Report in Brief
Date: March 2024
Report No. A-18-22-09005

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

South Carolina MMIS and E&E System Security Controls Were Adequate, but Some Improvements Are Needed

Why OIG Did This Audit

We are conducting a series of audits of State Medicaid Management Information Systems (MMIS) and Eligibility and Enrollment (E&E) systems of selected States to determine how well these systems are protected when subjected to cyberattacks.

Our objectives were to determine: (1) whether security controls in operation at South Carolina's MMIS and E&E system environments were effective in preventing certain cyberattacks, (2) the likely level of sophistication or complexity an attacker needs to compromise the South Carolina Medicaid System or its data, and (3) South Carolina's ability to detect cyberattacks against its MMIS and E&E system and respond appropriately.

How OIG Did This Audit

We conducted a penetration test of the South Carolina MMIS and E&E system from April through July 2022. The penetration test focused on the MMIS and E&E system's public IP addresses and web application URLs. We also conducted a simulated phishing campaign targeting South Carolina personnel. We contracted with XOR Security, LLC (XOR), to conduct the penetration test. We closely oversaw the work performed by XOR, and the assessment was performed in accordance with agreed upon Rules of Engagement among OIG, XOR, and South Carolina.

What OIG Found

The South Carolina MMIS and E&E system had adequate security controls in place to prevent our simulated cyberattacks from resulting in a successful compromise; however, we identified security controls that could be further enhanced to better prevent certain cyberattacks. Specifically, South Carolina did not correctly implement four security controls required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5.

We estimated that an adversary would need at least a moderate level of sophistication to compromise the South Carolina MMIS and E&E system. At this level, an adversary would need a moderate level of expertise with moderate resources and opportunities to support multiple successful coordinated attacks. Additionally, although penetration testers were able to exploit an application-level vulnerability that was not blocked by network firewalls or other mechanisms, testers were not able to gain access to any systems or networks. We shared this information with South Carolina, who later provided us adequate evidence of the remediation of the security control findings related to Flaw Remediation (SI-2) and Error Handling (SI-11).

What OIG Recommends and South Carolina Comments

We recommend that South Carolina remediate the remaining two control findings (SI-10 and SC-8) in accordance with government standards and periodically test the effectiveness of these controls.

South Carolina did not indicate concurrence or nonconcurrence with our recommendation; however, it indicated that it took corrective action to address the two control findings. Although we have not yet confirmed South Carolina's remediation of the two control findings identified in our report, we commend South Carolina's ongoing efforts to improve the overall security posture of its MMIS and E&E system environments.

The full report can be found on the OIG website.