Report in Brief
Date: March 2024
Report No. A-18-21-09001

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

Utah MMIS and E&E System Had Adequate Security Controls In Place, but Improvements Are Needed

Why OIG Did This Audit

We are conducting a series of audits of State Medicaid Management Information Systems (MMISs) 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 whether: (1) security controls in operation at Utah'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 Utah MMIS and E&E system or its data, and (3) Utah'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 Utah MMIS and E&E system from February to March 2021. 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 Utah personnel. We contracted with XOR Security, LLC (XOR), to assist in conducting 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 Utah.

What OIG Found

The Utah MMIS and E&E system had adequate security controls in place to prevent our simulated cyberattacks from resulting in a successful compromise; however, some of those security controls could be improved to better prevent certain cyberattacks and reduce overall risk. Specifically, Utah did not correctly implement seven security controls required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4. We shared this information with Utah, which provided evidence that four of the security control findings have been remediated.

We estimated that the level of sophistication needed by an adversary to compromise the Utah MMIS and E&E system was significant. At this level, an adversary would need a significant level of expertise through advanced training and persistence to circumvent most of the current security controls. Finally, based on the results of our simulated cyberattacks, Utah demonstrated the ability to detect some attacks and respond appropriately. However, Utah did not detect and prevent other penetration test activities we performed in later phases.

Utah may not have correctly implemented security controls because system administrators were not aware of Government standards or industry best practices that require securely configured systems before deployment to production. Also, Utah's flaw remediation procedures were not consistent with the timeframe defined in the CMS ARS policy for correcting identified security-related information system flaws on production systems. Lastly, there is no requirement from CMS for more frequent penetration testing unless the system is considered a high value asset.

What OIG Recommends and Utah Comments

We recommend that Utah: (1) remediate the remaining three security control findings and (2) revise flaw remediation procedures such that they fully implement the flaw remediation requirements defined in the CMS Acceptable Risk Safeguards.

Utah agreed with our recommendations and stated that it has addressed and remediated the security control findings identified by OIG (first recommendation) and is in the process of addressing our second recommendation. We are encouraged by Utah's actions and we look forward to receiving and reviewing its supporting documentation through our audit resolution process.

The full report can be found on the OIG website.