Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

ALABAMA MMIS AND E&E SYSTEM SECURITY CONTROLS WERE ADEQUATE, 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 2024
A-18-22-09010

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: March 2024
Report No. A-18-22-09010

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: (1) whether security controls in operation for Alabama 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 Alabama's MMIS and E&E system or its data, and (3) Alabama'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 the Alabama MMIS and E&E system from November through December 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 Alabama personnel in December 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 Alabama.

Alabama MMIS and E&E System Security Controls Were Adequate, but Some Improvements Are Needed

What OIG Found

The Alabama MMIS and E&E system had adequate security controls in place to prevent our simulated cyberattacks from resulting in a successful compromise; however, we found six security controls required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, that could be improved to better prevent certain cyberattacks.

In addition, we estimated that an adversary would need a moderate level of sophistication to compromise the Alabama MMIS and E&E system. Finally, Alabama demonstrated that it has implemented adequate controls to detect and block phishing emails sent from a known malicious IP address. However, improvements to its detection controls are needed to better identify certain web application cyberattacks.

Alabama did not effectively implement some security controls because, in part, its vulnerability scanning tools did not identify the flaws and vulnerabilities we discovered in its systems. Additionally, Alabama did not adequately follow secure coding practices during their software development lifecycle and remediate vulnerabilities before deployment to Alabama's production systems. As a result of Alabama not effectively implementing security controls or identifying vulnerabilities, an attacker could potentially launch certain cyberattacks against the Alabama MMIS and E&E system to remotely execute malicious code on a computer or redirect users to malicious websites. Such cyberattacks could facilitate an attacker's ability to get initial unauthorized access to an Alabama system and potentially allow them to move deeper into the network and/or extract sensitive information such as Personal Health Information.

What OIG Recommends and Alabama Comments

We made a series of recommendations for Alabama to improve its security controls over its MMIS and E&E system, including that it require its developers to follow secure coding best practice requirements.

Alabama concurred with our recommendations and stated that it has mitigated or has developed plans to mitigate the findings we identified. Although we have not yet confirmed the changes Alabama described in its comments, we commend Alabama for its ongoing efforts to improve the overall security posture of its MMIS and E&E system environments.

The full report can be found on the OIG website

TABLE OF CONTENTS

INTRODUCTION 1

Why We Did This Audit 1

Objectives 1

Background 1

How We Conducted This Audit 3

FINDINGS 3

RECOMMENDATIONS 5

ALABAMA COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE 6

APPENDICES

A: Audit Scope and Methodology 7

B: Tools We Used to Conduct the Audit 10

C: Federal Requirements 11

D: Alabama Comments 13

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]

As part of this body of work, we conducted a penetration test of the Alabama Medicaid Agency's (Alabama's) MMIS and E&E system in accordance with guidelines outlined by the National Institute of Standards and Technology (NIST).[2] This is part of a series of audits of other MMIS and E&E systems in other states.

OBJECTIVES

Our objectives were to determine:

- whether security controls in operation for Alabama's 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 Alabama MMIS and E&E system or its data, and
- Alabama'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 (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 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 the enrollment of people between 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) sought by cyber criminals and foreign adversaries for financial gain, to sabotage State systems, or both.

Alabama Medicaid Agency is responsible for administering Alabama's State Medicaid program. The Medicaid program covered over 25 percent of all Alabama citizens at some point during FY 2021, including nearly 54 percent of all children. In 2021, Alabama's Medicaid expenditures were $7.671 billion for which they received $5.693 billion in federal matching funds to cover the cost.[3]

Alabama outsources the operations and maintenance of its MMIS to a contractor. The Alabama MMIS is composed of different software components which are engineered to enable ease of use, development, and maintainability. It is divided into different subsystems supporting business processes of the Alabama Medicaid Agency, such as case management, claims processing, and Medicaid eligibility verification. The Eligibility and Enrollment (E&E) system is separate from the MMIS. It is operated and managed in house by the Alabama Medicaid Agency and provides eligibility data to the Alabama MMIS system. Alabama has provided an online Medicaid application system to its residents since 2004. In 2017, Alabama launched a multi-year effort to replace its current legacy MMIS with a modern suite of systems.

[3] Alabama Medicaid Agency's Annual Report for Fiscal Year 2021.

