Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

ILLINOIS MMIS AND E&E SYSTEM HAD ADEQUATE SECURITY CONTROLS IN PLACE, BUT SOME IMPROVEMENTS ARE NEEDED

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Amy J. Frontz
Deputy Inspector General
for Audit Services

August 2024
A-18-22-09009

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: August 2024
Report No. A-18-22-09009

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

Illinois MMIS and E&E System Had Adequate Security Controls in Place, but Some 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 Illinois' 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 Illinois MMIS and E&E system or its data, and (3) Illinois' 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 Illinois MMIS and E&E system from August through September 2022. The penetration test focused on the MMIS and E&E system's public IP addresses and web application URLs. We also conducted a simulated phishing campaign targeting Illinois 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 Illinois.

What OIG Found

The Illinois 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 Illinois' risk of compromise. Specifically, Illinois did not correctly implement four security controls required by the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4.

We estimated that an adversary would need a significant level of sophistication to compromise the Illinois MMIS and E&E system. At this level, an adversary would need a significant level of expertise through advanced training and a significant level of persistence to circumvent most of the current security controls. Illinois demonstrated the ability to detect some of our cyberattacks against its MMIS and E&E system by blocking our testing domain after it detected our hacking attempts.

Potential reasons why Illinois did not correctly implement these security controls may be that system developers and administrators were not aware of Government standards, due to a lack of documented enterprise flaw remediation procedures, and ineffective testing procedures when periodically assessing implementation of NIST security controls. As a result, an attacker could potentially execute multiple types of targeted attacks against the Illinois MMIS and E&E system.

What OIG Recommends and Illinois Comments

We made a series of recommendations for Illinois to improve its security controls over its MMIS and E&E system, including that it enhances its security control assessment testing procedures and takes corrective actions when deficiencies in controls are identified. The full recommendations are in the report.

In written comments, Illinois did not indicate concurrence or nonconcurrence with our recommendations. Rather, Illinois stated that it concurs with each of the needed improvements mentioned in the draft report and described actions ongoing or taken to address the four control findings we identified. Although we have not yet confirmed whether our recommendations were effectively implemented, we are encouraged by Illinois's response and we look forward to receiving and reviewing the supporting documentation through our audit resolution process.

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 (MMISs) and Eligibility and Enrollment (E&E) systems. In the last 10 years, we have performed multiple audits of State MMISs 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 Illinois Department of Healthcare and Family Services' (Illinois') MMIS and E&E system in accordance with guidelines outlined by the National Institute of Standards and Technology (NIST).[2] This audit is part of a series of audits of other MMIS and E&E systems in other states.

OBJECTIVES

Our objectives were to determine:

- whether security controls in operation for the Illinois'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 Illinois MMIS and E&E system or its data, and
- Illinois' 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] NIST Special Publication (SP) 800-115, *Technical Guide to Information Security Testing and Assessment*. Available online at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf. Accessed on April 12, 2024.

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) that is sought by cyber criminals and foreign adversaries for financial gain, to sabotage State systems, or both.

Illinois is responsible for providing health care coverage for adults and children who qualify for Medicaid, and for providing child support services to help ensure that Illinois children receive financial support from both parents. The agency is organized into two major divisions, Medical Programs and Child Support Services. In addition, the State's Office of Inspector General is maintained within the agency, but functions as a separate, independent entity reporting directly to the Governor's office. The Division of Medical Programs administers and, in conjunction with the Federal Government, funds medical services provided to about 25 percent of the State's population. Illinois' medical assistance programs, consisting of Medicaid and numerous other medical programs associated with it, provide comprehensive health care coverage to about 3.2 million Illinoisans. In fiscal year 2022, Illinois' Medicaid spending was $20.8 billion.

HOW WE CONDUCTED THIS AUDIT

We conducted a penetration test of Illinois' MMIS and E&E system from August through September 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 Illinois personnel during this timeframe.

To assist us with the penetration test, we relied on the work of specialists. Specifically, we contracted with XOR Security, LLC (XOR), to assist in conducting the penetration test of the Illinois 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 Illinois' Enterprise Compliance Division.

