Report in Brief
Date: May 2023
Report No. A-18-20-08003

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

Massachusetts MMIS and E&E System 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 (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 for Massachusetts 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 Massachusetts' Medicaid System or its data, and (3) Massachusetts' 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 the Massachusetts MMIS and E&E system from September 2020 to October 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 Massachusetts 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 Massachusetts.

What OIG Found

The Massachusetts MMIS and E&E system had generally effective 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. Massachusetts did not correctly implement three 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 needed by an adversary to compromise the Massachusetts 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 multiple successful coordinated attacks. Finally, based on the results of certain simulated cyberattacks that we conducted, we determined that some improvements were needed in Massachusetts detection controls to better identify cyberattacks against its MMIS and E&E system and respond appropriately.

A potential reason why Massachusetts did not implement these security controls correctly may be that system administrators were not aware of certain published vendor security advisories or mitigation guidance. Additionally, Massachusetts's procedures for periodically assessing the implementation of the weak NIST security controls we identified were not effective. Because Massachusetts did not correctly implement these controls, an attacker could potentially collect sensitive server information to facilitate exploitation of an application or web server or cause a denial-of-service.

What OIG Recommends

We recommend that Massachusetts: (1) remediate the three 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 and adjust, if necessary, vulnerability management procedures to ensure any pertinent publicly disclosed computer security vulnerabilities are assessed for risk and remediated promptly, if necessary.

Massachusetts concurred with our recommendations and outlined actions it has taken to improve its overall security posture and mitigate the findings.