HOW WE CONDUCTED THIS AUDIT

We conducted a penetration test audit of the Alabama MMIS and E&E system from November 7 through December 16, 2022. 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 against state employees and contractors that access the MMIS and E&E system. Political appointees were excluded. Additionally, we interviewed Alabama's officials and contractors to understand the security framework applicable to the Alabama MMIS and E&E system and to understand the reasons for control gaps we identified.

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

We provided detailed information about our preliminary findings to Alabama in advance of issuing our draft reports.

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 Alabama MMIS and E&E system had adequate security controls in place to prevent our simulated cyberattacks from resulting in a successful compromise; however, we found six security controls that could be improved to better prevent certain cyberattacks. In addition, we estimated that an adversary would need a moderate level of sophistication to compromise the MMIS and E&E system.[4] At this level, an adversary would need a moderate level of expertise,

[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 Oct. 2, 2023.

with moderate resources and opportunities to support multiple successful coordinated attacks. Finally, Alabama demonstrated that it has implemented adequate controls to detect and block phishing emails sent from a known malicious IP address. However, improvements to its detection controls are needed to better identify certain web application cyberattacks.

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 information technology (IT) systems and information processing.[5]

Alabama did not effectively implement the following Federal NIST Special Publication (SP) 800-53, Revision 4, security controls, as shown in the table below.

Table: MMIS and E&E System Security Control Findings

NIST SP 800-53, Revision 4, Security Control	Security Control Finding	Control No*	Risk Rating†
Information Flow Enforcement	Alabama did not restrict access to a public-facing system that was intended for internal employee access.	AC-4	High
Transmission Confidentiality and Integrity	Alabama did not effectively implement website protections to ensure that information transmitted to four of its systems was protected.	SC-8	Moderate
Flaw Remediation	Alabama did not install six security updates in its MMIS and E&E system.	SI-2	Moderate
Information Input Validation	Alabama did not enforce adequate input validation controls to properly sanitize or verify information system input for one public-facing system.	SI-10	Moderate
Error Handling	Alabama did not prevent one of its systems from revealing system-generated error information that could	SI-11	Moderate

[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 Oct. 2, 2023.

	be used to facilitate a cyberattack by adversaries.		
Authenticator Management	Alabama did not prevent its MMIS and E&E system from disclosing credential information to client web browsers.	IA-5	Low

[*] 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.

Alabama failed to correctly implement these security controls because its developers did not adequately follow secure coding practices during their software development lifecycle and remediate vulnerabilities before deployment to Alabama's production systems.[6] Additionally, the security scanning tools that Alabama utilized did not detect certain vulnerabilities so that they knew to remediate them. As a result of Alabama not effectively implementing these controls or identifying vulnerabilities, an attacker could potentially launch certain cyberattacks against the Alabama MMIS and E&E system to remotely execute malicious code on a computer or redirect users to malicious websites. Such cyberattacks could facilitate an attacker's ability to get initial unauthorized access to an Alabama system and potentially allow them to move deeper into the network and/or extract sensitive information such as PHI.

Regarding our email phishing campaign, the XOR penetration testers sent a phishing email to 772 Alabama employees and contractors using a known malicious IP address and determined that none of the emails were opened. The reason for the zero-open rate is that Alabama's email filtering systems successfully prevented the emails from being successfully delivered to targeted employees because they were sent from a known malicious IP address. We have shared these results as information only and encouraged Alabama 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 Alabama Medicaid Agency:

- remediate the six control findings OIG identified;
- evaluate its current vulnerability scanning tools and update if necessary in order to better detect system flaws (e.g., common web server vulnerabilities) in its MMIS and E&E system and software components;

[6] NIST SP 800-218 *Secure Software Development Framework* refers to following secure coding standards.

- require its developers to follow secure coding standards and best practices, at a minimum, such as those recommended by NIST SP 800-218 or the Open Web Application Security Project (OWASP), when developing web applications;

- implement procedures to periodically verify that its developers are adhering to secure coding standards and remediating vulnerabilities before releasing code to production; and

- perform more robust technical testing of web-facing systems that includes the emulation of an adversary's tactics and techniques on a defined reoccurring basis in order to better assess the effectiveness of NIST 800-53 controls.

