Report in Brief
Date: November 2022
Report No. A-18-20-08005

U.S. Department of Health & Human Services
Office of Inspector General

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 Puerto Rico 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 Puerto Rico Medicaid System or its data, and (3) Puerto Rico'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 Puerto Rico's MMIS and E&E systems from November to December 2020. The penetration test focused on the MMIS and E&E systems' public IP addresses and web application URLs. We also conducted a simulated phishing campaign that included a limited number of Puerto Rico 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 Puerto Rico.

Puerto Rico MMIS and E&E Systems Security Controls Were Generally Effective, but Some Improvements Are Needed

What OIG Found

The Puerto Rico 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. Puerto Rico did not correctly implement five 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 by an adversary to compromise the Puerto Rico 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 Puerto Rico detection controls to better identify cyberattacks against its MMIS and E&E system and respond appropriately.

Potential reasons why Puerto Rico 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 Puerto Rico 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, Puerto Rico's procedures for periodically assessing the implementation of the NIST security controls above were not effective. By addressing the root causes of the security control failures we identified, Puerto Rico can bolster its ability to detect and prevent certain cyberattacks.

What OIG Recommends and Puerto Rico Comments

We recommend that Puerto Rico: (1) remediate the vulnerabilities related to the five security control findings identified by properly implementing and regularly assessing the associated NIST SP 800-53 controls and (2) assess the cryptographic configurations of public servers at least annually and adjust if the requirements have changed. In written comments on our draft report, Puerto Rico concurred with our recommendations and stated that it has addressed and remediated our findings. We look forward to receiving documentation from Puerto Rico through our audit follow-up process that demonstrates the recommendations have been effectively implemented.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/182008005.asp.