Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

WIRELESS PENETRATION TEST OF THE CENTERS FOR MEDICARE & MEDICAID SERVICES' DATA CENTERS

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

Amy J. Frontz
Assistant Inspector General
for Audit Services

August 2016
A-18-15-30400

Office of Inspector General

http://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 http://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.

Although the Centers for Medicare & Medicaid Services had security controls that were effective in preventing certain types of wireless cyber-attacks, we identified four vulnerabilities in security controls over its wireless networks.

This summary report provides an overview of the results of our wireless penetration test of selected Centers for Medicare & Medicaid Services' (CMS) data centers and facilities. It does not include specific details of the vulnerabilities that we identified because of the sensitive nature of the information. We have provided more detailed information and recommendations to CMS so that it can address the vulnerabilities we identified. The findings listed in this summary reflect a point in time regarding system security and may have changed since we reviewed these systems.

WHY WE DID THIS REVIEW

Wireless technology offers Federal agencies opportunities to improve employee productivity and flexibility. In addition, wireless networks can provide tremendous cost savings when compared to traditional wired infrastructures. However, wireless networks and devices also present significant security challenges, including how to best protect against outside attacks and how to control access to wireless infrastructure and devices. The increased use of wireless technology has introduced several new security risks to the computing environment that can compromise sensitive information, including eavesdropping, unauthorized access points, and signal leakage. To minimize these risks, Federal agencies must implement the security controls necessary to ensure that sensitive information processed on its wireless networks and devices is protected.

CMS is the agency within the Department of Health and Human Services (HHS) that administers several key Federal healthcare programs including Medicare, Medicaid, and the Children's Health Insurance Program. CMS collects, generates, and stores financial and health care information. CMS's mission is to strengthen and modernize the Nation's health care system by providing access to high-quality care and improved health at lower cost. CMS relies on extensive information systems operations at its central office and contractor sites. CMS's Office of Enterprise Information is responsible for ensuring the effective management of the agency's information systems and resources. CMS's Office of Technology Solutions provides information technology (IT) management and oversight of all activities associated with the operation, enhancement, and delivery of IT services. This office also provides IT support services through contracts that may be used by CMS and other Federal agencies. Within CMS, the goal of the information security program is to safeguard the confidentiality, integrity, and availability of its information and systems.

Our objective was to determine whether CMS's security controls over its wireless networks were effective.

HOW WE CONDUCTED THIS REVIEW

We performed our penetration test of selected CMS data centers and employee and contractor facilities in accordance with the Rules of Engagement document we executed with CMS. Our

test simulated certain wireless cyber-attacks using tools and techniques commonly used by attackers to gain unauthorized access to wireless networks and sensitive data.

We coordinated with CMS personnel to perform the penetration testing from August 31, 2015, to December 4, 2015. The wireless penetration testing was performed at 13 CMS data centers and facilities.

We conducted the performance audit described here in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

WHAT WE FOUND

Although the Centers for Medicare & Medicaid Services had security controls that were effective in preventing certain types of wireless cyber-attacks, we identified four vulnerabilities in security controls over its wireless networks.

According to CMS, these vulnerabilities existed because of improper configurations and failure to complete necessary upgrades that CMS previously identified and reported as having been currently underway.

The vulnerabilities that we identified were collectively and, in some cases, individually significant. Although we did not identify evidence that the vulnerabilities had been exploited, exploitation could have resulted in unauthorized access to and disclosure of personally identifiable information, as well as disruption of critical operations. In addition, exploitation could have compromised the confidentiality, integrity, and availability of CMS's data and systems. We promptly shared detailed information with CMS about our preliminary findings in advance of issuing our draft report.

WHAT WE RECOMMENDED

We recommended that CMS improve its security controls to address the wireless network vulnerabilities we identified. When implemented, these recommendations should further strengthen the information security of CMS's wireless networks. Because of the sensitive nature of our findings, we have not listed the detailed recommendations in this summary report.

CMS COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments, CMS concurred with all of our findings and reported that it had already addressed several of them and is in the process of addressing the rest. CMS commented separately on the more detailed information that we sent to CMS and stated that it had accepted the risk of some of the vulnerabilities. CMS's comments on this public summary are included in their entirety as the Appendix.

The assumption of risk is a part of the security control process and each U.S. Department of Health and Human Services operating division has the authority to make risk-based decisions. The justification of risk acceptance must be documented and should be certified by the appropriate operating division management. As part of our audit followup process, we will review CMS's risk acceptance documents once they are completed.

APPENDIX: CMS COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

JUL - 8 2016

200 Independence Avenue SW
Washington, DC 20201

To: Daniel R. Levinson
Inspector General
Office of Inspector General

From: Andrew M. Slavitt
Acting Administrator
Centers for Medicare & Medicaid Services

Subject: Wireless Penetration Test of the Centers for Medicare & Medicaid Services' Data Centers (A-18-15-30400)

The Centers for Medicare & Medicaid Services (CMS) appreciates the opportunity to review and comment on the OIG report on wireless penetration testing of CMS data centers and offsite facilities. The security and privacy of data is a top priority for CMS. CMS complies with relevant laws and uses established processes, controls, and standards to secure consumer data. As the OIG reported, CMS has a number of wireless security controls that are effective in preventing wireless cyber-attacks. OIG also reported that they found no evidence of unauthorized access to or disclosure of personally identifiable information (PII). In addition, there was no evidence of any disruption of critical operations.

To secure against any potential vulnerabilities, CMS vigilantly monitors, tests, and strengthens its systems against cyber-attacks. In addition, CMS has procedures and processes in place to quickly identify, mitigate, and remove threats, in accordance with the Federal Information Security Management Act (FISMA) requirements and guidelines issued by the United States Computer Emergency Readiness Team (US-CERT). CMS also uses security prevention technology to protect the CMS network and identify rogue wireless access points, which OIG reported worked effectively during their testing. In addition CMS client devices, such as laptops, are denied connections to rogue access points, when used within CMS offsite facilities.

The CMS Employee Wireless network requires two-factor authentication; the internal network can then only be accessed through a virtual private network (VPN) over the wireless connection. The Guest Wireless Network, which provides only public Internet access at CMS buildings, is isolated from the internal network and the CMS Employee Wireless network. Both wireless networks are continuously monitored and automatically block threats using a security prevention technology.

CMS acknowledges that risks exist inherently for every IT system and that as technology progresses, additional safeguards will be needed. Through the enforcement of documented policies and procedures, as well as dedicated information security staff, CMS protects the security and privacy of data. CMS appreciates the OIG's suggestion of controls and processes that could be improved to further reduce or mitigate risk. CMS concurred with all of the OIG findings and has already addressed several of the findings and is in the process of addressing the remaining findings.