Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

PUERTO RICO MMIS AND E&E SYSTEMS SECURITY CONTROLS WERE GENERALLY EFFECTIVE, 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

November 2022
A-18-20-08005

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The 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. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These audits help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning 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: November 2022
Report No. A-18-20-08005

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

Puerto Rico MMIS and E&E Systems Security Controls Were Generally Effective, 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 Puerto Rico 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 Puerto Rico Medicaid System or its data, and (3) Puerto Rico'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 Puerto Rico's MMIS and E&E systems from November to December 2020. The penetration test focused on the MMIS and E&E systems' public IP addresses and web application URLs. We also conducted a simulated phishing campaign that included a limited number of Puerto Rico personnel in December 2020. 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 Puerto Rico.

What OIG Found

The Puerto Rico MMIS and E&E system had reasonable security controls in place to prevent our simulated cyberattacks from resulting in a successful compromise; however, some of those security controls could be further enhanced to better prevent certain cyberattacks. Puerto Rico did not correctly implement five security controls required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

In addition, we estimated that the level of sophistication required by an adversary to compromise the Puerto Rico MMIS and E&E system was significant. At this level, an adversary would need a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks. Finally, based on the results of our simulated cyberattacks, some improvements were needed in Puerto Rico detection controls to better identify cyberattacks against its MMIS and E&E system and respond appropriately.

Potential reasons why Puerto Rico did not implement these security controls correctly may be that software developers did not follow secure coding standards to prevent security vulnerabilities or system administrators were not aware of government standards or industry best practices that require securely configuring systems before deployment to production Puerto Rico also may not have properly factored in cybersecurity risks during the design and implementation of authentication management for their MMIS and E&E systems. Additionally, Puerto Rico's procedures for periodically assessing the implementation of the NIST security controls above were not effective. By addressing the root causes of the security control failures we identified, Puerto Rico can bolster its ability to detect and prevent certain cyberattacks.

What OIG Recommends and Puerto Rico Comments

We recommend that Puerto Rico: (1) remediate the vulnerabilities related to the five security control findings identified by properly implementing and regularly assessing the associated NIST SP 800-53 controls and (2) assess the cryptographic configurations of public servers at least annually and adjust if the requirements have changed. In written comments on our draft report, Puerto Rico concurred with our recommendations and stated that it has addressed and remediated our findings. We look forward to receiving documentation from Puerto Rico through our audit follow-up process that demonstrates the recommendations have been effectively implemented.

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. Specifically, 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 Puerto Rico's MMIS and E&E system in accordance with recommendations outlined by the National Institute of Standards and Technology (NIST).[2]

OBJECTIVES

Our objectives were to determine:

- whether security controls in operation for Puerto Rico 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 Puerto Rico MMIS and E&E system or its data, and
- Puerto Rico'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 800-115. Available online at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf. Accessed on Jan. 10, 2022.

Under Federal law, each State is eligible to receive reimbursement through Federal funds for the design, development, or installation of Medicaid claims processing and information retrieval systems, including an MMIS and E&E system. States are eligible for an enhanced Federal matching rate of 90 percent for the design, development, or installation, and a 75 percent matching rate for the operation and maintenance of these systems.

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,
- beneficiary and provider inquiries and services,
- operations of claims control and computer systems, and
- management reports for planning and control.

Traditionally, State E&E systems supported 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 and care 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 Medicaid beneficiary records containing 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 Puerto Rico Health Insurance Administration (in Spanish called the Administración de Seguros de Salud de Puerto Rico, or ASES) administers Puerto Rico's Government health care delivery system, which includes Medicaid. The Puerto Rico Department of Health is the single State agency responsible for developing and administering Puerto Rico's Medicaid plan.

HOW WE CONDUCTED THIS AUDIT

We conducted a penetration test of Puerto Rico's MMIS and E&E system in November and December 2020. 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 Puerto Rico personnel in December 2020.

Additionally, we held interviews with and made inquiries to Puerto Rico officials and contractors to understand the security framework applicable to the Puerto Rico MMIS and E&E system.

To assist us with the penetration test, we relied on the work of specialists. OIG contracted with XOR Security, LLC (XOR), to assist in conducting the penetration test of the Puerto Rico 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 2020 by OIG, XOR, and Puerto Rico's Office of Information Security.

We provided detailed documentation about our preliminary findings to Puerto Rico 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, Appendix C contains State and Federal requirements and industry best practices.

FINDINGS

The Puerto Rico MMIS and E&E system had reasonable security controls in place to prevent our simulated cyberattacks from resulting in a successful compromise; however, some of those security controls could be further enhanced to better prevent certain cyberattacks. In addition, we estimated that the level of sophistication required to compromise the MMIS and E&E systems was significant.[3] At this level, an adversary would need a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks. Finally, based on the results of our simulated cyberattacks, Puerto Rico would need to improve its monitoring controls to better detect cyberattacks against its MMIS and E&E system and respond appropriately.

