Department of Health and Human Services

**OFFICE OF
INSPECTOR GENERAL**

MARYLAND 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

May 2023
A-18-21-09003

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: May 2023
Report No. A-18-21-09003

U.S. Department of Health & Human Services
Office of Inspector General

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

Why OIG Did This Audit

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

Our objectives were to determine whether (1) security controls in operation at Maryland 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 Maryland Medicaid System or its data, and (3) Maryland's ability to detect cyberattacks against its Medicaid MMIS and E&E system and respond appropriately.

How OIG Did This Audit

We conducted a penetration test of Maryland's MMIS and E&E system from September through November 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 that included a limited number of Maryland personnel in November 2021. 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 Maryland.

What OIG Found

The Maryland 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, improvements are needed to better prevent certain cyberattacks. Maryland did not correctly implement seven 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 Maryland MMIS and E&E system was limited.[1] At this level, an adversary would need a limited level of expertise, with limited resources and opportunities to support a successful attack. Finally, Maryland demonstrated a partial ability to detect some of our cyberattacks against its MMIS and E&E system and respond appropriately.

A potential reason why Maryland 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 configured systems before deployment to production. Maryland also may not have considered the latest email phishing tactics used by cyber adversaries in developing the cybersecurity awareness training provided to its employees and contractors. Additionally, Maryland's procedures for periodically assessing the implementation of the NIST security controls above were not effective. As a result of Maryland 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 an initial foothold and potentially move deeper into the network, thereby exposing critical systems and data to attack and compromise.

What OIG Recommends

We recommend that Maryland: (1) remediate the seven control findings OIG identified; (2) assess the effectiveness of all required NIST SP 800-53 controls according to the organization's defined frequency; (3) assess at least annually and if necessary, adjust baseline configurations for its MMIS and E&E public servers; and (4) perform periodic phishing exercises and enhance employee and contractor cybersecurity awareness training based on the results of the phishing exercises, if needed.

In written comments on our draft report, Maryland concurred with our recommendations and stated that they have remediated our findings. Although we have not yet confirmed the changes Maryland described in its response, we commend Maryland's ongoing efforts to improve the overall security posture of its MMIS and E&E system environments.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/182109003.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 Maryland'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 for Maryland 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 Maryland MMIS and E&E system or its data, and

- Maryland's ability to detect cyberattacks against its MMIS and E&E system and respond appropriately.

BACKGROUND

The Medicaid program provides medical assistance to low-income individuals and individuals with disabilities. The Federal and State Governments jointly fund and administer the Medicaid program. At the Federal level, the Centers for Medicare & Medicaid Services (CMS) administers the program. Each State administers its Medicaid program in accordance with a CMS-approved State plan. Although the State has considerable flexibility in designing and operating its Medicaid program, it must comply with applicable Federal requirements.

[1] Penetration testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. It often involves launching real attacks on real systems and data using tools and techniques commonly used by attackers.

[2] NIST Special Publication (SP) 800-115, Technical Guide to Information Security Testing and Assessment.

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

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

State E&E systems support all processes related to determining Medicaid eligibility. After the implementation of the Patient Protection and Affordable Care Act (ACA) in 2014, States were required to coordinate beneficiary enrollment 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 that is sought by cyber criminals and foreign adversaries for financial gain, to sabotage State systems, or both.

The Maryland Department of Health is responsible for administering the State Medicaid program through its Maryland Medicaid Administration. Medicaid and the Children's Health Insurance Program (CHIP) provide health and long-term care coverage to nearly 1.3 million low-income children, pregnant women, adults, seniors, and people with disabilities in Maryland. As of 2022, Maryland reported that 20 percent of Maryland citizens were covered by Medicaid or CHIP. In fiscal year 2021, Medicaid spending in Maryland was $13.5 billion.

HOW WE CONDUCTED THIS AUDIT

We conducted a penetration test of Maryland's MMIS and E&E system from September through November 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 that covered a limited number of Maryland personnel in November 2021.

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

We provided detailed documentation about our preliminary findings to Maryland 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 Maryland 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, improvements are needed to better prevent certain cyberattacks. In addition, we estimated that the level of sophistication needed by an adversary to compromise the Maryland MMIS and E&E system was limited.[3] At this level, an adversary would need a limited level of expertise, with limited resources and opportunities to support a successful attack. Finally, Maryland demonstrated a partial ability to detect some of our 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 security of Federal IT systems and information processing.[4] Maryland did not correctly implement the

[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 March 27, 2023.

[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 September 7, 2022.

