Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

MASSACHUSETTS MMIS AND E&E SYSTEMS SECURITY CONTROLS WERE GENERALLY EFFECTIVE, BUT SOME IMPROVEMENTS ARE NEEDED

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Amy J. Frontz
Deputy Inspector General
for Audit Services

May 2023
A-18-20-08003

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG) is to provide objective oversight to promote the economy, efficiency, effectiveness, and integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of the people they serve. Established by Public Law No. 95-452, as amended, OIG carries out its mission through audits, investigations, and evaluations conducted by the following operating components:

Office of Audit Services. OAS provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. The audits examine the performance of HHS programs, funding recipients, and contractors in carrying out their respective responsibilities and provide independent assessments of HHS programs and operations to reduce waste, abuse, and mismanagement.

Office of Evaluation and Inspections. OEI's national evaluations provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. To promote impact, OEI reports also provide practical recommendations for improving program operations.

Office of Investigations. OI's criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs and operations often lead to criminal convictions, administrative sanctions, and civil monetary penalties. OI's nationwide network of investigators collaborates with the Department of Justice and other Federal, State, and local law enforcement authorities. OI works with public health entities to minimize adverse patient impacts following enforcement operations. OI also provides security and protection for the Secretary and other senior HHS officials.

Office of Counsel to the Inspector General. OCIG provides legal advice to OIG on HHS programs and OIG's internal operations. The law office also imposes exclusions and civil monetary penalties, monitors Corporate Integrity Agreements, and represents HHS's interests in False Claims Act cases. In addition, OCIG publishes advisory opinions, compliance program guidance documents, fraud alerts, and other resources regarding compliance considerations, the anti-kickback statute, and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC

at https://oig.hhs.gov

Section 8M of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG website.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

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.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS AUDIT

The Department of Health and Human Services (HHS), Office of Inspector General (OIG), is conducting a series of audits of State Medicaid Management Information Systems (MMIS) and Eligibility and Enrollment (E&E) systems. In the last 10 years, we have performed multiple audits of State MMIS and E&E systems and found that most did not have adequate internal controls to protect the systems from internal and external attacks. Therefore, we are using penetration testing to determine how well these State Medicaid systems are protected when subjected to cyberattacks.[1]

Specifically, as part of this body of work, we conducted a penetration test of Massachusetts MMIS and E&E system in accordance with guidelines outlined by the National Institute of Standards and Technology (NIST).[2]

OBJECTIVES

Our objectives were to determine:

- whether security controls in operation for Massachusetts MMIS and E&E system environments were effective in preventing certain cyberattacks,

- the likely level of sophistication or complexity an attacker needs to compromise the Massachusetts MMIS and E&E system or its data, and

- Massachusetts' ability to detect cyberattacks against its MMIS and E&E system and respond appropriately.

BACKGROUND

The Medicaid program provides medical assistance to low-income individuals and individuals with disabilities. The Federal and State Governments jointly fund and administer the Medicaid program. At the Federal level, the Centers for Medicare & Medicaid Services (CMS) administers the program. Each State administers its Medicaid program in accordance with a CMS-approved State plan. Although the State has considerable flexibility in designing and operating its Medicaid program, it must comply with applicable Federal requirements.

[1] Penetration testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. It often involves launching real attacks on real systems and data using tools and techniques commonly used by attackers.

[2] NIST Special Publication (SP) 800-115, *Technical Guide to Information Security Testing and Assessment*.

The MMIS is an automated system of claims processing and information retrieval used in State Medicaid programs. The system processes Medicaid claims submitted by providers and produces and retrieves utilization data and management information about medical care and services furnished to Medicaid recipients. The MMIS performs Medicaid business functions such as:

- program administration and cost control,
- enrollee and provider inquiries and services,
- operations of claims control and computer systems, and
- management reports for planning and control.

State E&E systems support all processes related to determining Medicaid eligibility. After the implementation of the Patient Protection and Affordable Care Act (ACA) in 2014, States were required to coordinate enrollment between both Medicaid and ACA health care coverage systems.