ALABAMA COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments to our draft report, Alabama concurred with our recommendations and stated that it has mitigated or has developed plans to mitigate the control findings we identified. Alabama also stated that it has developed its vulnerability management plan to better implement security controls surrounding vulnerability monitoring, developer testing, and flaw remediation. Although we have not yet confirmed the changes Alabama described in its response, we commend Alabama for its ongoing efforts to improve the overall security posture of its MMIS and E&E system environments. Alabama's written comments are included in their entirety as Appendix D.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

The penetration test focused on public IP addresses and web application URLs related to the Alabama MMIS and E&E system, as specified within the ROE document. Alabama 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 did not assess all internal control components and principles. We only assessed control activities specific to IT general controls and application controls for the Alabama MMIS and E&E system. Our penetration test assessed the operating effectiveness of select IT general and application controls. We identified deficiencies that we believe could affect Alabama's ability to detect, or effectively prevent certain cyberattacks. The IT general and application control deficiencies we identified are listed in the table in the Findings section of this report. However, the penetration test we performed may not have disclosed all IT general and application control deficiencies that may have existed at the time of this audit.[7]

We performed our work remotely. Penetration testing began on November 7, 2022, and ended December 16, 2022, and the simulated phishing campaign took place in December 2022. For the simulated phishing campaign, Alabama provided us with a list of 722 email addresses. This list included all employees except for political appointees. We sent phishing emails to the provided 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 Alabama 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 list of email addresses provided by Alabama. 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 Alabama MMIS and E&E system. To accomplish our objectives, OIG and Alabama prepared the ROE document that outlined the general rules, logistics, and expectations for the penetration test. Alabama officials provided a signed ROE document indicating that it agreed with the rules to be followed during our testing.

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

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 2022, XOR conducted a simulated phishing attack to determine whether Alabama had implemented appropriate controls to detect and prevent successful phishing campaigns and to determine whether Alabama personnel were adequately trained to recognize and appropriately respond to such malicious emails. The campaign was designed to send a phishing email containing a web link to a website that, if accessed, would redirect the user to a server within the HHS OIG Cyber Range.[8] Once the user was redirected, the website would attempt to

[8] 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.

run code in the user’s web browser and deploy more code onto the 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.

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.[9] 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.

[9] 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

CMS Acceptable Risk Safeguards (ARS)

45 CFR § 95.621(f)(3) – Automatic Data Processing Equipment and Services – Conditions for Federal Financial Participation.

45 CFR § 164.308 (a)(1)(i) – Subpart C—Security Standards for the Protection of Electronic Protected Health Information, Administrative safeguards. Standard: Security management process.

Federal Information Processing Standard (FIPS) 140-3 – Security Requirements for Cryptographic Modules.

National Institute of Standards and Technology (NIST) SP 800-44, Version 2, *Guidelines on Securing Public Web Servers.*

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

(1) ADP System Security Requirement.[10] 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*:

AC-4 Information Flow Enforcement

Control: Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].

IA-5 AUTHENTICATOR MANAGEMENT

Control: Manage system authenticator by:

a. verifying, as part of the initial authenticator distribution, the identity of the

[10] 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.

individual, group, role, service, or device receiving the authenticator;

b. establishing initial authenticator content for any authenticators issued 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 or compromised or damaged authenticators, and for revoking authenticators;
e. changing default authenticators prior to first use;
f. changing or refreshing authenticators [*Assignment: organization-defined time period by authenticator type*] or when [*Assignment: organization-defined events*] occur;
g. protecting authenticator content from unauthorized disclosure and modification;
h. requiring individuals to take, and having devices implement, specific controls to protect authenticators; and
i. changing authenticators for group or role accounts when membership to those accounts changes.

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Control: Protect the [*Selection (one or more): confidentiality; integrity*] of transmitted information.

SI-2 FLAW REMEDIATION

Control:

a. Identify, report, and correct system flaws;
b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Install security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates; and
d. Incorporate flaw remediation into the organizational configuration management process.

