Department of Health and Human Services
Office of Inspector General
Office of Audit Services

October 2025 | A-18-24-00002

Summary Report of Prior Office of Inspector General Penetration Tests of 10 State MMIS and E&E Systems

REPORT HIGHLIGHTS

October 2025 | A-18-24-00002

Summary Report of Prior Office of Inspector General Penetration Tests of 10 State MMIS and E&E Systems

Why OIG Did This Audit

- In the health care sector, State Medicaid Management Information Systems (MMIS) and Eligibility & Enrollment (E&E) systems are increasingly targeted by cybercriminals because of the valuable sensitive information they contain. There has been a noticeable increase in ransomware, phishing, and denial-of-service attacks that pose significant risks to critical health care systems and the data they manage.
- Between 2020 and 2022, OIG conducted penetration tests on 10 State MMIS and E&E systems. These tests were designed to simulate cyberattacks to evaluate how effectively these systems were protected against such threats.

What OIG Found

Overall, we found that:

- the 10 States implemented generally effective information technology security controls for their web-facing MMIS and E&E systems to prevent unsophisticated or limited cyberattacks, but they need to continue to improve these controls to prevent more sophisticated and persistent cyberattacks;
- cyber attackers would likely need a moderate to significant level of sophistication or complexity to compromise the State systems we audited; and
- the 10 States effectively detected and responded to some of our simulated cyberattacks but they need to improve their detection and response to other types of cyberattacks.

What OIG Recommends

This summary report contains no recommendations to the Centers for Medicare & Medicaid Services (CMS); however, it does provide an overview of the recommendations previously made to the 10 States.

CMS informed us that it did not have comments on our draft report.

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

Summary Report of Prior Office of Inspector General Penetration Tests of 10 State MMIS and E&E Systems

Report No. A-18-24-00002
October 2025

Table of Contents

Why We Performed Penetration Test Audits (2020-2022)

- Based on reported data breaches, State Medicaid Management Information Systems (MMIS) and Eligibility & Enrollment (E&E) systems have been a target for malicious actors because of the sensitive information they hold. Ransomware, phishing, and denial-of-service attacks are on the rise and threaten these important systems and their data.

- In a previous round of penetration test audits performed on select State MMIS and E&E systems between 2010 and 2012, we found that most States did not have adequate information technology (IT) security controls to protect the systems from cyberattacks.

Reported Cybersecurity Data Breaches

- 2012 • South Carolina Medicaid Data Breach – Data of 228,000 individuals compromised
- 2012 • Utah Medicaid Data Breach – Data of 780,000 individuals compromised
- 2020 • Iowa Medicaid Data Breach – Data of 116,000 individuals compromised
- 2021 • Texas Medicaid Data Breach – Data of 1.8 million individuals compromised
- 2023 • Illinois Eligibility Data Breach – Data of 41,000 individuals compromised
- 2023 • Maine Medicaid Data Breach – Data of 1.3 million individuals compromised

Overview

This summary report provides the Centers for Medicare & Medicaid Services with an overview of:

- actionable insights regarding the cybersecurity posture of State MMIS and E&E systems we audited,
- ineffective implementation of certain National Institute of Standards and Technology (NIST) Special Publication 800-53 security controls in MMIS and E&E systems, and
- opportunities for States to strengthen cybersecurity in their MMIS and E&E systems.

Background

- From August 2020 through December 2022, we assessed the effectiveness of IT security controls in 10 State MMIS and E&E systems through a series of penetration tests to determine how well these systems were protected when subjected to emulated cyberattacks.

- The audits 1) provided valuable insights into the strengths and weaknesses of the systems' cyber defenses, 2) revealed ineffective security controls implementations, and 3) evaluated the potential impact of successful exploitation of the vulnerabilities identified.

- Although cybersecurity defenses cannot guarantee complete protection against cyber breaches, State agencies can reduce their risk by effectively implementing required IT security controls and industry best practices for protecting web applications and web services.