With significant increases in cyberattacks against the health care industry, including email phishing, denial of service, and ransomware attacks, States' MMIS and E&E systems are likely targets for hackers. These systems host numerous records of people enrolled in Medicaid, e.g., Protected Health Information (PHI) and other sensitive information that is sought by cyber criminals and foreign adversaries for financial gain, to sabotage State systems, or both.

In Massachusetts, Medicaid and the Children's Health Insurance Program (CHIP) are combined into one program called MassHealth.[3] MassHealth provides comprehensive health insurance and dental coverage for eligible individuals, families, and people with disabilities across the Commonwealth of Massachusetts. The MMIS and the Provider Online Service Center (POSC) both support the web-based provider portal that is used by MassHealth providers to access, submit, and retrieve transactions and information that support the administration of health care to MassHealth members. Massachusetts reported over 1.9 million Medicaid and CHIP enrollees as of June 2022.

HOW WE CONDUCTED THIS AUDIT

We conducted a penetration test of the Massachusetts MMIS and E&E system from September 2020 through 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 covered a limited number of Massachusetts personnel in December 2020.

[3] Mass.gov. Available online at https://www.mass.gov/topics/masshealth. Accessed on Oct. 6, 2022.

To assist us with the penetration test, we relied on the work of specialists. OIG contracted with XOR Security, LLC (XOR), to assist in conducting the penetration test of the Massachusetts MMIS and E&E system. XOR provided subject matter expertise throughout the assessment of the MMIS and E&E system.

To simulate a real-world attack more closely, the penetration testing team was given no substantive information about the environment before testing began. This scenario is known as a zero-knowledge, or black box, penetration test. We performed testing in accordance with the agreed-upon Rules of Engagement (ROE) document, signed in September 2020 by OIG, XOR, and the Massachusetts Executive Office of Health and Human Services.

We provided detailed documentation about our preliminary findings to Massachusetts in advance of issuing our draft report.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix A contains the details of our audit scope and methodology, Appendix B describes the tools we used to conduct the audit, and Appendix C contains Federal requirements.

FINDINGS

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. In addition, we estimated that the level of sophistication needed by an adversary to compromise the MMIS and E&E system was moderate.[4] 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.

[4] Based on MITRE's Cyber Prep Methodology, threat levels are assigned to cyber adversaries indicating the approximate level of sophistication and resources an adversary will likely employ to achieve its goals. See *How Do You Assess Your Organization's Cyber Threat Level?* Available online at https://www.mitre.org/sites/default/files/pdf/10_2914.pdf. Accessed on March 28, 2023.

State agencies operating MMIS and E&E systems must implement appropriate information security controls based on recognized industry standards or standards governing the security of Federal IT systems and information processing.[5] Massachusetts did not correctly implement the following NIST Special Publication (SP) 800-53, Revision 4, security controls as shown in the table below:

Table: Weak MMIS and E&E System Security Controls

NIST SP 800-53, Revision 4, Security Control	Security Control Finding	Control No.*	Risk Rating†
Access Enforcement	Massachusetts did not properly enforce access control to information and system resources for a public-facing system in its MMIS and E&E system.	AC-3	Moderate
Session Authenticity	Massachusetts did not properly implement controls to protect the authenticity and validity of communication sessions for a public-facing system in its MMIS and E&E system.	SC-23	Moderate
Information System Monitoring	Massachusetts did not adequately monitor its MMIS and E&E system to detect and prevent certain attacks.	SI-4	Moderate

* The Control No. is the abbreviation of the control family name and the number of the specific control within NIST SP 800-53, Revision 4.

† Security Control Risk Rating as determined by HHS-OIG.

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 procedures for periodically assessing the implementation of the NIST security controls above were not effective. As a result of Massachusetts not correctly implementing 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.

Regarding our email phishing campaign, we sent 49 phishing emails to specific employees, and we determined that none of those emails were opened and none of the web links embedded in the emails were clicked. The reason for the zero open and click rate could be that

[5] For more information, see https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-A/part-95/subpart-F/subject-group-ECFR8ea7e78ba47a262/section-95.621. Accessed on Jan. 13, 2022.

Massachusetts network defenses successfully detected the phishing emails and did not deliver them to the intended employee or the employees who received the emails simply did not open them during our campaign. We have shared these results as information only and encouraged Massachusetts to continue challenging their defenses and employees with increasingly more sophisticated phishing campaigns so that they remain prepared for future phishing attacks.

