Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

MICHIGAN 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

March 2023
A-18-20-08004

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The 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. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These audits help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning 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: March 2023
Report No. A-18-20-08004

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

Michigan MMIS and E&E Systems 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 (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 Michigan 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 Michigan Medicaid System or its data, and (3) Michigan'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 Michigan's MMIS and E&E system from October through December 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 Michigan 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 Michigan.

What OIG Found

The Michigan 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. Michigan did not correctly implement six 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 to compromise the Michigan 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 Michigan's detection controls to better identify cyberattacks against its MMIS and E&E system and respond appropriately.

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

What OIG Recommends

We recommend that Michigan (1) remediate the six 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 the cryptographic configurations of public servers at least annually and adjust if the requirements have changed.

In written comments to our draft report, Michigan concurred with our recommendations and stated that they have either remediated or were in process of remediating our findings. Although we have not yet confirmed whether our recommendations were effectively implemented, we are encouraged by Michigan's response and we look forward to receiving and reviewing the supporting documentation through our audit resolution process.

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. Specifically, we are using penetration testing to determine how well these State Medicaid systems are protected when subjected to cyberattacks.[1]

As part of this body of work, we conducted a penetration test of Michigan's MMIS and E&E system in accordance with recommendations outlined by the National Institute of Standards and Technology (NIST).[2]

OBJECTIVES

Our objectives were to determine:

- whether security controls in operation for Michigan 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 Michigan MMIS and E&E system or its data, and
- Michigan's 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 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,
- beneficiary 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 beneficiary enrollment and care 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 Medicaid beneficiary records containing 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.

The Michigan Department of Health and Human Services (MDHHS) is responsible for providing a variety of services to the residents of Michigan and administering the State Medicaid program. In particular, the Medical Services Administration administers the Medicaid program, providing health care services to eligible Michigan residents. They include families enrolled in the Family Independence Program, other low-income families, Supplemental Security Income (SSI) recipients, pregnant women, children, the elderly, the disabled, the blind, and the medically needy, who, except for income, would qualify for regular Medicaid. MDHHS also administers many other programs, including the Healthy Michigan Plan and MIChild, which serves children whose families have incomes up to twice the Federal poverty level. MDHHS is in all 83 Michigan counties and provides services to residents of Michigan via its offices and departments. As of 2020, MDHHS has enrolled more than 2.5 million residents.

The Michigan MMIS is a web-based, rules-driven, role-based, real-time Medicaid Management System. The MMIS comprises multiple subsystems that perform the following processes and functions for State, provider, and member users in support of Medicaid and other MDHHS programs:

- Provider Management – enrollment/screening,
- Member Services – eligibility/enrollment for managed care and fee-for-service benefit plans,
- Member Portal,
- Prior Authorization Requests and Approvals,
- Claims Adjudication/Payments & Health Plan Capitation Payments, and
- Facility Settlement Cost Activities.

The Michigan MI Bridges E&E system is a public-private partnership that aims to connect greater numbers of individuals and families in Michigan to a range of State and local resources, as well as to MDHHS benefit programs, to promote household stability. Clients may use MI Bridges not only to apply for benefits and manage their cases, but also to locate resources in their community to support a wide range of needs, including food, housing and shelter, utilities, health, income and employment, transportation, childcare, and education. Community partners can receive client referrals sent through MI Bridges and have access to a directory of clients they have assisted.

HOW WE CONDUCTED THIS AUDIT

We conducted a penetration test of Michigan's MMIS and E&E system from October through December 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 Michigan personnel in December 2020.

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 Michigan 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 October 2020 by OIG, XOR, and Michigan's Enterprise Compliance Division.

We provided detailed documentation about our preliminary findings to Michigan 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 Michigan 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. In addition, we estimated that the level of sophistication required to compromise the MMIS and E&E system was significant. [3] 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 Michigan's detection controls to better identify cyberattacks against its MMIS and E&E system and respond appropriately.

