Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

SOUTH CAROLINA 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-18-22-09005

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-18-22-09005

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

South Carolina MMIS and E&E System Security Controls Were Adequate, 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: (1) whether security controls in operation at South Carolina's MMIS and E&E system environments were effective in preventing certain cyberattacks, (2) the likely level of sophistication or complexity an attacker needs to compromise the South Carolina Medicaid System or its data, and (3) South Carolina'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 South Carolina MMIS and E&E system from April through July 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 targeting South Carolina personnel. We contracted with XOR Security, LLC (XOR), to conduct the penetration test. We closely oversaw the work performed by XOR, and the assessment was performed in accordance with agreed upon Rules of Engagement among OIG, XOR, and South Carolina.

What OIG Found

The South Carolina MMIS and E&E system had adequate security controls in place to prevent our simulated cyberattacks from resulting in a successful compromise; however, we identified security controls that could be further enhanced to better prevent certain cyberattacks. Specifically, South Carolina did not correctly implement four security controls required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5.

We estimated that an adversary would need at least a moderate level of sophistication to compromise the South Carolina MMIS and E&E system. At this level, an adversary would need a moderate level of expertise with moderate resources and opportunities to support multiple successful coordinated attacks. Additionally, although penetration testers were able to exploit an application-level vulnerability that was not blocked by network firewalls or other mechanisms, testers were not able to gain access to any systems or networks. We shared this information with South Carolina, who later provided us adequate evidence of the remediation of the security control findings related to Flaw Remediation (SI-2) and Error Handling (SI-11).

What OIG Recommends and South Carolina Comments

We recommend that South Carolina remediate the remaining two control findings (SI-10 and SC-8) in accordance with government standards and periodically test the effectiveness of these controls.

South Carolina did not indicate concurrence or nonconcurrence with our recommendation; however, it indicated that it took corrective action to address the two control findings. Although we have not yet confirmed South Carolina's remediation of the two control findings identified in our report, we commend South Carolina's 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

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 South Carolina Department of Health and Human Services (SCDHHSs) 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 SCDHHS 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 SCDHHS MMIS and E&E system or its data, and
- SCDHHS'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 cyber 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.

SCDHHS is responsible for administering South Carolina's State Medicaid program. SCDHHS contracts with a university in South Carolina and other commercial partners to operate and maintain systems related to Medicaid enrollment, claims, and reporting including some mainframe components.

Since 2013, South Carolina consumers have been able to apply for Medicaid benefits through an online portal that is a part of the SCDHHS MMIS and E&E system. The portal interfaces with the federally-facilitated Marketplace and other SCDHHS MMIS and E&E system components. SCDHHS was undergoing a transition to a new MMIS during our audit period.

HOW WE CONDUCTED THIS AUDIT

We conducted a penetration test audit of the SCDHHS MMIS and E&E system from April through July 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 against a limited number of SCDHHS personnel in April 2022. Additionally, we interviewed SCDHHS officials and contractors to understand the security framework applicable to the SCDHHS MMIS and E&E system.

To assist us with the penetration test, we relied on the work of specialists. Specifically, OIG contracted with XOR Security, LLC (XOR), to assist in conducting the penetration test of the SCDHHS 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 March 2022 by OIG, XOR, and SCDHHS.

We provided detailed information about our preliminary findings to SCDHHS 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 SCDHHS MMIS and E&E system had adequate security controls in place to prevent our simulated cyberattacks from resulting in a successful compromise; however, we identified security controls that could be further enhanced to better prevent certain cyberattacks. During the penetration test, XOR penetration testers were able to exploit an application-level vulnerability that was not blocked by SCDHHS network firewalls or other mechanisms but were not able to gain access to any systems or networks. In addition, we estimated that an adversary would need at least a moderate level of sophistication to compromise the SCDHHS MMIS and E&E system.[3] At this level, an adversary would need a moderate level of expertise with moderate resources and opportunities to support multiple successful coordinated attacks. Lastly, we determined that the SCDHHS MMIS and E&E system design provides the ability to protect, detect, and respond to cyberattacks using network firewalls and other mechanisms for analyzing and monitoring traffic.

[3] 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 Oct. 12, 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 information technology (IT) systems and information processing.[4] SCDHHS did not effectively implement the following Federal NIST Special Publication (SP) 800-53, Revision 5, security controls in a subset of its MMIS and E&E system, detailed in the table below.