SI-10 INFORMATION INPUT VALIDATION

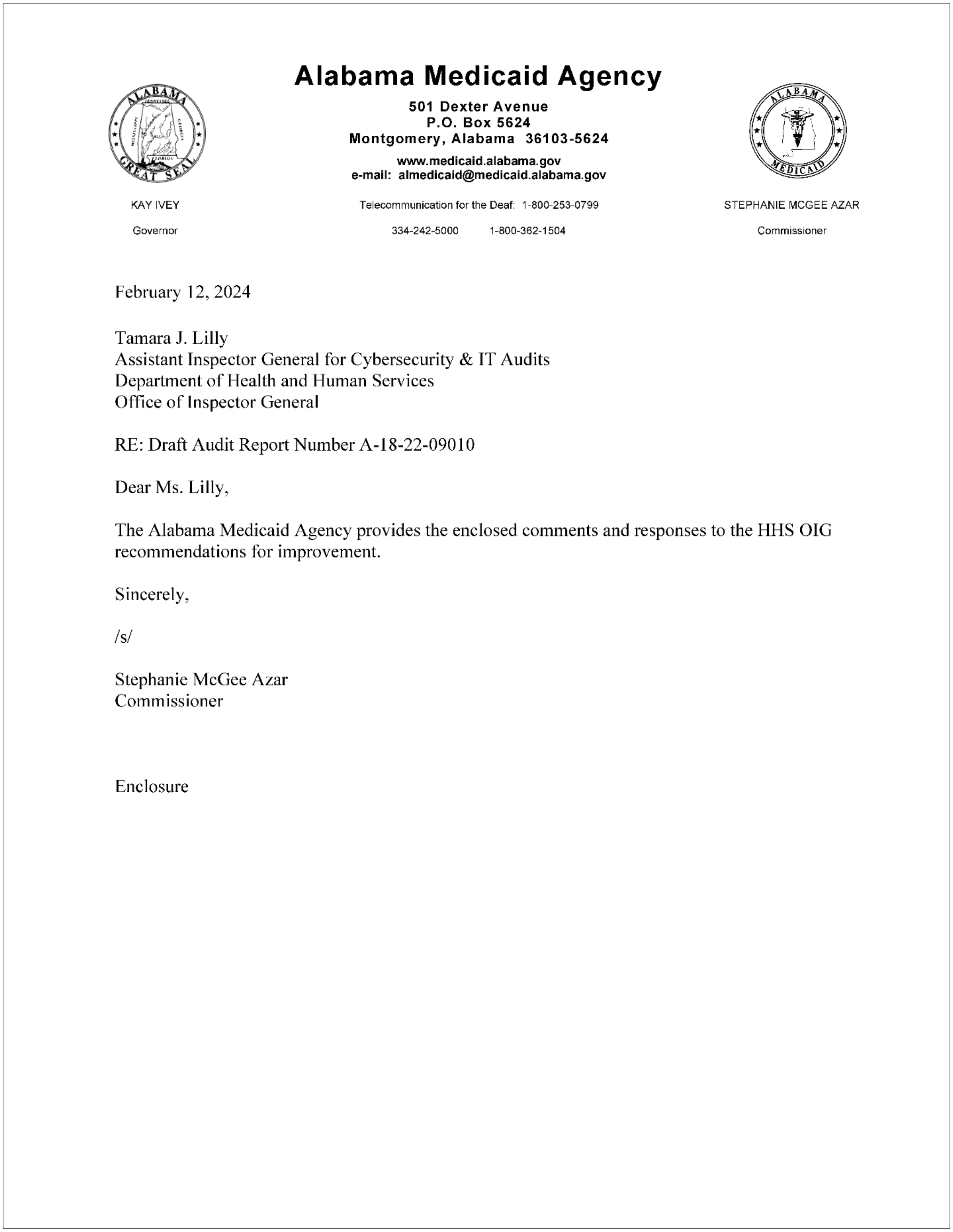
Control: Check the validity of the following information inputs: [*Assignment: organization-defined information inputs to the system*].

SI-11 ERROR HANDLING

Control:

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and
b. Reveal error messages only to [*Assignment: organization-defined personnel or roles*].

