Report in Brief
Date: March 2023
Report No. A-18-20-08004

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

Michigan MMIS and E&E Systems Security Controls Were Generally Effective, 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 whether (1) security controls in operation at Michigan 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 Michigan Medicaid System or its data, and (3) Michigan'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 Michigan's MMIS and E&E system from October through December 2020. 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 that included a limited number of Michigan personnel in December 2020. 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 Michigan.

What OIG Found

The Michigan MMIS and E&E System had reasonable security controls in place to prevent our simulated cyberattacks from resulting in a successful compromise; however, some of those security controls could be further enhanced to better prevent certain cyberattacks. Michigan did not correctly implement six security controls required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

In addition, we estimated that the level of sophistication required to compromise the Michigan MMIS and E&E system was significant. At this level, an adversary would need a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks. Finally, based on the results of our simulated cyberattacks, some improvements were needed in Michigan's detection controls to better identify cyberattacks against its MMIS and E&E system and respond appropriately.

Potential reasons why Michigan did not implement these security controls correctly may be that software developers did not follow secure coding standards to prevent security vulnerabilities or system administrators were not aware of government standards or industry best practices that require securely configuring systems before deployment to production. Michigan also may not have properly factored in cybersecurity risks during the design and implementation of authentication management for their MMIS and E&E systems. Additionally, Michigan's procedures for periodically assessing the implementation of the weak NIST security controls we identified were not effective. By addressing the root causes of the security control failures we identified, Michigan can bolster its ability to detect and prevent certain cyberattacks.

What OIG Recommends

We recommend that Michigan (1) remediate the six security control findings OIG identified, (2) assess the effectiveness of all required NIST SP 800-53 controls according to the organization's defined frequency, and (3) assess the cryptographic configurations of public servers at least annually and adjust if the requirements have changed.

In written comments to our draft report, Michigan concurred with our recommendations and stated that they have either remediated or were in process of remediating our findings. Although we have not yet confirmed whether our recommendations were effectively implemented, we are encouraged by Michigan's response and we look forward to receiving and reviewing the supporting documentation through our audit resolution process.