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

Table: Weak MMIS and E&E Systems Security Controls

NIST SP 800-53, Revision 4, Security Control	Security Control Finding	Control No. *	Risk Rating†
Configuration Settings	Michigan did not establish configuration settings for its MMIS and E&E system that reflect the most restrictive mode consistent with operational requirements.	CM-6	Moderate

[3] How Do You Assess Your Organization's Cyber Threat Level? Available online at https://apps.dtic.mil/sti/pdfs/AD1137499.pdf. Accessed on Oct. 6, 2022.

[4] For more information, please see https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-A/part-95/subpart-F/subject-group-ECFR8ea7e78ba47a262/section-95.621. Accessed on Oct. 6, 2022.

NIST SP 800-53, Revision 4, Security Control	Security Control Finding	Control No. *	Risk Rating†
Authenticator Management	Michigan did not adequately implement controls to prevent credential reuse in its MMIS and E&E system.	IA-5	Moderate
Denial of Service Protection	Michigan did not correctly configure its MMIS and E&E system to protect against or limit denial of service attacks.	SC-5	Moderate
Cryptographic Protection	Michigan did not meet FIPS-validated and/or NSA-approved cryptographic protection controls for certain public-facing systems in its MMIS and E&E system.	SC-13	Moderate
Session Authenticity	Michigan did not properly implement controls to protect the authenticity and validity of communications sessions for a public-facing system in its MMIS and E&E system.	SC-23	Moderate
Information System Monitoring	Michigan 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 OIG.

Potential reasons why Michigan 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. Michigan 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, Michigan's procedures for periodically assessing the implementation of the NIST security controls above were not effective. As a result of Michigan not correctly implementing these controls, an attacker could potentially extract parts of sensitive data in client-server communications, access PII and other data contained in related websites, cause a denial-of-service, expose sensitive user documents, and redirect users to malicious websites.

Regarding our email phishing campaign, we sent 234 phishing emails to specific employees and 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 opened emails could be that Michigan's email filtering systems may have prevented the emails from being successfully delivered to the

targeted employees or the targeted employees who received the emails simply did not open them during our campaign. We have shared these results as information only and encouraged Michigan 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 Michigan Department of Health:

- remediate the six 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 the cryptographic configurations of public servers at least annually and adjust if the requirements have changed.

MICHIGAN'S COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments to our draft report, Michigan concurred with our recommendations and stated that they have either remediated or were in process of remediating our findings. Although we have not yet confirmed whether our recommendations were effectively implemented, we are encouraged by Michigan's response and we look forward to receiving and reviewing the supporting documentation through our audit resolution process.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

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

Regarding internal controls that were reviewed during our audit, we identified the component 'Control Activities' as significant to our audit objective.[5] We reviewed various NIST SP 800-53 Revision 4 security controls, including, but not limited to:

- AC-3 Access Enforcement
- AC-6 Least Privilege
- SA-8 Security Engineering Principles
- SC-8 Transmission Confidentiality and Integrity
- SC-23 Session Authenticity
- SI-2 Flaw Remediation
- SI-10 Information Input Validation

Based on our penetration test we assessed the operating effectiveness of these internal controls and identified deficiencies that we believe could affect Michigan's 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 October 20 and ended December 9, 2020, and the simulated phishing campaign began on November 18 and ended December 8, 2020.

For the simulated phishing campaign, Michigan provided us with a list of 234 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. OAS contracted with XOR to conduct the penetration test of the Michigan 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

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

against a subset of the Michigan Medicaid agency's employees. OAS 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 Michigan MMIS and E&E system. To accomplish our objectives, OIG and Michigan prepared the ROE document that outlined the general rules, logistics, and expectations for the penetration test. Michigan officials provided a signed ROE document indicating that Michigan agreed with the rules to be followed during our testing.

In October 2020, we began reconnaissance and scope verification of network subnets owned, operated, and maintained by Michigan. 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 Michigan had implemented appropriate controls to detect and prevent successful phishing campaigns and to determine whether Michigan personnel were adequately trained to recognize and appropriately respond to such malicious emails. Michigan identified for us the employees who would be subject to XOR's simulated phishing campaign. The campaign was designed to send a phishing email to the 234 Michigan personnel identified containing a web link to a malicious website that, when accessed, would redirect the user to a server within the HHS OIG Cyber Range that would attempt to run code in the user's web browser and deploy more code onto the system, allowing for remote access by the penetration testers.[6]

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.

