Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

SOUTH DAKOTA MMIS AND E&E SYSTEM SECURITY CONTROLS WERE PARTIALLY EFFECTIVE AND 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

October 2023
A-18-21-09004

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: October 2023
Report No. A-18-21-09004

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 (MMIS) and Eligibility and Enrollment (E&E) system 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 South Dakota'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 Dakota MMIS and E&E system or its data, and (3) South Dakota'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 South Dakota's MMIS and E&E system from November 2021 through January 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 a limited number of South Dakota personnel in February 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 South Dakota.

South Dakota MMIS and E&E System Security Controls Were Partially Effective and Improvements Are Needed

What OIG Found

The South Dakota MMIS and E&E system had security controls in place that were partially effective 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. South Dakota did not correctly implement six security controls from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

In addition, we estimated that the level of sophistication needed by an adversary to compromise the South Dakota MMIS and E&E system was moderate. At this level, an adversary would need a moderate level of expertise, with moderate resources and opportunities to support a successful attack. Finally, based on the results of our simulated cyberattacks, South Dakota would need to improve its monitoring controls to better detect cyberattacks against its MMIS and E&E system and respond appropriately.

Potential reasons why South Dakota did not implement these security controls correctly may be that system developers and system administrators were not aware of government standards or industry best practices that require securely configured systems or did not correct flaws in systems before deployment to production. Additionally, South Dakota's procedures for periodically assessing the implementation of the NIST security controls above were not effective. As a result of South Dakota not correctly implementing these controls, an attacker could potentially extract sensitive data and PII, impersonate other users, and redirect users to malicious websites.

What OIG Recommends and South Dakota Comments

We recommend that South Dakota remediate the six control findings OIG identified. In written comments on our draft report, South Dakota did not state whether it concurred with our recommendation. Instead, South Dakota stated that it took steps to address five of the six control findings and that it partially implemented the remaining control finding that had a low-risk rating. We have not confirmed that South Dakota implemented these steps. We will validate the actions taken by South Dakota during the audit resolution process.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/182109004.asp.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS AUDIT

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

Specifically, as part of this body of work, we conducted a penetration test of South Dakota's 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 at South Dakota'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 South Dakota MMIS and E&E system or its data, and

- South Dakota'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 system 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 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 that is sought by cyber criminals and foreign adversaries for financial gain, to sabotage State systems, or both.

The South Dakota Department of Social Services administers South Dakota's Government health care delivery system, which includes Medicaid, is the single State agency responsible for developing and administering South Dakota's Medicaid plan. Medicaid is one of the largest healthcare insurers in South Dakota with 16 percent of the population being covered by Medicaid or Children's Health Insurance Program (CHIP) in 2022. More than 64 percent of individuals covered by Medicaid or CHIP are children. In 2022, South Dakota's Medicaid expenditures were $955.27 million in Federal funding.

HOW WE CONDUCTED THIS AUDIT

We conducted a penetration test of South Dakota's MMIS and E&E system from November 2021 through January 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 covered a limited number of South Dakota personnel in February 2022.

To assist us with the penetration test, we relied on the work of specialists. We contracted with XOR Security, LLC (XOR), to assist in conducting the penetration test of the South Dakota 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 November 2021 by OIG, XOR, and South Dakota's Office of Information Security.

We provided detailed documentation about our preliminary findings to South Dakota 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 South Dakota MMIS and E&E system had security controls in place that were partially effective to prevent our simulated cyberattacks from resulting in a successful compromise; however, some of those security controls could be further enhanced to better prevent certain cyberattacks. In addition, we estimated that the level of sophistication needed by an adversary to compromise the South Dakota MMIS and E&E system was moderate.[3] At this level, an adversary would need a moderate level of expertise, with moderate resources and opportunities to support multiple successful coordinated attacks. Finally, based on the results of our simulated cyberattacks, South Dakota would need to improve its monitoring controls to better detect cyberattacks against its MMIS and E&E system and respond appropriately.