Table: MMIS and E&E System Security Control Findings

NIST SP 800-53, Revision 5, Security Control	Security Control Finding	Control No*	Risk Rating†
Flaw Remediation	SCDHHS did not properly identify, report, and correct system flaws in its MMIS and E&E system.	SI-2	High
Information Input Validation	SCDHHS did not properly sanitize or verify information system input for a public-facing system in its MMIS and E&E system.	SI-10	Moderate
Error Handling	SCDHHS did not properly configure the handling of internal error messages on a public-facing system.	SI-11	Low
Transmission Confidentiality and Integrity	SCDHHS did not implement sufficient website protections to ensure that information transmitted to its systems was protected.	SC-8	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 5.

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

Potential reasons why SCDHHS did not implement these security controls correctly may be that system administrators were not aware of government standards or industry best practices that require securely designing, configuring, and testing systems before deployment to production and implementing ongoing flaw detection and remediation. As a result of this, an attacker could potentially execute remote code on the system, gather sensitive system details, intercept data being sent from users of the application, and redirect users to malicious websites which facilitates an attacker's ability to gain initial unauthorized access and potentially move deeper into the network, thereby exposing critical systems and data to compromise.

[4] 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. 12, 2023.

We shared this information with SCDHHS, who later provided us adequate evidence of the remediation of the security control findings related to Flaw Remediation (SI-2) and Error Handling (SI-11).

Regarding our email phishing campaign, we sent a phishing email to 1,534 SCDHHS employees and contractors. We determined that 134 emails (9 percent) were opened. Of these 134 emails, 5 recipients (0.3 percent of total emails) clicked an embedded web link according to the data reported by our automated tool. Only one of the clicks resulted in a successful connection to a test web site we controlled; however, this click may have been generated by SCDHHS email protection tools and not from the actual user. The reason for the low open-and-click rate could be that SCDHHS uses email defense tools that block the delivery of some malicious emails and inspects any attachments or web links included in suspicious emails within a testing sandbox environment. After the testing, SCDHHS provided evidence that an employee had detected and reported the phishing email to its malware detection teams, which is a desired response. The results of our phishing campaign indicated that adequate security controls did not lead to systemic failures; therefore, we are not making a recommendation concerning this finding. We shared these results with SCDHHS as information-only and encouraged SCDHHS to continue challenging its defenses and employees with increasingly more sophisticated phishing campaigns so they remain prepared for future phishing attacks.

RECOMMENDATION

We recommend that the SCDHHS remediate the remaining two control findings (SI-10 and SC-8) in accordance with government standards and periodically test the effectiveness of these controls.

SOUTH CAROLINA COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments on our draft report, South Carolina did not indicate concurrence or nonconcurrence with our recommendation. However, South Carolina indicated that it took corrective action to address the two control findings. Although we have not yet confirmed South Carolina's remediation of the two control findings identified in our report, we commend South Carolina's ongoing efforts to improve the overall security posture of its MMIS and E&E system environments. South Carolina'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 SCDHHS MMIS and E&E system, as specified within the ROE document. SCDHHS 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 SCDHHS 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 SCDHHS'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.[5]

We performed our work remotely. Penetration testing began on April 1, 2022, and ended July 5, 2022. The simulated phishing campaign was conducted in April 2022. For the simulated phishing campaign, SCDHHS provided us with a list of employee, service account, and contractor email addresses. We sent phishing emails to the 1,534 employee and contractor email addresses on the list.

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 SCDHHS 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 SCDHHS addresses provided by SCDHHS. 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 SCDHHS MMIS and E&E system. To accomplish our objectives, OIG and SCDHHS prepared the ROE document that outlined the general rules, logistics, and expectations for the penetration test. SCDHHS officials signed the ROE document indicating agreement.

Additionally, we reviewed SCDHHS MMIS and E&E system documentation and inquired of SCDHHS officials and contractors about the control framework governing the MMIS and E&E

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

system. We also met with a penetration testing team that SCDHHS had engaged to conduct a penetration test of its non-production systems as part of its CMS certification requirements.

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,
    - hostnames,
    - 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 April 2022, XOR conducted a simulated phishing campaign to determine whether SCDHHS had implemented appropriate controls to detect and prevent successful phishing campaigns and to determine whether SCDHHS personnel were adequately trained to recognize and appropriately respond to such malicious emails. This campaign targeted 1,534 employee and contractor email addresses provided by SCDHHS. 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.[6] Once the user was redirected, the website 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.