Audit Objectives

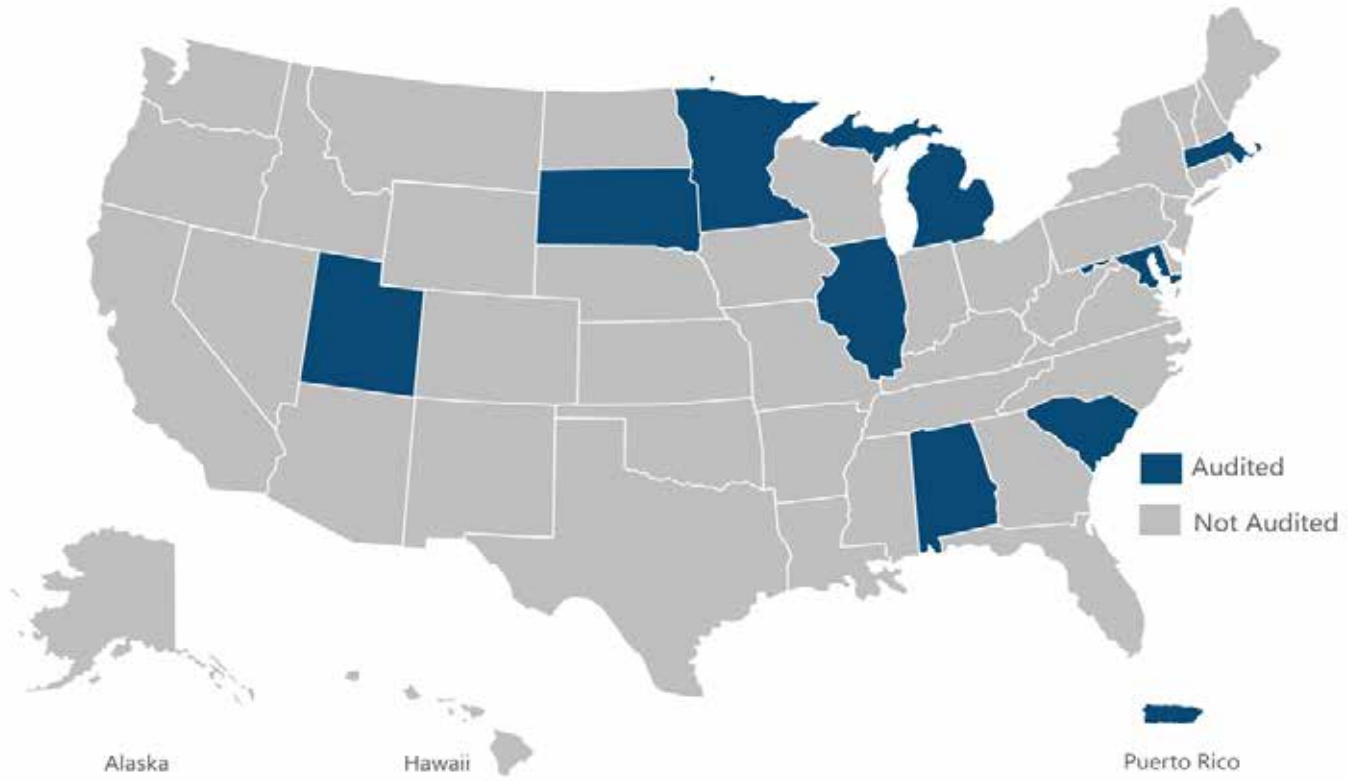
The objectives of the prior MMIS and E&E systems audits performed at 10 States were to determine:

- whether security controls in operation for MMIS and E&E system environments were effective in preventing certain cyberattacks,
- the likely level of sophistication or complexity an attacker needs to compromise MMIS and E&E systems or data, and
- the States' ability to detect cyberattacks against their MMIS and E&E systems and respond appropriately.

How We Did These Audits

- We conducted penetration testing on 10 State MMIS and E&E systems between 2020 and 2022.
- We contracted with XOR Security, LLC (XOR) to assist with conducting the penetration testing for our performance audits.
- We performed our audits in accordance with generally accepted government auditing standards (GAGAS) and agreed-upon rules of engagement between OIG, XOR, and the various States.