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

Table: Weak MMIS and E&E System Security Controls

NIST SP 800-53, Revision 4, Security Control	Security Control Finding	Control No.*	Risk Rating†
Least Functionality	Maryland did not adequately restrict use of software and services in its MMIS and E&E system.	CM-7	High
Access Enforcement	Maryland did not properly enforce approved authorizations for logical access to information and system resources in its MMIS and E&E system.	AC-3	Moderate
Security Awareness Training	Maryland did not provide effective security awareness training to users of its MMIS and E&E system.	AT-2	Moderate
Transmission Confidentiality and Integrity	Maryland did not properly protect the confidentiality of transmitted information in its MMIS and E&E system.	SC-8	Moderate
Flaw Remediation	Maryland did not properly identify, report, and correct system flaws in its MMIS and E&E system.	SI-2	Moderate
Information Input Validation	Maryland did not properly sanitize or verify information system input for a public facing MMIS and E&E system server.	SI-10	Moderate
Configuration Settings	Maryland did not properly establish configuration settings in the MMIS and E&E system that reflect the most restrictive mode consistent with operational 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.

A potential reason why Maryland 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 configured systems before deployment to production. Maryland also may not have considered the latest email phishing tactics used by cyber adversaries in developing the cybersecurity awareness training provided to its employees and contractors. Additionally, Maryland's procedures for periodically assessing the implementation of the NIST security controls above were not effective. As a result of Maryland 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 an initial foothold and potentially move deeper into the network, thereby exposing critical systems and data to attack and compromise.

Regarding our email phishing campaign, we sent 49 phishing emails to specific employees and we determined that 15 emails were opened and the web link embedded in the emails was clicked 15 times. Approximately 30 percent of the employees targeted by the phishing campaign clicked the malicious link. 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 high click rate is that the employees may not be adequately trained to identify or properly respond to phishing emails. We have shared these results as information only and encouraged Maryland to investigate its email phishing controls to determine what improvements may be necessary.

RECOMMENDATIONS

We recommend that the Maryland Department of Health:

- remediate the seven control findings OIG identified;

- assess the effectiveness of all required NIST SP 800-53 controls according to the organization's defined frequency;

- assess at least annually and if necessary, adjust baseline configurations for its MMIS and E&E public servers; and

- perform periodic phishing exercises and enhance employee and contractor cybersecurity awareness training based on the results of the phishing exercises, if needed.

MARYLAND'S COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments on our draft report, Maryland concurred with our recommendations and stated that they have remediated our findings. Although we have not yet confirmed the changes Maryland described in its response, we commend Maryland's ongoing efforts to improve the overall security posture of its MMIS and E&E system environments.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

The penetration test focused on both public IP addresses and web application URLs related to the Maryland MMIS and E&E system, as specified within the ROE document. Maryland 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 only assessed control activities specific to IT general controls and application controls for the Maryland MMIS and E&E system. We did not assess all internal control components and principles.[5] Based on our penetration test we assessed the operating effectiveness of these internal controls and identified deficiencies that we believe could affect Maryland's ability to detect, or effectively prevent certain cyberattacks. The internal control deficiencies we identified are listed as Security Control Findings in the Findings section of this report. However, the penetration test we performed may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

We performed our work remotely. Penetration testing began on September 20 and ended November 19, 2021, and the simulated phishing campaign began on November 2, 2021, and ended November 12, 2021.

For the simulated phishing campaign, Maryland provided us with a list of 49 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 Maryland 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 Maryland Medicaid Administration'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 Maryland MMIS and E&E system. To accomplish our objectives, OIG and Maryland prepared the ROE document that outlined the general rules, logistics, and expectations for the penetration test. Maryland officials provided a signed ROE document indicating that Maryland agreed with the rules to be followed during our testing.

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

In September 2021, we began reconnaissance and scope verification of network subnets owned, operated, and maintained by Maryland. 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 November 2021, XOR conducted a simulated phishing campaign to determine whether Maryland had implemented appropriate controls to detect and prevent successful phishing campaigns and to determine whether Maryland's personnel were adequately trained to recognize and appropriately respond to such malicious emails. Maryland provided a list of the employees who would be subject to XOR's simulated phishing campaign. The campaign was designed to send a phishing email to the 49 Maryland personnel 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. [6] A program would then attempt to run code in the employee's browser and 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 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.[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 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.
>
> AT-2 SECURITY AWARENESS TRAINING (page F-37)
>
> Control: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):
>
> a. As part of initial training for new users;
>
> b. When required by information system changes; and

[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.

c. [Assignment: organization-defined frequency] thereafter.

Supplemental Guidance: Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

CM-6 CONFIGURATION SETTINGS (page F-70)

Control: The organization:

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

b. Implements the configuration settings;

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

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

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

CM-7 LEAST FUNCTIONALITY (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.

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.

