Report in Brief
Date: May 2023
Report No. A-18-21-09003

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

Maryland MMIS and E&E System Security Controls Were Partially Effective and 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 Maryland 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 Maryland Medicaid System or its data, and (3) Maryland's ability to detect cyberattacks against its Medicaid MMIS and E&E system and respond appropriately.

How OIG Did This Audit

We conducted a penetration test of Maryland's MMIS and E&E system from September through November 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 that included a limited number of Maryland personnel in November 2021. 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 Maryland.

What OIG Found

The Maryland MMIS and E&E system had security controls in place that were partially effective to prevent our simulated cyberattacks from resulting in a successful compromise; however, improvements are needed to better prevent certain cyberattacks. Maryland did not correctly implement seven security controls from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

In addition, we estimated that the level of sophistication needed by an adversary to compromise the Maryland MMIS and E&E system was limited.[1] At this level, an adversary would need a limited level of expertise, with limited resources and opportunities to support a successful attack. Finally, Maryland demonstrated a partial ability to detect some of our cyberattacks against its MMIS and E&E system and respond appropriately.

A potential reason why Maryland did not implement these security controls correctly may be that system administrators were not aware of government standards or industry best practices that require securely configured systems before deployment to production. Maryland also may not have considered the latest email phishing tactics used by cyber adversaries in developing the cybersecurity awareness training provided to its employees and contractors. Additionally, Maryland's procedures for periodically assessing the implementation of the NIST security controls above were not effective. As a result of Maryland not correctly implementing these controls, an attacker could potentially extract sensitive data and PII, impersonate other users, and redirect users to malicious websites which facilitates an attacker's ability to get an initial foothold and potentially move deeper into the network, thereby exposing critical systems and data to attack and compromise.

What OIG Recommends

We recommend that Maryland: (1) remediate the seven control findings OIG identified; (2) assess the effectiveness of all required NIST SP 800-53 controls according to the organization's defined frequency; (3) assess at least annually and if necessary, adjust baseline configurations for its MMIS and E&E public servers; and (4) perform periodic phishing exercises and enhance employee and contractor cybersecurity awareness training based on the results of the phishing exercises, if needed.

In written comments on our draft report, Maryland concurred with our recommendations and stated that they have remediated our findings. Although we have not yet confirmed the changes Maryland described in its response, we commend Maryland's ongoing efforts to improve the overall security posture of its MMIS and E&E system environments.