10 Audited States and Territories



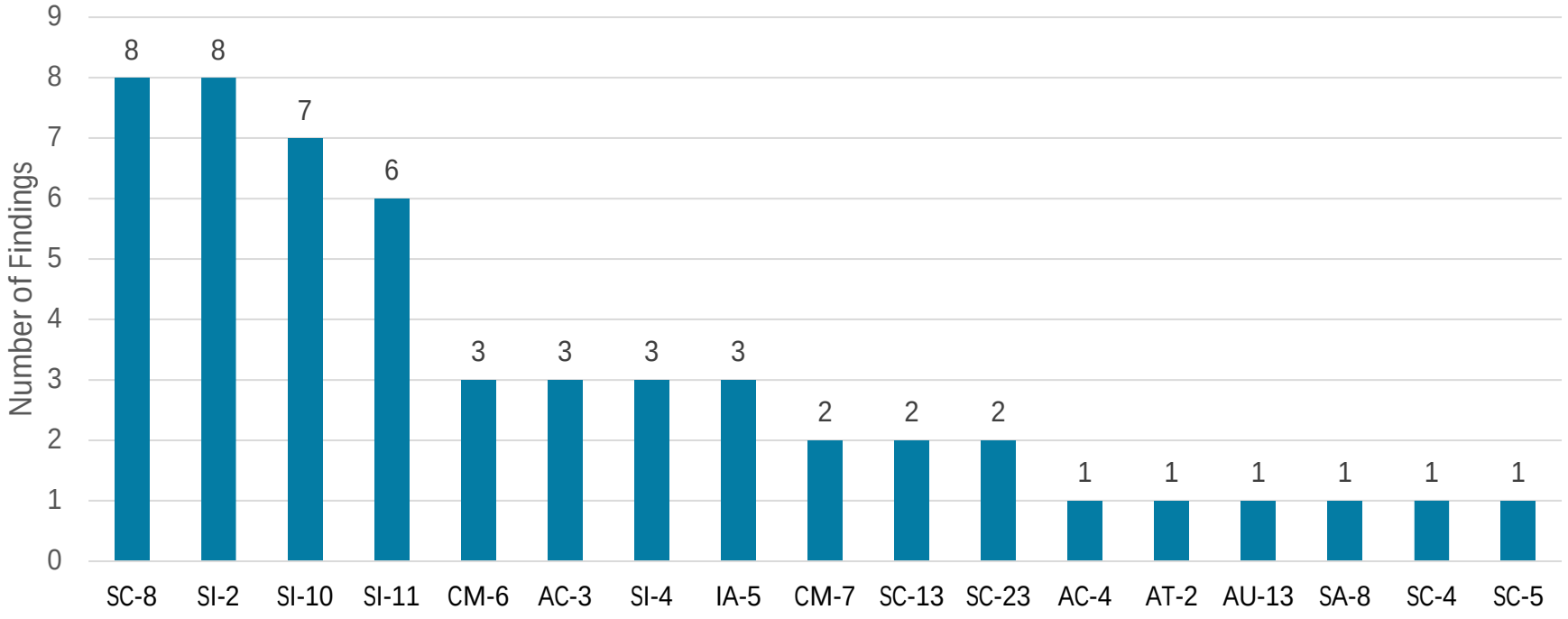
What We Found

- The 10 States implemented generally effective IT security controls for their web-facing MMIS and E&E systems to prevent unsophisticated or limited cyberattacks, but they need to continue to improve these controls to prevent more sophisticated and persistent cyberattacks.

- Cyber attackers would likely need a moderate to significant level of sophistication or complexity to compromise the State systems we audited.

- The 10 States effectively detected and responded to some of our simulated cyberattacks, but they need to improve their detection and response to other types of cyberattacks.

What We Found: 53 Total Findings Across 10 States' Systems by NIST Control



NIST SP 800-53, Revision 4, Security Controls

What We Found: Top Four NIST Controls Not Effectively Implemented in Most State MMIS and E&E Systems

Most of the States we audited did not effectively implement the following four security controls in public facing MMIS and E&E systems to mitigate risks.

- Transmission confidentiality and integrity controls in websites to ensure the protection of information transmitted. (SC-8)
- Flaw remediation controls to properly identify, report, and correct software flaws. (SI-2)
- Information input validation controls to verify the validity or properly sanitize the information system input for public-facing systems. (SI-10)
- Error handling controls to prevent disclosure of information that could be used to facilitate a cyberattack by adversaries. (SI-11)

Common Causes

- Developers or contractors were not aware of Government standards or industry best practices that require them to adhere to secure coding practices and identify and resolve flaws in systems before deploying to production.

- Certain States did not effectively implement procedures to securely configure and patch flaws timely for their production systems.

- States were not assessing all components that make up MMIS and E&E systems (e.g., outdated third-party libraries and plugins for web applications).

Common Causes (continued)

- Certain States performed ineffective testing procedures when periodically assessing the implementation of security controls in operation.

- Certain States had delays in detecting, reporting, and fixing flaws in systems, along with failure to comply with MMIS and E&E systems Federal requirements.

