Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

UTAH MMIS AND E&E SYSTEM HAD ADEQUATE SECURITY CONTROLS IN PLACE, BUT 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-18-21-09001

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-18-21-09001

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

Utah MMIS and E&E System Had Adequate Security Controls In Place, but Improvements Are Needed

Why OIG Did This Audit

We are conducting a series of audits of State Medicaid Management Information Systems (MMISs) and Eligibility and Enrollment (E&E) systems of selected States to determine how well these systems are protected when subjected to cyberattacks.

Our objectives were to determine whether: (1) security controls in operation at Utah'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 Utah MMIS and E&E system or its data, and (3) Utah'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 Utah MMIS and E&E system from February to March 2021. 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 Utah personnel. 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 Utah.

What OIG Found

The Utah MMIS and E&E system had adequate security controls in place to prevent our simulated cyberattacks from resulting in a successful compromise; however, some of those security controls could be improved to better prevent certain cyberattacks and reduce overall risk. Specifically, Utah did not correctly implement seven security controls required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4. We shared this information with Utah, which provided evidence that four of the security control findings have been remediated.

We estimated that the level of sophistication needed by an adversary to compromise the Utah MMIS and E&E system was significant. At this level, an adversary would need a significant level of expertise through advanced training and persistence to circumvent most of the current security controls. Finally, based on the results of our simulated cyberattacks, Utah demonstrated the ability to detect some attacks and respond appropriately. However, Utah did not detect and prevent other penetration test activities we performed in later phases.

Utah may not have correctly implemented security controls because system administrators were not aware of Government standards or industry best practices that require securely configured systems before deployment to production. Also, Utah's flaw remediation procedures were not consistent with the timeframe defined in the CMS ARS policy for correcting identified security-related information system flaws on production systems. Lastly, there is no requirement from CMS for more frequent penetration testing unless the system is considered a high value asset.

What OIG Recommends and Utah Comments

We recommend that Utah: (1) remediate the remaining three security control findings and (2) revise flaw remediation procedures such that they fully implement the flaw remediation requirements defined in the CMS Acceptable Risk Safeguards.

Utah agreed with our recommendations and stated that it has addressed and remediated the security control findings identified by OIG (first recommendation) and is in the process of addressing our second recommendation. We are encouraged by Utah's actions and we look forward to receiving and reviewing its supporting documentation through our audit resolution process.

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 Utah Department of Health's (Utah's)[2] MMIS and E&E system in accordance with guidelines outlined by the National Institute of Standards and Technology (NIST).[3]

OBJECTIVES

Our objectives were to determine:

- whether security controls in operation for Utah 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 Utah MMIS and E&E system or its data, and
- Utah'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

[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] Subsequent to our audit period, the Department of Health merged with the former Utah Department of Health Services to form the Utah Department of Health & Human Services.

[3] NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment.

State plan. Although the State has considerable flexibility in designing and operating its Medicaid program, it must comply with applicable Federal requirements.

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

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

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

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

At the start of 2021, the Utah Medicaid program served approximately 398,000 residents in the State. Utah's legacy MMIS component facilitates Medicaid functions such as Medicaid care, member eligibility, claims adjudication, and claims payment. During our audit, Utah was in the process of migrating to an integrated Medicaid system referred to as the Provider Reimbursement Information System (PRISM) that facilitates provider enrollment, managed care processes, claims adjudication, claims payment, and web portal access for Medicaid enrollees to see an overview of their providers, benefits, and claims, as well as capabilities to analyze and detect fraud and abuse.[4]

HOW WE CONDUCTED THIS AUDIT

We conducted a penetration test of Utah's MMIS and E&E system from February through March 2021. The penetration test focused on the MMIS and E&E system's public IP addresses

[4] Subsequent to audit period, Utah replaced the legacy MMIS and E&E system we audited with PRISM.

and web application URLs. We also conducted a simulated phishing campaign that covered a limited number of Utah personnel in March 2021.

