have all been addressed.

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