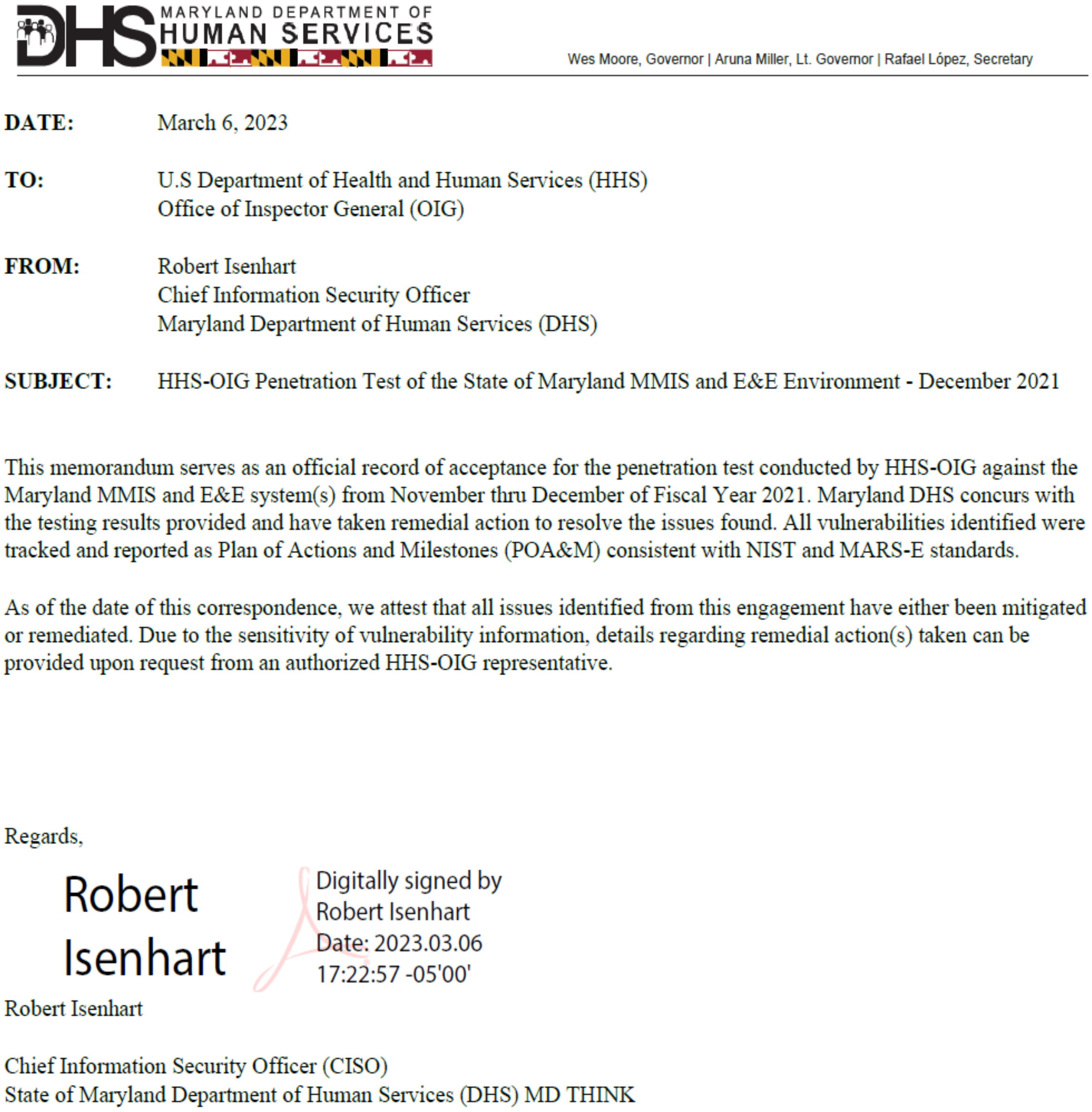
Supplemental Guidance: Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software 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.

APPENDIX D: MARYLAND'S COMMENTS



MARYLAND DEPARTMENT OF HUMAN SERVICES

Wes Moore, Governor | Aruna Miller, Lt. Governor | Rafael López, Secretary

DATE: March 6, 2023

TO: U.S Department of Health and Human Services (HHS)
Office of Inspector General (OIG)

FROM: Robert Isenhart
Chief Information Security Officer
Maryland Department of Human Services (DHS)

SUBJECT: HHS-OIG Penetration Test of the State of Maryland MMIS and E&E Environment - December 2021

This memorandum serves as an official record of acceptance for the penetration test conducted by HHS-OIG against the Maryland MMIS and E&E system(s) from November thru December of Fiscal Year 2021. Maryland DHS concurs with the testing results provided and have taken remedial action to resolve the issues found. All vulnerabilities identified were tracked and reported as Plan of Actions and Milestones (POA&M) consistent with NIST and MARS-E standards.

As of the date of this correspondence, we attest that all issues identified from this engagement have either been mitigated or remediated. Due to the sensitivity of vulnerability information, details regarding remedial action(s) taken can be provided upon request from an authorized HHS-OIG representative.

Regards,

Robert Isenhart

Digitally signed by Robert Isenhart
Date: 2023.03.06 17:22:57 -05'00'

Robert Isenhart

Chief Information Security Officer (CISO)
State of Maryland Department of Human Services (DHS) MD THINK