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 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 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

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 5, *Security and Privacy Controls for Information Systems and Organizations*:

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

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

Discussion: Protecting the confidentiality and integrity of transmitted information applies to internal and external networks as well as any system components that can transmit information, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of information can be accomplished by physical or logical means. Physical protection can be achieved by using protected distribution systems. A protected distribution system is a wireline or fiber-optics telecommunications system that includes terminals and adequate electromagnetic, acoustical, electrical, and physical controls to permit its use for the unencrypted transmission of classified information. Logical protection can be achieved by employing encryption techniques.

Organizations that rely on commercial providers who offer transmission services as commodity services rather than as fully dedicated services may find it difficult to obtain the necessary assurances regarding the implementation of needed controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality or integrity services are available in standard, commercial telecommunications service packages. If it is not feasible to obtain the necessary controls and assurances of control

[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.

effectiveness through appropriate contracting vehicles, organizations can implement appropriate compensating controls.

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*].

Discussion: Checking the valid syntax and semantics of system inputs—including character set, length, numerical range, and acceptable values—verifies that inputs match specified definitions for format and content. For example, if the organization specifies that numerical values between 1-100 are the only acceptable inputs for a field in a given application, inputs of "387," "abc," or "%K%" are invalid inputs and are not accepted as input to the system. Valid inputs are likely to vary from field to field within a software application. Applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the corrupted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing them to interpreters prevents the content from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevents attacks such as cross-site scripting and a variety of injection attacks.

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].

Discussion: Organizations consider the structure and content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes stack traces and implementation details; erroneous logon attempts with passwords mistakenly entered as the username; mission or business information that can be derived from, if not stated explicitly by, the information recorded; and personally identifiable information, such as account numbers, social security numbers, and credit card numbers. Error messages may also provide a covert channel for transmitting information.

APPENDIX D: SOUTH CAROLINA COMMENTS

SOUTH CAROLINA DEPARTMENT OF HEALTH AND HUMAN SERVICES
Healthy Connections MEDICAID

Henry McMaster GOVERNOR
Robert M. Kerr DIRECTOR
P.O. Box 8206 • Columbia, SC 29202
www.scdhhs.gov

January 22, 2024

Tamara J. Lilly
Assistant Inspector General for Cybersecurity & IT Audits
Department of Health and Human Services
Office of Inspector General
330 Independence Avenue, SW
Washington, DC 20201

Re: Report Number: A-18-22-09005

Dear Ms. Lilly:

The South Carolina Department of Health and Human Services (SCDHHS) appreciates the opportunity to respond to the U.S. Department of Health and Human Services, Office of Inspector General (OIG), draft report *South Carolina MMIS and E&E System Security Controls Were Adequate, but Some Improvements Are Needed* provided to us December 5, 2023. The SCDHHS concurs with the MMIS and E&E Security Control Findings highlighted on page 4 of the report. As indicated on page 5 of the report, SCDHHS provided adequate evidence of the remediation of the security control findings related to Flaw Remediation (SI-2) and Error Handling (SI-11). The table below reflects the final two Security Control Findings which SCDHHS has completed the remediation. The security controls were assessed by Deloitte, an independent third-party vendor, May 2023 and will be tested annually by an independent third party.

MMIS and E&E Security Control Findings:

NIST SP 800-53, Revision 5, Security Control	Security Control Finding	Control No	Risk Rating	SCDHHS Remediation
Information Input Validation	SCDHHS did not properly sanitize or verify information system input for a public-facing system in its MMIS and E&E system.	SI-10	Moderate	Determined to be a false positive. SCDHHS/Clemson Data Center unsuccessfully attempted to reproduce the attack. It was found that the Palo Altos were making the DNS calls rather than the target server. This functionality is a part of the Palo Alto's threat detection mechanism when intercepting traffic. Multiple operating system and attack signature updates have been

				applied to the Palo Altos since this audit.
Transmission Confidentiality and Integrity	SCDHHS did not implement sufficient website protections to ensure that information transmitted to its systems was protected.	SC-8	Low	The affected hosts have been updated to set secure flag on all cookies and enabling HttpOnly property.

If you have any questions or comments about our response, please do not hesitate to contact the SCDHHS Chief Information Officer at (803) 898-0430 or morrison@scdhhs.gov.

Sincerely,

Robert M. Kerr