State agencies operating MMIS and E&E systems must implement appropriate information security controls based on recognized industry standards or standards governing the security of Federal IT systems and information processing.[4] South Dakota did not correctly implement the

[3] The MITRE Corporation, *How Do You Assess Your Organization's Cyber Threat Level*. Available online at https://apps.dtic.mil/sti/pdfs/AD1137499.pdf. Accessed on September 7, 2022

[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 June 1, 2022.

following Federal NIST Special Publication (SP) 800-53, Revision 4, security categories as shown in the table below.

Table: Weak South Dakota MMIS and E&E System Security Controls

NIST SP 800-53, Revision 4, Security Control	Security Control Finding	Control No.[*]	Risk Rating[†]
Information Input Validation	South Dakota did not properly sanitize or verify information system input for a public-facing system in its MMIS and E&E system.	SI-10	Moderate
Flaw Remediation	South Dakota did not properly identify, report, and correct system flaws in its MMIS and E&E system.	SI-2	Moderate
Error Handling	South Dakota did not implement secure error handling configurations to prevent disclosure of information for its MMIS and E&E system.	SI-11	Low
Monitoring for Information Disclosure	South Dakota did not properly monitor the MMIS and E&E system for evidence of unauthorized disclosure of organizational information.	AU-13	Low
Transmission Confidentiality and Integrity	South Dakota did not properly protect the confidentiality of transmitted information in its MMIS and E&E system.	SC-8	Low
Configuration Settings	South Dakota did not properly establish configuration settings in the MMIS and E&E system that reflect the most restrictive mode consistent with operations requirements.	CM-6	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.

Potential reasons why South Dakota did not implement these security controls correctly may be that system developers and system administrators were not aware of government standards or industry best practices that require securely configured systems or did not correct flaws in systems before deployment to production. Additionally, South Dakota's procedures for periodically assessing the implementation of the NIST security controls above were not effective. As a result of South Dakota not correctly implementing these controls, an attacker could potentially extract sensitive data and PII, impersonate other users, and redirect users to malicious websites which facilitates an attacker’s ability to get a foothold and potentially move laterally through the network, thereby exposing critical systems to attack and compromise.

Regarding our email phishing campaign, we sent 394 phishing emails to specific employees and determined that 8 emails were opened, and the web link embedded in an email was clicked 1 time. This action allowed our penetration test team to successfully execute code within the user’s web browser and perform some basic unauthorized data gathering against the computer. The reason for the low open and click rate could be that South Dakota's email filtering system may have prevented the emails from being successfully delivered to targeted employees, or the targeted employees who received the emails simply did not open them during our campaign. The results of the phishing campaign were not considered systemic and therefore, we are not making a recommendation. We have shared these results as information only and encouraged South Dakota to review its email phishing controls to determine whether any improvements may be helpful.

RECOMMENDATION

We recommend that the South Dakota Department of Social Services remediate the six control findings OIG identified.

SOUTH DAKOTA COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments on our draft report, South Dakota did not state whether it concurred with our recommendation.[5] Instead, South Dakota stated that it took steps to address five of the six control findings and that it partially implemented the remaining control finding that had a low-risk rating. We have not confirmed that South Dakota implemented these steps. We will validate during the audit resolution process. South Dakota’s written comments are included in their entirety as Appendix D.

[5] We removed the second and third recommendations included in our draft report after reviewing additional documentation provided by South Dakota.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

The penetration test focused on both public IP addresses and web application URLs related to the South Dakota MMIS and E&E system, as specified within the ROE document. South Dakota 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 South Dakota 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 South Dakota'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.[6]

We performed our work remotely. Penetration testing began on November 22, 2021, and ended January 21, 2022, and the simulated phishing campaign began on February 1 and ended February 11, 2022. For the simulated phishing campaign, South Dakota provided us with a list of 394 employee email addresses.