We provided detailed documentation about our preliminary findings to Illinois 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 Illinois 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 Illinois' risk of compromise. In addition, we estimated that an adversary would need a significant level of sophistication to compromise the MMIS and E&E system.[3] At this level, an adversary would need a significant level of expertise through advanced training and need a significant level of persistence to circumvent most of the current security controls. Finally, based on the results of

[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 April 12, 2024.

our simulated cyberattacks, Illinois demonstrated the ability to detect some of our cyberattacks against its MMIS and E&E system and respond appropriately by blocking our testing domain after the systems detected our hacking attempts. However, we identified four security controls that were not effective. We shared this information with Illinois, which immediately began work to remediate the ineffective controls. We have not confirmed that Illinois completed its corrective actions. We will validate the actions taken by Illinois during 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 security of Federal information technology (IT) systems and information processing.[4] Illinois did not correctly implement the following NIST Special Publication (SP) 800-53, Revision 4, security controls as shown in the table.

Table: MMIS and E&E System Security Controls Findings

NIST SP 800-53, Revision 4, Security Control	Security Control Finding	Control No.*	Risk Rating†
Flaw Remediation	Illinois did not identify, report, and correct system flaws for one public-facing system in its MMIS and E&E system.	SI-2	High
Error Handling	Illinois did not implement secure error handling configurations to prevent disclosure of information on two public-facing systems in its MMIS and E&E system.	SI-11	Moderate
Transmission Confidentiality and Integrity	Illinois did not effectively implement website protections to ensure that information transmitted to two of its systems was protected.	SC-8	Moderate
Authenticator Management	Illinois did not adequately implement controls in its MMIS and E&E system to protect authenticator content stored in client web browsers from unauthorized disclosure and modification.	IA-5	Low

[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 April 12, 2024.

NIST SP 800-53, Revision 4, Security Control	Security Control Finding	Control No.*	Risk Rating†

* 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 Illinois did not implement these security controls correctly may be that system developers and administrators were not aware of Government policies, standards, or industry best practices that require designing, configuring, and testing secure systems before deploying to production. Also, Illinois did not have documented enterprise flaw remediation procedures for effectively identifying vulnerabilities and assessing, prioritizing, and remediating them in a timely manner. Finally, Illinois' testing procedures for assessing the implementation of NIST security controls were not effective in identifying cybersecurity control weaknesses. For example, an attacker could potentially execute targeted attacks against Illinois' MMIS and E&E system using the information revealed from error messages generated by systems due to the error handling weakness, extract sensitive data in client-server communications, access personally identifiable information and other sensitive data, such as passwords, cause a denial-of-service, or execute malicious code.

Regarding our email phishing campaign, we sent 5,848 phishing emails to specific Illinois employees and contractors; however, our tools indicated that none of those emails were opened and none of the web links embedded in the emails were clicked. The reason no emails were opened could be that Illinois' email filtering systems may have prevented the emails from being successfully delivered to the targeted employees because they were sent from a known malicious IP address or that employees recognized the malicious IP address and knew not to click on it. This is a desired response. We have shared these results as information only and encouraged Illinois to continue challenging their email defenses and employees with increasingly more sophisticated phishing campaigns.

RECOMMENDATIONS

We recommend that the Illinois Department of Healthcare and Family Services:

- remediate the four security control findings identified by OIG;

- develop and implement flaw remediation policies and procedures for effectively identifying vulnerabilities, prioritizing them based on potential impact and exploitability, and remediating them within a defined timeframe as required by NIST SP 800-53, SI-2,

Flaw Remediation, or other standards governing security of Federal systems and information; and

- enhance its testing procedures to include performing more robust technical testing of web-facing systems and emulation of an adversary's tactics and techniques on a defined reoccurring basis, in order to better assess the effectiveness of NIST SP 800-53 controls.