[6] The HHS/OIG Cyber Range is a virtual private cloud solution to support IT auditing and assessment responsibilities. It is hosted on top of 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 which 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.[7] 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 launching attacks against a system.

[7] 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

FEDERAL REGULATIONS

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

> (1) ADP System Security Requirement.[8] 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,*** states:

CM-6 CONFIGURATION SETTINGS (Page F-70)

Control: The organization:

a. Establishes and documents configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements;

b. Implements the configuration settings;

c. Identifies, documents, and approves any deviations from established configuration settings for [*Assignment: organization-defined information system components*] based on [*Assignment: organization-defined operational requirements*]; and

d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Supplemental Guidance: Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy,

[8] 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.

file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baseline.

Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Common secure configurations include the United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems. Related controls: AC-19, CM-2, CM-3, CM-7, SI-4.

IA-5 AUTHENTICATOR MANAGEMENT (Page F-95)

Control: The organization manages information system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;

b. Establishing initial authenticator content for authenticators defined by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

e. Changing default content of authenticators prior to information system installation;

f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

g. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*];

h. Protecting authenticator content from unauthorized disclosure and modification;

i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and

j. Changing authenticators for group/role accounts when membership to those accounts changes.

Supplemental Guidance: When individuals have accounts on multiple information systems, there is the risk that the compromise of one account may lead to the compromise of other accounts if individuals use the same authenticators. Possible alternatives include, for example: (i) having different authenticators on all systems; (ii) employing some form of single sign-on mechanism; or (iii) including some form of one-time passwords on all systems.

SC-5 DENIAL OF SERVICE PROTECTION (page F-187)

Control: The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards].

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect information system components on internal organizational networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks.

SC-13 CRYPTOGRAPHIC PROTECTION (page F-196)

Control: The information system implements organization-defined cryptographic uses and type of cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Supplemental Guidance: Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography).

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 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]].

APPENDIX D: MICHIGAN'S RESPONSE

STATE OF MICHIGAN
DEPARTMENT OF HEALTH AND HUMAN SERVICES
LANSING

GRETCHEN WHITMER
GOVERNOR

ELIZABETH HERTEL
DIRECTOR

January 26, 2022

Ms. Tamara Lilly
Assistant Inspector General for Cybersecurity & Operations
330 Independence Avenue, SW
Room 5700, Cohen Building
Washington, DC 20201

Re: Report Number A-18-20-08004

Dear Ms. Lilly:

Enclosed is the Michigan Department of Health and Human Services response to the draft report entitled *"Michigan MMIS and E&E Systems Security Controls Were Generally Effective, but Some Improvements Are Needed"* that covered the period of October 1, 2020 to December 31, 2020.

We appreciate the opportunity to review and comment on the report before it is released. If you have any questions regarding this response, please refer them to Pam Myers at Myersp3@michigan.gov or 517-230-4879.

Sincerely,

Elizabeth Hertel

Elizabeth Hertel

EH:wb

Enclosure

333 SOUTH GRAND AVENUE • PO BOX 30195 • LANSING, MICHIGAN 48909
www.michigan.gov/mdhhs • 517-241-3740

Michigan MMIS and E&E Systems Security Controls Were Generally Effective, but Some Improvements Are Needed
(A-18-20-08004)

Finding:

The Michigan Medicaid Management Information System (MMIS) and Eligibility and Enrollment Systems (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. In addition, we estimated that the level of sophistication required to compromise the 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 Michigan's detection controls to better identify cyberattacks against its MMIS and E&E system and respond appropriately.

Recommendations:

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

- remediate the six 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 the cryptographic configurations of public servers at least annually and adjust if the requirements have changed.

Michigan Department of Health and Human Services (MDHHS) Response:

MDHHS agrees with the recommendations.

- All six security control findings have been remediated except for the low-risk item identified. That exception will be remediated by April 1, 2023.
- NIST SP 800-53 controls are already covered as part of the MDHHS' annual ACA/3rd party audit.
- MDHHS will work with its partners at the Department of Technology, Management, and Budget to incorporate a scan of cryptographic modules into its annual processes.