Report in Brief
Date: August 2024
Report No. A-18-22-09009

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

Illinois MMIS and E&E System Had Adequate Security Controls in Place, but Some 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 Illinois' 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 Illinois MMIS and E&E system or its data, and (3) Illinois' 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 Illinois MMIS and E&E system from August through September 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 Illinois 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 Illinois.

What OIG Found

The Illinois 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 Illinois' risk of compromise. Specifically, Illinois did not correctly implement four security controls required by the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4.

We estimated that an adversary would need a significant level of sophistication to compromise the Illinois MMIS and E&E system. At this level, an adversary would need a significant level of expertise through advanced training and a significant level of persistence to circumvent most of the current security controls. Illinois demonstrated the ability to detect some of our cyberattacks against its MMIS and E&E system by blocking our testing domain after it detected our hacking attempts.

Potential reasons why Illinois did not correctly implement these security controls may be that system developers and administrators were not aware of Government standards, due to a lack of documented enterprise flaw remediation procedures, and ineffective testing procedures when periodically assessing implementation of NIST security controls. As a result, an attacker could potentially execute multiple types of targeted attacks against the Illinois MMIS and E&E system.

What OIG Recommends and Illinois Comments

We made a series of recommendations for Illinois to improve its security controls over its MMIS and E&E system, including that it enhances its security control assessment testing procedures and takes corrective actions when deficiencies in controls are identified. The full recommendations are in the report.

In written comments, Illinois did not indicate concurrence or nonconcurrence with our recommendations. Rather, Illinois stated that it concurs with each of the needed improvements mentioned in the draft report and described actions ongoing or taken to address the four control findings we identified. Although we have not yet confirmed whether our recommendations were effectively implemented, we are encouraged by Illinois's response and we look forward to receiving and reviewing the supporting documentation through our audit resolution process.