Potential Effects of Ineffective Controls

- Ineffective implementation of security controls in some State MMIS and E&E systems may lead to exploitation of vulnerabilities by malicious actors or insiders seeking to commit fraud, steal sensitive data, and evade detection.

- Lapses in security controls significantly increase the likelihood of successful cyberattacks and gaining unauthorized access to sensitive information.

OIG Recommendations to the States

- Overall, our recommendations to the States were aimed at improving cybersecurity controls and mitigating cybersecurity risk in MMIS and E&E systems.

- We issued 27 recommendations in total to the 10 States.

OIG Recommendations to the States (cont.)

For all 10 States we reviewed, we recommended the remediation of the security issues we identified. The recommendations included:

- update MMIS and E&E systems and software, including patching outdated servers and web applications, improving input sanitization on web applications, and ensuring server configurations supported secure protocols;
- assess and enhance tools for detecting vulnerabilities,
- enforce secure coding practices according to established guidelines, and regularly checking for compliance; and
- conduct testing and periodic evaluations to verify the effectiveness of security controls, updating cryptographic settings annually, and refining vulnerability management strategies.

States' Responses to OIG Recommendations

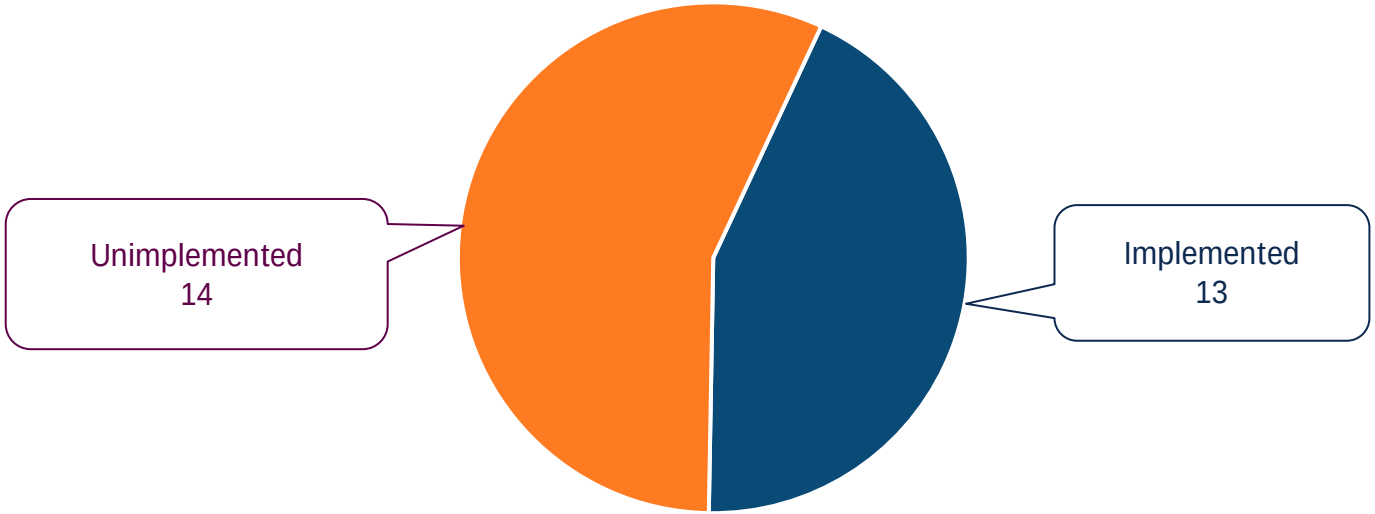
- Seven of 10 States concurred with OIG recommendations.

- Three States—Illinois, South Carolina, and South Dakota—did not indicate whether they concurred or non-concurred with our recommendations. Illinois specifically indicated that they agreed with the improvements outlined in our report and South Carolina concurred with the control findings.

- All 10 States reported that they had either fixed the weaknesses we identified or were working on resolving them at the time the reports were issued.

Implementation Status of Recommendations (as of May 2025)

27 Total Recommendations Were Issued



Note: Newly issued recommendations begin as Unimplemented. Once CMS concurs or partially concurs with the recommendation and provides evidence that the recommendation was implemented, the recommendation moves to Implemented.

CMS Comments

CMS informed us that it did not have comments on our draft report.