RECOMMENDATIONS

We recommend that the Massachusetts Department of Health and Human Services:

- remediate the three security control findings OIG identified;
- assess the effectiveness of all required NIST SP 800-53 controls according to the organization's defined frequency; and
- 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' COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments on our draft report, Massachusetts concurred with our recommendations. Massachusetts stated that MassHealth IT has reviewed and re-engineered system access policies and procedures and reviewed the applications against the NIST standards since the OIG assessment in late 2020. Furthermore, Massachusetts wrote that in early 2021 MassHealth IT improved its overall security posture and, in the process, mitigated the vulnerabilities identified in the OIG findings.

Although we have not confirmed the changes Massachusetts described in its response, we commend Massachusetts' ongoing efforts to improve the overall security posture of its MMIS and E&E system environments.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

The penetration test focused on both public IP addresses and web application URLs related to the Massachusetts MMIS and E&E system, as specified within the ROE document. Massachusetts provided us with a list of its external public facing hosts that were related to the MMIS and E&E system.

Regarding internal controls that were reviewed during our audit, we only assessed control activities specific to IT general controls and application controls for the Massachusetts MMIS and E&E system. We did not assess all internal control components and principles.[6] Based on our penetration test we assessed the operating effectiveness of these internal controls and identified deficiencies that we believe could affect Massachusetts' ability to detect, or effectively prevent certain cyberattacks. The internal control deficiencies we identified are listed as Security Control Findings in the Findings section of this report. However, the penetration test we performed may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

We performed our work remotely. Penetration testing began on September 28, 2020 and ended October 30, 2020, and the simulated phishing campaign began on December 1, 2020 and ended December 8, 2020.

For the simulated phishing campaign, Massachusetts provided us with a list of 49 employee email addresses.

METHODOLOGY

We relied on the work of specialists to assist with the series of OIG audits utilizing network and web application penetration testing and social-engineering techniques. OIG contracted with XOR to conduct the penetration test of the Massachusetts MMIS and E&E system. XOR provided subject matter experts who conducted the penetration test of all systems identified in the ROE document. In addition, XOR planned and executed a simulated email phishing campaign against a subset of the Massachusetts Medicaid agency's employees. OIG oversaw the work to ensure that all objectives were met and that testing was performed in accordance with Government auditing standards and the ROE document.

Our testing focused on the publicly available web applications and infrastructure used to support the Massachusetts MMIS and E&E system. To accomplish our objectives, OIG and Massachusetts prepared the ROE document that outlined the general rules, logistics, and

[6] *Standards for Internal Control in the Federal Government*, GAO-14-704G

expectations for the penetration test. Massachusetts officials provided a signed ROE document indicating that it agreed with the rules to be followed during our testing.

In September 2020, we began reconnaissance and scope verification of network subnets owned, operated, and maintained by Massachusetts. We performed external penetration testing to determine whether internet-facing systems were susceptible to exploits by an external attacker.

XOR performed procedures including:

- using information-gathering techniques to discover:
  - network address ranges
  - host names;
  - hosts exposed to the internet
  - applications running on exposed hosts
  - operating system, application version, and current patch levels on specific systems
  - the structure of the applications and supporting servers, and
  - domain name server records
- using vulnerability analysis techniques to discover possible methods of attack;
- attempting to exploit vulnerabilities identified in the vulnerability analysis to gain root- or administrator-level access to the targeted systems or other trusted user accounts;
- conducting a simulated phishing attack; and
- testing web applications, which included assessing the security controls and design and implementation of targeted web applications to find errors, trying to create unintended responses from the application, and identifying any flaws in the application that could be used to access resources or circumvent security controls.

In December 2020, XOR conducted a simulated phishing campaign to determine whether Massachusetts had implemented appropriate controls to detect and prevent successful

phishing campaigns and to determine whether Massachusetts personnel were adequately trained to recognize and appropriately respond to such malicious emails. Massachusetts provided a list of 49 employees who would be subject to XOR's simulated phishing campaign. The campaign was designed to send those employees a phishing email that contained a web link to a malicious website. If any of the employees clicked the link, their web browser would be redirected to a website hosted within the HHS-OIG Cyber Range.[7] A program would then attempt to run code in the employee's browser and system, allowing for remote access by the penetration testers.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[7] The HHS-OIG Cyber Range is a virtual private cloud solution to support IT auditing and assessment responsibilities. It is hosted on top of the Amazon Web Services infrastructure.