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 Utah 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 by OIG, XOR, and the State of Utah.

We provided detailed documentation about our preliminary findings to Utah 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 Utah MMIS and E&E system had adequate security controls in place to prevent our simulated cyberattacks from resulting in a successful compromise; however, some of its security controls could be improved to better prevent certain cyberattacks and reduce overall risk. In addition, we estimated that the level of sophistication needed by an adversary to compromise the Utah MMIS and E&E system was significant.[5] At this level, an adversary would need a significant level of expertise through advanced training and persistence to circumvent most of the current security controls. Finally, based on the results of our simulated cyberattacks, Utah demonstrated the ability to detect some attacks and respond appropriately. For example, Utah detected the reconnaissance activity during our active reconnaissance testing phase and enabled countermeasures. However, Utah did not prevent other penetration test activities we performed in later phases.

[5] 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 Mar. 28, 2023.

As a result of the penetration test, we identified seven security controls that were not effective. We shared this information with Utah, which later provided evidence of remediation of some of these security control findings or evidence of how some no longer present risk because the affected systems we audited are no longer in operation, as Utah subsequently migrated to a new MMIS and E&E system. We reviewed the evidence that Utah provided and determined that the security control findings related to four security controls (Access Enforcement (AC-3), Information Input Validation (SI-10), Least Functionality (CM-7), and Error Handling (SI-11)) were successfully remediated or no longer present risk as a result of the system migration. We commend Utah for its efforts to immediately track and address these security control findings. The remaining security control findings relate to (SI-2) Flaw Remediation, (SA-8) Secure Engineering Principles and (SC-8) Transmission Confidentiality and Integrity. These control findings still apply to PRISM–Utah's new MMIS and E&E system–and have not yet been remediated. We will review Utah's evidence of remediation as part of our audit resolution process.

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.[6] Utah did not correctly implement the following NIST Special Publication (SP) 800-53, Revision 4, security controls, as shown in the table on the following page.

[6] For more information, please see https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-A/part-95/subpart-F/subject-group-ECFR8ea7e78ba47a262/section-95.621. Accessed on June 15, 2023.

Table: MMIS and E&E System Security Control Findings

NIST SP 800-53, Revision 4, Security Control	Security Control Finding	Control No*	Risk Rating†
Flaw Remediation	Utah did not identify, report, and correct system flaws for a public-facing system in its MMIS and E&E system within the timeframe required by the CMS Acceptable Risk Safeguards (ARS).	SI-2	High
Access Enforcement	Utah did not properly enforce approved authorizations for logical access control to information and system resources for a public-facing system in its MMIS and E&E system. This has been remediated or is no longer applicable.	AC-3	Moderate
Information Input Validation	Utah did not properly sanitize or verify information system input for a public-facing system in its MMIS and E&E system. This has been remediated or is no longer applicable.	SI-10	Moderate
Least Functionality	Utah did not properly restrict functions and services that may not be necessary to support essential organizational operations for a public-facing system in its MMIS and E&E system. This has been remediated or is no longer applicable.	CM-7	Low
Security Engineering Principles	Utah did not adequately apply information system security engineering principles in the design and implementation to certain public-facing systems in its MMIS and E&E system.	SA-8	Low
Transmission Confidentiality and Integrity	Utah did not implement sufficient website protections to ensure that information transmitted to systems in its MMIS and E&E system was protected.	SC-8	Low
Error Handling	Utah did not implement secure error handling configurations to prevent disclosure of information for a public-facing system in its MMIS and E&E system. This has been remediated or is no longer applicable.	SI-11	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.