APPENDIX D: ALABAMA COMMENTS



Alabama Medicaid Agency

501 Dexter Avenue
P.O. Box 5624
Montgomery, Alabama 36103-5624

www.medicaid.alabama.gov
e-mail: almedicaid@medicaid.alabama.gov

KAY IVEY	Telecommunication for the Deaf: 1-800-253-0799	STEPHANIE MCGEE AZAR
Governor	334-242-5000 1-800-362-1504	Commissioner

February 12, 2024

Tamara J. Lilly
Assistant Inspector General for Cybersecurity & IT Audits
Department of Health and Human Services
Office of Inspector General

RE: Draft Audit Report Number A-18-22-09010

Dear Ms. Lilly,

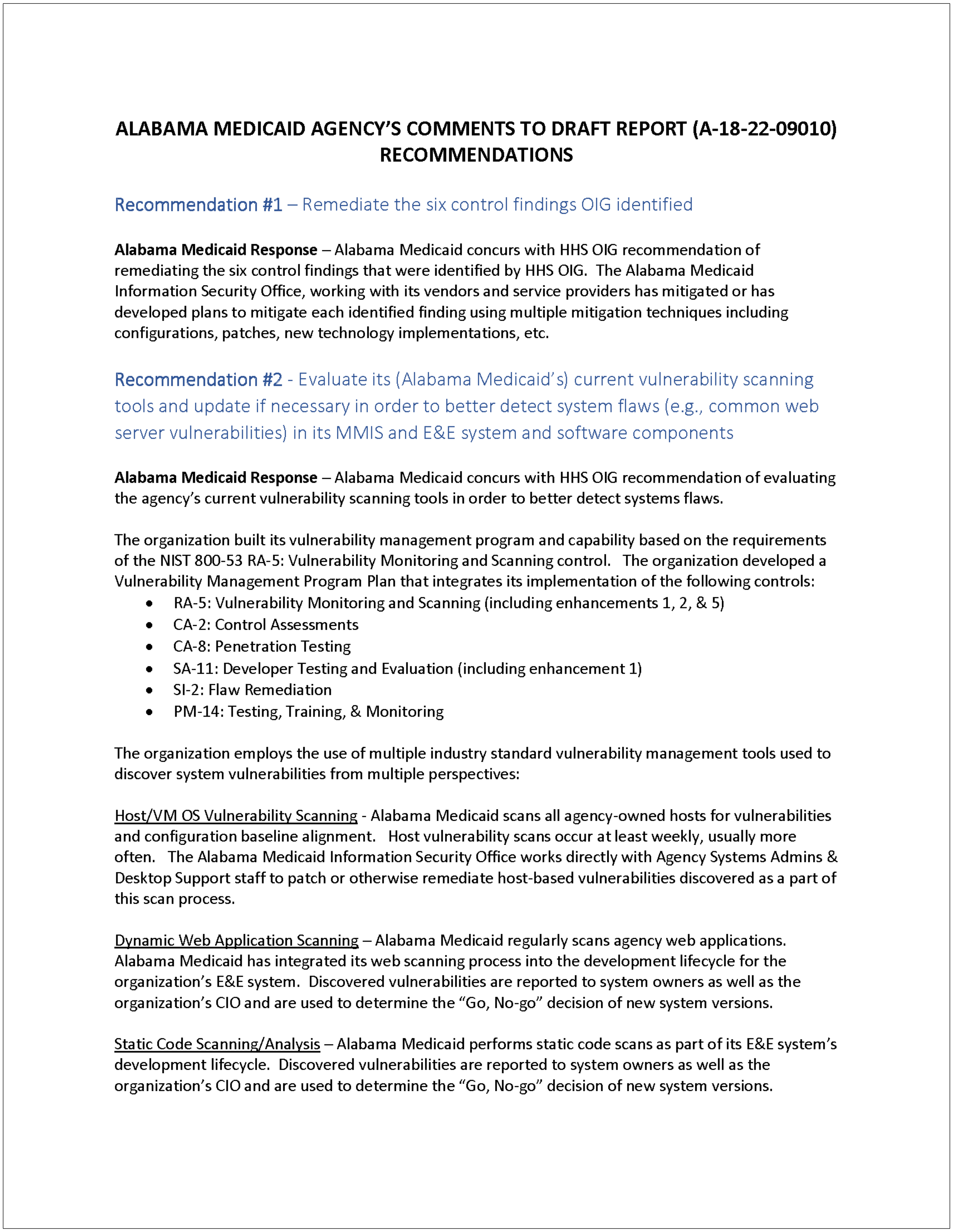
The Alabama Medicaid Agency provides the enclosed comments and responses to the HHS OIG recommendations for improvement.