ILLINOIS COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments on our draft report, Illinois did not indicate concurrence or nonconcurrence with our recommendations. Rather, Illinois stated that it concurs with each of the needed improvements mentioned in the draft report and described actions ongoing or taken to address the first recommendation to remediate the four security control findings we identified. Illinois did not provide specific responses to the remaining two recommendations. Although we have not yet confirmed whether the actions described effectively implement our recommendation, we are encouraged by Illinois's response and we look forward to receiving and reviewing the supporting documentation. We will validate the actions taken by Illinois during the audit resolution process. Illinois' 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 Illinois MMIS and E&E system, as specified within the ROE document. Illinois 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.[5] We assessed only control activities specific to IT general controls and application controls for the Illinois 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 Illinois' ability to detect or effectively prevent certain cyberattacks. The IT 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.

We performed our work remotely. Penetration testing began on August 1 and ended September 28, 2022, and the simulated phishing campaign began on August 25 and ended September 9, 2022. For the simulated phishing campaign, Illinois provided us with a list of 5,848 employee email addresses.

METHODOLOGY

We relied on the work of specialists to assist with the series of OIG audits using network and web application penetration testing and social-engineering techniques. OIG contracted with XOR to conduct the penetration test of the Illinois 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 Illinois 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 Illinois MMIS and E&E system. To accomplish our objectives, OIG and Illinois prepared the ROE document that outlined the general rules, logistics, and expectations for the penetration test. Illinois officials provided a signed ROE document indicating that Illinois agreed with the rules to be followed during our testing.

In August 2022, we began reconnaissance and scope verification of network subnets owned, operated, and maintained by Illinois. 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 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.

From August to September 2022, XOR conducted a simulated phishing campaign to determine whether Illinois had implemented appropriate controls to detect and prevent phishing campaigns and to determine whether Illinois personnel were adequately trained to recognize and appropriately respond to such malicious emails. Illinois provided us a list of 5,848 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.[6] Once the user was redirected, the website

[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.

would attempt to run code in the employee's web 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.

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 attacks against a system.

[7] A "Client-Side Attack" occurs when a user (the client) downloads malicious code from the server that 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:

SI-2 FLAW REMEDIATION

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.

SI-11 ERROR HANDLING

Control: The information system:

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

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

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

[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.

IA-5 AUTHENTICATOR MANAGEMENT

Control: The organization manages information system authenticators by:

a. verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. establishing initial authenticator content for authenticators defined by the organization;
c. ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
e. changing default content of the authenticators prior to information system installation;
f. changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*];
g. protecting authenticator content from unauthorized disclosure and modification;
h. requiring individuals to take, and having devices implement, specific controls to protect authenticators; and
i. changing authenticators for group/role accounts when membership to those accounts changes.

APPENDIX D: ILLINOIS COMMENTS

HFS
Illinois Department of
Healthcare and Family Services

JB Pritzker, Governor
Elizabeth M. Whitehorn, Director

401 S. Clinton St., Chicago, Illinois 60607
Telephone: +1 312-793-4792, TTY: +1 800-526-5812

June 21, 2024

Response to Report Number: A-18-22-09009

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

Dear Tamara Lilly:

The Illinois Department of Healthcare and Family Services (HFS) concurs with each of the needed improvements mentioned in the draft report *Illinois MMIS and E&E System Had Adequate Security Controls in Place, but Some Improvements Are Needed* and have the following responses for each of the corresponding controls identified:

NIST 800-53, Revision 4, Security Control	Control No.	Security Control Response
Flaw Remediation	SI-2	This is being addressed as part of a much larger effort to meet federal standards.
Error Handling	SI-11	Error messages have since been standardized to limit disclosure while providing accurate descriptions within the system.
Transmission Confidentiality and Integrity	SC-8	Configurations have been updated within in the system to protect the confidentiality and integrity of the information being transmitted.
Authenticator Management	IA-5	Configurations have been updated within in the system to prevent the use of stored authenticators within the browser.

We thank you for the opportunity to provide comments on the corrective actions we've since taken address the insufficiencies of the controls we had in place.

Sincerely,

Graham Osmonson

Digitally signed by Graham Osmonson
Date: 2024.06.24 10:01:04 -05'00'

Graham Osmonson
Chief Information Officer
Illinois Department of Healthcare and Family Services