METHODOLOGY

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

Our testing focused on the publicly available web applications and infrastructure used to support the South Dakota MMIS and E&E system. To accomplish our objectives, OIG and South Dakota prepared the ROE document that outlined the general rules, logistics, and expectations for the penetration test. South Dakota officials provided a signed ROE document indicating that South Dakota agreed with the rules to be followed during our testing.

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

In November 2021, we began reconnaissance and scope verification of network subnets owned, operated, and maintained by South Dakota. 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 February 2022, XOR conducted a simulated phishing campaign to determine whether South Dakota had implemented appropriate controls to detect and prevent successful phishing campaigns and to determine whether South Dakota personnel were adequately trained to recognize and appropriately respond to such malicious emails. South Dakota provided a list of the employees who would be subject to XOR's simulated phishing campaign. The campaign was designed to send to the 394 South Dakota personnel a phishing email that contained 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.[7]

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

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

APPENDIX B: TOOLS WE USED TO CONDUCT THE AUDIT

Kali Linux

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

Burp Suite Pro

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

GoPhish

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

Cobalt Strike

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

BeEF

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

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

APPENDIX C: FEDERAL REQUIREMENTS

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

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

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

> AU-13 MONITORING FOR INFORMATION DISCLOSURE (page F-52)
>
> Control: The organization monitors [Assignment: organization-defined open-source information and/or information sites] [Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information.
>
> Supplemental Guidance: Open-source information includes, for example, social networking sites. Related controls: PE-3, SC-7.
>
> 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

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

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, 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.

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY (page F-193)

Control: The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.

Supplemental Guidance: This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing protected distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk.

SI-2 FLAW REMEDIATION (page F-215)

Control: The organization:

a. Identifies, reports, and corrects information system flaws;

b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and

d. Incorporates flaw remediation into the organizational configuration management process.

Supplemental Guidance: Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.

SI-10 INFORMATION INPUT VALIDATION (page F-229)

Control: The information system checks the validity of [Assignment: organization-defined information inputs].

Supplemental Guidance: Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software 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 tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

SI-11 ERROR HANDLING (page F-230)

Control: The information system:

a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and

b. Reveals error messages only to [Assignment: organization-defined personnel or roles].

Supplemental Guidance: Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitting information. Related controls: AU-2, AU-3, SC-31.

APPENDIX D: SOUTH DAKOTA COMMENTS

DSS South Dakota Department of Social Services

DEPARTMENT OF SOCIAL SERVICES
DIVISION OF ECONOMIC ASSISTANCE
700 GOVERNORS DRIVE
PIERRE, SD 57501
PHONE: (605) 773-4678
FAX: (605) 773-7183

May 30, 2023

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

RE: A-18-21-09004 Report Recommendation Responses

Dear Ms. Lilly:

Please see below for responses to the recommendations of the draft report *South Dakota MMIS and E&E System Security Controls Were Partially Effective and Improvements are Needed* (A-18-21-09004).

1. **Remediate the six control findings OIG identified**
   Five (5) of the six (6) control findings have been fully remediated. The outstanding control has a low-risk rating and is partially implemented.

2. **Assess the effectiveness of all required NIST SP 800-53 controls according to the organization's defined frequency**
   All NIST SP 800-53 controls are assessed by the State on at least an annual basis and audits are completed by numerous entities including the Social Security Administration, Internal Revenue Service, Centers for Medicare & Medicaid Services, and state-contracted independent 3rd party auditors.

3. **Assess, at least annually, and, if necessary, adjust configurations for its MMIS and E&E public servers management policies and procedures to ensure that public servers do not disclose sensitive information**
   All Bureau of Information and Telecommunications policies and procedures are reviewed and updated annually prior to March 1st, with the last review being completed in March 2023.

We appreciate the opportunity to review and comment on this report before its publication. If you have any questions regarding these responses, please contact me at Samuel.Masten@state.sd.us or (605) 773-4678.

Sincerely,

Samuel Masten

Samuel Masten
Application/Business Project Manager
South Dakota Department of Social Services