Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

OFFICE OF INSPECTOR GENERAL PENETRATION TEST OF THE CENTERS FOR MEDICARE & MEDICAID SERVICES AFFORDABLE CARE ACT INFORMATION SYSTEMS

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-18-18-08400

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-18-18-08400

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

Office of Inspector General Penetration Test of the Centers for Medicare & Medicaid Services Affordable Care Act Information Systems

Why OIG Did This Audit

We are conducting a series of OIG audits using network and web application penetration testing to determine how well these information technology (IT) systems are protected against cyberattacks. As part of this body of work, we conducted a test of the Centers for Medicare & Medicaid Services' (CMS) Affordable Care Act (ACA) information systems.

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

How OIG Did This Audit

To complete penetration testing of CMS's ACA information systems, we contracted with Accenture Federal Services to provide knowledgeable subject-matter experts to conduct penetration testing on behalf of OIG. In accordance with the *HHS OIG Penetration Testing and Reporting Guidelines*, the testing methodology was divided into three main categories—discovery, vulnerability analysis, and exploitation. We performed the testing in accordance with the agreed-upon Rules of Engagement document.

What OIG Found

Overall, we determined that most security controls in place for CMS's ACA information systems were operating effectively, but some controls needed further improvement to more adequately prevent certain cyberattacks. We identified a total of 18 vulnerabilities, of which, 2 were classified as "Critical," 9 were classified as "High," and 7 were classified as "Medium."

Of the 18 vulnerabilities discovered, 2 critical vulnerabilities were identified that could potentially present a risk to CMS's ACA data. We determined that the likely level of sophistication needed to exploit and compromise CMS's ACA information systems was medium, as most of the attacks did not require significant technical knowledge to exploit the vulnerabilities; however, there were some security controls in place to delay or prevent our attacks. Finally, we determined that CMS's IT security controls were somewhat effective at detecting and responding appropriately to our cyberattacks. This was largely attributed to the use of a security appliance that identified and appropriately stopped a subset of our initial attacks against certain CMS ACA web applications.

What OIG Recommends and CMS's Comments

We recommend that CMS improve IT security controls in accordance with Federal requirements and address the vulnerabilities identified in our report.

In written comments to our draft report, CMS concurred with eight recommendations and did not concur with two recommendations. CMS also provided technical comments, which we addressed as appropriate.

We maintain that our findings and recommendations are accurate and valid.