Report in Brief
Date: October 2023
Report No. A-18-21-09004

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

South Dakota 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) system 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 South Dakota'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 South Dakota MMIS and E&E system or its data, and (3) South Dakota'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 South Dakota's MMIS and E&E system from November 2021 through January 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 that included a limited number of South Dakota personnel in February 2022. 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 South Dakota.

What OIG Found

The South Dakota 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, some of those security controls could be further enhanced to better prevent certain cyberattacks. South Dakota did not correctly implement six 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 South Dakota MMIS and E&E system was moderate. At this level, an adversary would need a moderate level of expertise, with moderate resources and opportunities to support a successful attack. Finally, based on the results of our simulated cyberattacks, South Dakota would need to improve its monitoring controls to better detect cyberattacks against its MMIS and E&E system and respond appropriately.

Potential reasons why South Dakota did not implement these security controls correctly may be that system developers and system administrators were not aware of government standards or industry best practices that require securely configured systems or did not correct flaws in systems before deployment to production. Additionally, South Dakota's procedures for periodically assessing the implementation of the NIST security controls above were not effective. As a result of South Dakota not correctly implementing these controls, an attacker could potentially extract sensitive data and PII, impersonate other users, and redirect users to malicious websites.

What OIG Recommends and South Dakota Comments

We recommend that South Dakota remediate the six control findings OIG identified. In written comments on our draft report, South Dakota did not state whether it concurred with our recommendation. Instead, South Dakota stated that it took steps to address five of the six control findings and that it partially implemented the remaining control finding that had a low-risk rating. We have not confirmed that South Dakota implemented these steps. We will validate the actions taken by South Dakota during the audit resolution process.