Sincerely,

/s/

Stephanie McGee Azar
Commissioner

Enclosure



ALABAMA MEDICAID AGENCY'S COMMENTS TO DRAFT REPORT (A-18-22-09010) RECOMMENDATIONS

Recommendation #1 – Remediate the six control findings OIG identified

Alabama Medicaid Response – Alabama Medicaid concurs with HHS OIG recommendation of remediating the six control findings that were identified by HHS OIG. The Alabama Medicaid Information Security Office, working with its vendors and service providers has mitigated or has developed plans to mitigate each identified finding using multiple mitigation techniques including configurations, patches, new technology implementations, etc.

Recommendation #2 - Evaluate its (Alabama Medicaid's) current vulnerability scanning tools and update if necessary in order to better detect system flaws (e.g., common web server vulnerabilities) in its MMIS and E&E system and software components

Alabama Medicaid Response – Alabama Medicaid concurs with HHS OIG recommendation of evaluating the agency's current vulnerability scanning tools in order to better detect systems flaws.

The organization built its vulnerability management program and capability based on the requirements of the NIST 800-53 RA-5: Vulnerability Monitoring and Scanning control. The organization developed a Vulnerability Management Program Plan that integrates its implementation of the following controls:

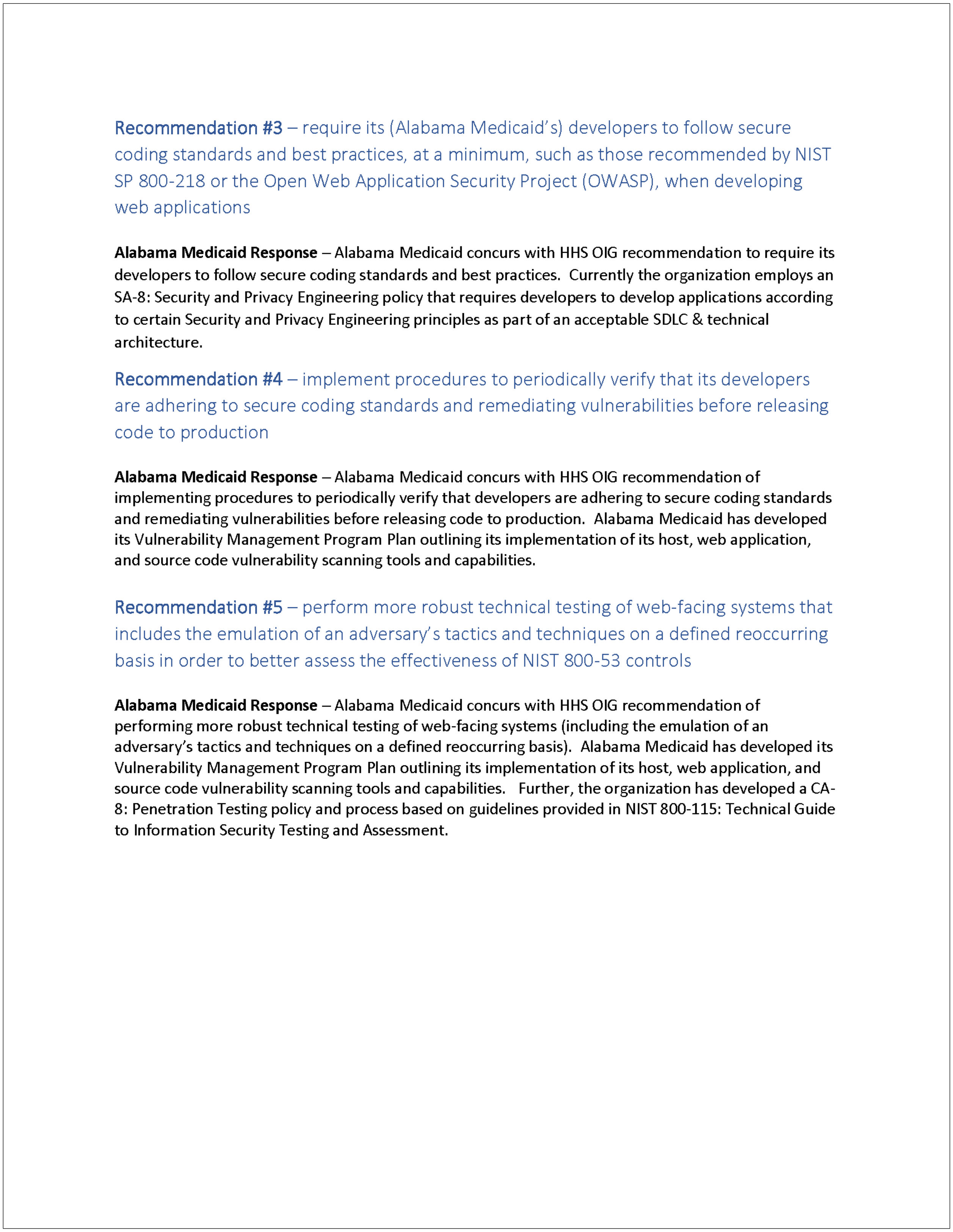
- RA-5: Vulnerability Monitoring and Scanning (including enhancements 1, 2, & 5)
- CA-2: Control Assessments
- CA-8: Penetration Testing
- SA-11: Developer Testing and Evaluation (including enhancement 1)
- SI-2: Flaw Remediation
- PM-14: Testing, Training, & Monitoring