APPENDIX B: TOOLS WE USED TO CONDUCT THE AUDIT

Kali Linux

Kali Linux (formerly known as BackTrack) is a Debian-based distribution with a collection of security and forensics tools that runs on a wide spectrum of devices. It is used for conducting vulnerability assessments, penetration tests, and digital forensics.

Burp Suite Pro

Burp Suite Pro is an integrated platform for performing security testing of web applications. It supports automated scans and manual testing. Burp Suite Pro also has a robust system of extensions that allows users to add functionality as new exploits and tools are released.

GoPhish

GoPhish is a powerful, open-source phishing framework that can easily be installed on a variety of operating systems. It allows penetration testers and businesses to conduct real-world phishing simulations.

Cobalt Strike

Cobalt Strike is a commercial, full-featured, penetration testing tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors." Cobalt Strike's interactive post-exploit capabilities cover a full range of tactics, all executed within a single, integrated system. In addition to its own capabilities, Cobalt Strike leverages the capabilities of other well-known tools such as Metasploit and Mimikatz.

BeEF

BeEF is a penetration testing tool that focuses on web browsers. BeEF allows professional penetration testers to assess the security posture of a target environment by using client-side attacks.[8] Unlike other security frameworks, BeEF examines exploitability within the web browser. BeEF attempts to gain control of a victim's web browser and use it as a launching point for attacks against a system.

[8] A "client-side attack" occurs when a user (the client) downloads malicious code from the server, which is then interpreted and rendered by the client browser.

APPENDIX C: FEDERAL REQUIREMENTS

45 CFR § 95.621(f), ***ADP System Security Requirements and Review Process***, states:

> (1) ADP System Security Requirement.[9] State agencies are responsible for the security of all ADP projects under development, and operational systems involved in the administration of HHS programs. State agencies shall determine the appropriate ADP security requirements based on recognized industry standards or standards governing security of Federal ADP systems and information processing.

NIST SP 800-53, Revision 4, ***Security and Privacy Controls for Federal Information Systems and Organizations,*** **Appendix F Security Control Catalog,** states:

AC-3 ACCESS ENFORCEMENT (page F-10)

> Control: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
>
> Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security.

SC-23 SESSION AUTHENTICITY (page F-201)

> Control: The information system protects the authenticity of communications sessions.
>
> Supplemental Guidance: This control addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the

[9] ADP means automated data processing performed by a system of electronic or electrical machines that are interconnected and interacting in a manner that minimizes the need for human assistance or intervention.

insertion of false information into sessions.

SI-4 INFORMATION SYSTEM MONITORING (Page F-219)

Control: The organization:

a. Monitors the information system to detect:
   1. Attacks and indicators of potential attacks in accordance with [*Assignment: organization-defined monitoring objectives*]; and
   2. Unauthorized local, network, and remote connections;
b. Identifies unauthorized use of the information system through [*Assignment: organization-defined techniques and methods*];
c. Deploys monitoring devices:
   1. Strategically within the information system to collect organization-determined essential information; and
   2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

The Commonwealth of Massachusetts
Executive Office of Health and Human Services
Office of Medicaid
One Ashburton Place, Room 1109
Boston, Massachusetts 02108

MAURA T. HEALEY
Governor

KIMBERLEY L. DRISCOLL
Lieutenant Governor

MARY A. BECKMAN
Acting Secretary

MIKE LEVINE
Assistant Secretary for
MassHealth

Tel: (617) 573-1600
Fax: (617) 573-1891
www.mass.gov/eohhs

January 25, 2023

Massachusetts Executive Office of Health and Human Services Response to U.S. Department of Health and Human Services, Office of the inspector General Draft Report No. A-18-20-08003

OIG Recommendations
OIG recommends 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 Response: We concur with the recommendations based on conditions at the time of the audit in 2020. Since the OIG Assessment in late 2020, MassHealth IT has reviewed and re-engineered the system access policies and procedures and reviewed the applications against the NIST standards. In early 2021 MassHealth IT improved its overall security posture and, in the process, mitigated the vulnerabilities identified in the OIG findings. Below are the findings and Massachusetts's mitigations.