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

Appendix

Scope, Methodology, and Criteria

Scope

- We conducted our penetration tests of 10 States' MMIS and E&E systems between 2020 and 2022.
- Our audits focused on the internet-accessible applications and infrastructure used to support the MMIS and E&E systems.
- 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 MMIS and E&E systems.
- Each audit report described IT security control weaknesses we identified during the penetration tests. However, the penetration tests we performed may not have disclosed all internal control weaknesses that may have existed at the time of the audits.

Methodology: Adherence to GAGAS

- We conducted the 10 performance audits in accordance with GAGAS, which requires that we plan and perform the audits 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 during the prior audits provided a reasonable basis for our findings and conclusions based on our audit objectives.

Methodology

- We assessed the MMIS and E&E systems for:
  - compliance with applicable IT security control requirements, CMS Acceptable Risk Safeguards (ARS), and defined organizational policies;
  - implementation and effectiveness of security controls;
  - the existence of security vulnerabilities; and
  - exploitability of identified vulnerabilities.

- We conducted penetration tests of MMIS and E&E systems' public IP addresses and web application URLs to assess for vulnerabilities that can be used to exploit the systems.

- We conducted simulated phishing campaigns against a subset of employees at each State MMIS & E&E organization to determine whether the employees were adequately trained to recognize and appropriately respond to malicious emails.

Methodology: Use of Subject Matter Experts

- We relied on subject matter experts from XOR and our OIG team to perform the penetration tests.
- XOR planned and executed the simulated email phishing campaigns.
- We monitored XOR's work to ensure the audits followed GAGAS and agreed-upon Rules of Engagement between OIG, XOR, and the States.

Applicable Federal Criteria and Guidance

- 45 CFR § 164.306 (c) *Security standards: General rules: Standards.*
- 45 CFR § 95.621 (f) *ADP System Security Requirements and Review Process.*
- 42 CFR § 433.112 *FFP for Design, Development, Installation or Enhancement of Mechanized Processing and Information Retrieval Systems.*
- CMS's *Streamlined Modular Certification (SMC) for Medicaid Enterprise Systems Certification Guidance*, Appendix D.
- CMS's *Conditions for Enhanced Funding. R*equirements and applicable regulations published on CMS GitHub for States https://github.com/CMSgov/CMCS-DSG-DSS-Certification/tree/main/Conditions%20for%20Enhanced%20Funding.

Applicable Federal Criteria and Guidance (continued)

- CMS's *Minimum Acceptable Risk Standards for Exchanges* (MARS-E) version 2.2 (**Note**: MARS-E maps to NIST 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.)

- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations.*

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

Report Fraud, Waste, and Abuse

OIG Hotline Operations accepts tips and complaints from all sources about potential fraud, waste, abuse, and mismanagement in HHS programs. Hotline tips are incredibly valuable, and we appreciate your efforts to help us stamp out fraud, waste, and abuse.

TIPS.HHS.GOV

Phone: 1-800-447-8477

TTY: 1-800-377-4950

Who Can Report?

Anyone who suspects fraud, waste, and abuse should report their concerns to the OIG Hotline. OIG addresses complaints about misconduct and mismanagement in HHS programs, fraudulent claims submitted to Federal health care programs such as Medicare, abuse or neglect in nursing homes, and many more. Learn more about complaints OIG investigates.

How Does It Help?

Every complaint helps OIG carry out its mission of overseeing HHS programs and protecting the individuals they serve. By reporting your concerns to the OIG Hotline, you help us safeguard taxpayer dollars and ensure the success of our oversight efforts.

Who Is Protected?

Anyone may request confidentiality. The Privacy Act, the Inspector General Act of 1978, and other applicable laws protect complainants. The Inspector General Act states that the Inspector General shall not disclose the identity of an HHS employee who reports an allegation or provides information without the employee's consent, unless the Inspector General determines that disclosure is unavoidable during the investigation. By law, Federal employees may not take or threaten to take a personnel action because of whistleblowing or the exercise of a lawful appeal, complaint, or grievance right. Non-HHS employees who report allegations may also specifically request confidentiality.

Stay In Touch

Follow HHS-OIG for up to date news and publications.

 OIGatHHS

 HHS Office of Inspector General

Subscribe To Our Newsletter

OIG.HHS.GOV

Contact Us

For specific contact information, please visit us online.

U.S. Department of Health and Human Services
Office of Inspector General
Public Affairs
330 Independence Ave., SW
Washington, DC 20201

Email: Public.Affairs@oig.hhs.gov