A potential reason why Utah did not correctly implement these security controls may be that system administrators were not aware of Government standards or industry best practices that require securely configured systems before deployment to production. Also, Utah's flaw remediation procedures were not consistent with the timeframe defined in the CMS ARS policy for correcting identified security-related information system flaws on production systems, which during our audit period was 10 business days. As a result, an attacker could potentially extract sensitive data and PII, impersonate other users, or 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 attack and compromise. Utah also indicated that, in accordance with what it described as CMS system certification requirements, it uses a contractor to conduct external risk assessments or penetration testing every 3 years. The CMS Acceptable Risk Safeguards (ARS) does require a risk assessment every 3 years and there is no other requirement from CMS for more frequent routine penetration testing unless the system is considered a high value asset. The lack of routine penetration testing increases the risk of not detecting an exploitable weakness timely, given the ever-changing cyber threat activity affecting healthcare today and doesn't align with established cybersecurity industry best practices for penetration testing.[7]

Regarding our email phishing campaign, we sent 951 phishing emails to specific Utah employees[8] and determined that 301 emails (32 percent) were opened, and the web link embedded in the email was clicked 10 times (3.3 percent). Although the low click-rate is a positive sign that most Utah users we tested may be trained to not click on suspicious links in emails, the high rate of those who received and opened the phishing email may be due to ineffective email filtering controls to block the delivery of potentially malicious emails to end users. We shared these results as information only and encouraged Utah to review its controls to determine whether any improvements can be made.

RECOMMENDATIONS

We recommend that the Utah Department of Health:

- remediate the remaining three security control findings identified by OIG and
- revise flaw remediation procedures such that they fully implement the flaw remediation requirements defined in the CMS Acceptable Risk Safeguards (ARS), SI-02 Flaw Remediation (High; Moderate; Low) control.

[7] Cybersecurity professionals recommend penetration tests once or twice a year because of how hackers change their approaches. https://cybriant.com/the-ceos-guide-to-penetration-testing/ Accessed on Nov. 15, 2023.

[8] Utah provided email addresses for all employees except political appointees.

UTAH'S COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments on our draft report, Utah agreed with our recommendations and stated that it has addressed and remediated the security control findings identified by OIG (first recommendation) and is in the process of addressing our second recommendation. Although we have not yet confirmed the changes Utah described in its response, we commend Utah's ongoing efforts to improve the overall security posture of its MMIS and E&E system environments. Utah'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 Utah MMIS and E&E system, as specified within the ROE document. Utah 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 Utah 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 Utah's ability to detect or effectively prevent certain cyberattacks. The 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 control deficiencies that may have existed at the time of this audit.[9]

We performed our work remotely. Penetration testing began on February 8 and ended March 9, 2021, and the simulated phishing campaign was conducted in March 2021. For the simulated phishing campaign, Utah provided us with a list of 951 employee email addresses. We sent a phishing email to all 951 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 Utah 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 Utah 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 Utah MMIS and E&E system. To accomplish our objectives, OIG and Utah prepared the ROE document that outlined the general rules, logistics, and expectations for the penetration test. State of Utah officials signed the ROE document indicating agreement.

In February 2021, we began reconnaissance and scope verification of network subnets owned, operated, and maintained by Utah. We performed external penetration testing to determine whether internet-facing systems were susceptible to exploits by an external attacker.

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

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, 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 March 2021, XOR conducted a simulated phishing campaign to determine whether Utah had implemented appropriate controls to detect and prevent successful phishing campaigns and to determine whether Utah's personnel were adequately trained to recognize and appropriately respond to such malicious emails. Utah provided a list of the employees who would be subject to XOR's simulated phishing campaign. The campaign was designed to send those employees a phishing email that contained a web link to a malicious website. If any of the employees clicked the link, their web browser would be redirected to a website hosted within the HHS OIG Cyber Range.[10] Once the user was redirected, the website would attempt to run code in the

[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.

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 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.[11] 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.

[11] 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.[12] State agencies are responsible for the security of all ADP projects under development, and operational systems involved in the administration of HHS programs. State agencies shall determine the appropriate ADP security requirements based on recognized industry standards or standards governing security of Federal ADP systems and information processing.

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

AC-3 ACCESS ENFORCEMENT (page F-10)

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

[12] 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.

CM-7 LEAST PRIVILEGE (page F-71)

Control: The organization:

a. Configures the information system to provide only essential capabilities; and

b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services*].