Recommendation 1: Massachusetts Should Remediate the Three Security Control Findings:

Finding: Access Enforcement (AC-3). Massachusetts did not properly enforce access control to information and system resources for a public-facing system in its MMIS and E&E system.

Massachusetts Response: MassHealth IT has updated its Systems Access Administration and Operations Guide document, which describes the process of evaluating all application access requests managed by the IT Access & Controls team as well as the MassHealth Access Profile Matrix. The documents represent the policies and procedures, guidelines, and best practices required for the creation and maintenance of user system access for employees, contractors, and vendor partner staff – among

other things, these policies and procedures, guidelines, and best practices govern access control to information and system resources. The Systems Access Administration and Operations Guide and MassHealth Access Profile Matrix are maintained and reviewed by the MassHealth IT Access & Controls Team. The policies and procedures are updated as systems change, reviewed by the team and IT leadership on an annual basis and monitored by EHS IT Teams per policy requirements throughout the year.

Finding: Session Authenticity (SC-23). Massachusetts did not properly implement controls to protect the authenticity and validity of communication sessions for a public-facing system in its MMIS and E&E system.

Massachusetts Response: MassHealth applications utilize a platform (MA Virtual Gateway) which serves as a single sign-on (SSO) access point utilizing an industry recognized IAM solution. This solution provides the functionality and protocols required to validate and protect application sessions from being compromised. More specifically the functionality leverages industry standards to allow users to log on to multiple applications, validate sessions, and logs session activity. The IDM additionally pushes down password complexity requirements.

Finding: Information System Monitoring (SI-4). Massachusetts did not adequately monitor its MMIS and E&E system to detect and prevent certain attacks.

Massachusetts Response: The Massachusetts Executive Office of Health and Human Services (EOHHS) receives hosting services from the Massachusetts Executive Office of Technology Services and Security (EOTSS). EOHHS works closely and partners with EOTSS on system security at a state level. EOTSS utilizes an industry recognized IDS solution. MassHealth's applications (including MMIS and the E&E system) comply with the EOTSS and EOHHS published security guidelines. Security logs are monitored at the portal application and database level regularly. In December of 2022, the Massachusetts Cyber Incident Response Team (MA-CIRT) was established in accordance with Executive Order 602. Led by the Secretary of the Executive Office of Technology Services and Security (EOTSS), MA-CIRT is established with the mission of enhancing the Commonwealth's ability to prepare for, respond to, mitigate against, and recover from significant cybersecurity threats. Executive order 602 was issued just as Massachusetts and other jurisdictions confront an overall increase in cybersecurity threats to websites and networks.

Recommendation 2: Assess the effectiveness of all required NIST SP 800- 53 controls according to the organization's defined frequency.

Massachusetts Response: MassHealth IT, in partnership with the EOHHS Chief Information Security Officer (CISO) Office, participates in the Nationwide Cybersecurity Review (NCSR), which is a voluntary security assessment conducted on an annual basis (since 2020), that overlaps with NIST SP 800-53. In addition, the CISO Office has created a Compliance Unit consisting of 4 FTEs to begin conducting NIST SP 800-53 controls assessments for all MassHealth IT systems, starting in the Spring of 2023.

Recommendation 3: Assess vulnerability management procedures to ensure any pertinent publicly disclosed computer security vulnerabilities are assessed for risk and remediated.

Massachusetts Response: As explained above, EOHHS (1) receives hosting services from EOTSS, and (2) works closely and partners with EOTSS on system security at a state level. The EOTSS Security Office maintains policies and procedures (including Vulnerability Management policies and procedures (IS.016)). Among other things, these policies and procedures require monthly vulnerability scans to identify, classify and remediate vulnerabilities across all technology environments and platforms to reduce the Commonwealth's exposure to cyber threats. EOTSS distributes alerts and industry guidance to the Commonwealth SOC and ensures that associated directives are implemented within established timeframes, or the issuing organization is notified of noncompliance. EOHHS and MassHealth IT participate in and receive the benefits of these services.