The organization employs the use of multiple industry standard vulnerability management tools used to discover system vulnerabilities from multiple perspectives:

Host/VM OS Vulnerability Scanning - Alabama Medicaid scans all agency-owned hosts for vulnerabilities and configuration baseline alignment. Host vulnerability scans occur at least weekly, usually more often. The Alabama Medicaid Information Security Office works directly with Agency Systems Admins & Desktop Support staff to patch or otherwise remediate host-based vulnerabilities discovered as a part of this scan process.

Dynamic Web Application Scanning – Alabama Medicaid regularly scans agency web applications. Alabama Medicaid has integrated its web scanning process into the development lifecycle for the organization's E&E system. Discovered vulnerabilities are reported to system owners as well as the organization's CIO and are used to determine the "Go, No-go" decision of new system versions.

Static Code Scanning/Analysis – Alabama Medicaid performs static code scans as part of its E&E system's development lifecycle. Discovered vulnerabilities are reported to system owners as well as the organization's CIO and are used to determine the "Go, No-go" decision of new system versions.



Recommendation #3 – require its (Alabama Medicaid's) developers to follow secure coding standards and best practices, at a minimum, such as those recommended by NIST SP 800-218 or the Open Web Application Security Project (OWASP), when developing web applications

Alabama Medicaid Response – Alabama Medicaid concurs with HHS OIG recommendation to require its developers to follow secure coding standards and best practices. Currently the organization employs an SA-8: Security and Privacy Engineering policy that requires developers to develop applications according to certain Security and Privacy Engineering principles as part of an acceptable SDLC & technical architecture.

Recommendation #4 – implement procedures to periodically verify that its developers are adhering to secure coding standards and remediating vulnerabilities before releasing code to production

Alabama Medicaid Response – Alabama Medicaid concurs with HHS OIG recommendation of implementing procedures to periodically verify that developers are adhering to secure coding standards and remediating vulnerabilities before releasing code to production. Alabama Medicaid has developed its Vulnerability Management Program Plan outlining its implementation of its host, web application, and source code vulnerability scanning tools and capabilities.

Recommendation #5 – perform more robust technical testing of web-facing systems that includes the emulation of an adversary's tactics and techniques on a defined reoccurring basis in order to better assess the effectiveness of NIST 800-53 controls

Alabama Medicaid Response – Alabama Medicaid concurs with HHS OIG recommendation of performing more robust technical testing of web-facing systems (including the emulation of an adversary's tactics and techniques on a defined reoccurring basis). Alabama Medicaid has developed its Vulnerability Management Program Plan outlining its implementation of its host, web application, and source code vulnerability scanning tools and capabilities. Further, the organization has developed a CA-8: Penetration Testing policy and process based on guidelines provided in NIST 800-115: Technical Guide to Information Security Testing and Assessment.