Supplemental Guidance: Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing). Organizations consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services. Related controls: AC-6, CM-2, RA-5, SA-5, SC-7.

SA-8 SECURITY ENGINEERING PRINCIPLES (page F-162)

Control: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Supplemental Guidance: Organizations apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs;

(vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. Related controls: PM-7, SA-3, SA-4, SA-17, SC-2, SC-3.

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.

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.

CMS Information Security and Privacy Acceptable Risk Safeguards (ARS) version 3.1, states:

SI-02 Flaw Remediation (High; Moderate; Low)

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 as directed in Implementation Standard 1; and
d. Incorporates flaw remediation into the organizational configuration management process.

Implementation Standards:
High, Moderate & Low:
Std.1 - Correct identified security-related information system flaws on production equipment within ten (10) business days and all others within thirty (30) calendar days.
(a) Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and

potential side effects of such changes; and

(b) Manage the flaw remediation process centrally.

Std.2 - A risk-based decision is documented through the configuration management process in the form of written authorization from the CMS CIO or his/her designated representative (e.g., the system data owner or CMS CISO) and updated documentation in the risk analysis and security plan if a security patch is not to be applied to an information technology component or a legacy (no-longer maintained by the vendor) component is to remain in use.

Std.3 - Flaw remediation requirements apply to all information technology components for which a patch or work-around exists for each vendor-identified and/or CVE/CWE -identified vulnerability.

Std.4 - The organization must provide timely responses, as defined by the CISO, to informational requests for organizational flaw (e.g., patch) status and posture information.

APPENDIX D: UTAH COMMENTS

State of Utah

SPENCER J. COX
Governor

DEIDRE M. HENDERSON
Lieutenant Governor

Department of Health & Human Services

TRACY S. GRUBER
Executive Director

NATE CHECKETTS
Deputy Director

DR. MICHELLE HOFMANN
Executive Medical Director

DAVID LITVACK
Deputy Director

NATE WINTERS
Deputy Director

February 12, 2024

Tamara J. Lilly
Assistant Inspector General
for Cybersecurity & IT Audits
Washington, DC 20201

Dear Assistant Inspector General Lilly:

On behalf of the Department of Health and Human Services (DHHS), thank you for the opportunity to respond to the audit titled *Utah MMIS and E&E System Had Adequate Security Controls In Place, but Improvements Are Needed* (Report Number: A-18-21-09001). I appreciate the effort and professionalism of you and your staff in this review. The final product reflects a significant effort and time of the DHHS staff collecting information for OIG review, answering questions, and planning changes to improve the program. This audit and its responses will result in a better, more efficient program.

DHHS agrees with the recommendations in this report. DHHS is committed to the efficient and effective use of taxpayer funds and values the insight this report provides on areas that need improvement.

Sincerely,

Jennifer Strohecker (Feb 12, 2024 09:21 MST)

Jennifer Strohecker, PharmD, BCPS
Medicaid Director
Director, Division of Integrated Healthcare

Division of Integrated Healthcare
288 North 1460 West • Salt Lake City, UT 84116
Mailing Address: P.O. Box 143101 • Salt Lake City, UT 84114-3101
Telephone (801) 538-6689 • medicaid.utah.gov/

Response to Recommendations

Recommendation 1

We recommend that the Utah Department of Health remediate the remaining three security control findings identified by OIG.

Department Response:

DHHS agrees with this recommendation and has already remediated the three security control findings identified by the OIG.

Recommendation 2

We recommend that the Utah Department of Health revise flaw remediation procedures such that they fully implement the flaw remediation requirements defined in the CMS Acceptable Risk Safeguards (ARS), SI-02 Flaw Remediation (High; Moderate; Low) control.

Department Response:

DHHS agrees with this recommendation. The Department of Workforce Services is currently working on a project with the Division of Technology Services to address this recommendation.

Anticipated Completion Date: June 30, 2024