[3] How Do You Assess Your Organization's Cyber Threat Level? Available online at https://apps.dtic.mil/sti/pdfs/AD1137499.pdf. Accessed on October 17, 2022

State agencies operating MMIS and E&E systems are responsible for the security of operational systems involved in the administration of HHS programs and determine appropriate security requirements based on recognized industry standards or standards governing security of Federal systems and information processing.[4] Puerto Rico did not correctly implement the Federal NIST Special Publication (SP) 800-53, Revision 4, security controls in the Table below:

Table: Weak MMIS and E&E Systems Security Controls

NIST SP 800-53, Revision 4, Security Control	Security Control Finding	Control No.*	Risk Rating†
Information System Monitoring	Puerto Rico did not adequately monitor its MMIS and E&E system to detect and prevent certain attacks.	SI-4	Moderate
Cryptographic Protection	Puerto Rico did not meet FIPS-validated and/or NSA-approved cryptographic protection controls for certain public-facing systems in its MMIS and E&E system.	SC-13	Moderate
Information Input Validation	Puerto Rico did not properly sanitize or verify information system input for a public-facing system in its MMIS and E&E system.	SI-10	Moderate
Error Handling	Puerto Rico did not implement secure error handling configurations to prevent disclosure of information for its MMIS and E&E system.	SI-11	Moderate
Transmission Confidentiality and Integrity	Puerto Rico 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

* 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 OIG.

[4] 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 Oct. 6, 2022.

Potential reasons why Puerto Rico did not implement these security controls correctly may be that software developers did not follow secure coding standards to prevent security vulnerabilities or system administrators were not aware of government standards or industry best practices that require securely configuring systems before deployment to production. The security controls were not correctly implemented because Puerto Rico improperly configured its production web servers or had not updated security configurations to align with the most current security best practices for public web connections. Additionally, Puerto Rico's procedures for periodically assessing the implementation of the NIST security controls above were not effective.

As a result of Puerto Rico not correctly implementing these controls, an attacker could have extracted parts of sensitive data in client-server communications, access PII and other data contained in related websites, cause a denial-of-service, expose sensitive user documents, redirect users to malicious websites, conduct reconnaissance on neighboring systems, or identify clues that would help them better target cyberattacks.

Regarding our email phishing campaign, we sent 708 phishing emails to specific employees and determined that 19 emails were opened and 1 web link embedded in an email was clicked. This action allowed our penetration test team to successfully execute code within the user's web browser and perform some basic unauthorized data gathering against the computer. The reason for the low open and click rate could be that Puerto Rico's email filtering systems may have prevented the emails from being successfully delivered to targeted users or the users who received the emails simply did not open them during our campaign. We have shared these results as information only and encouraged Puerto Rico to investigate their email phishing controls to determine whether any improvements may be necessary.

RECOMMENDATIONS

We recommend that the Puerto Rico Department of Health:

- remediate the vulnerabilities related to the five security control findings identified by properly implementing and regularly assessing the associated NIST SP 800-53 controls, and

- assess and adjust, if necessary, at least annually, the cryptographic configurations of public servers.

PUERTO RICO'S COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments to our draft report, Puerto Rico concurred with our recommendations and stated that they were addressed and remediated. Although we have not yet confirmed whether our recommendations were effectively implemented, we are encouraged by Puerto

Rico's response and we look forward to receiving and reviewing the supporting documentation through our audit follow-up process.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

The penetration test focused on both public IP addresses and web application URLs related to the Puerto Rico MMIS and E&E system, as specified within the ROE document. Puerto Rico provided us with a list of its external and internal hosts that were related to the MMIS and E&E system.

Penetration testing began on November 9 and ended December 14, 2020, and the simulated phishing campaign began on December 1 and ended December 18, 2020.

For the simulated phishing campaign, Puerto Rico provided us with a list of 708 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. OAS contracted with XOR to conduct the penetration test of the Puerto Rico 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 Puerto Rico Medicaid agency's employees. OAS 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 Puerto Rico MMIS and E&E system. To accomplish our objectives, OIG and Puerto Rico prepared the ROE document that outlined the general rules, logistics, and expectations for the penetration test. Puerto Rico officials provided a signed ROE document indicating that Puerto Rico agreed with the rules to be followed during our testing.

In November 2020, we began reconnaissance and scope verification of network subnets owned, operated, and maintained by Puerto Rico. 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;
    - host names;
    - 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 December 2020, XOR conducted a simulated phishing campaign to determine whether Puerto Rico had implemented appropriate controls to detect and prevent successful phishing campaigns and to determine whether Puerto Rico personnel were adequately trained to recognize and appropriately respond to such malicious emails. Puerto Rico identified for us the employees who would be subject to XOR's simulated phishing campaign. The campaign was designed to send a phishing email to the 708 Puerto Rico personnel identified containing a web link to a malicious website that, when accessed, would redirect the user to a server within the HHS/OIG Cyber Range that would attempt to run code in the user's web browser and deploy more code onto the system, allowing for remote access by the penetration testers.[5]

[5] 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.

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 which 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.[6] 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.

[6] 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: STATE AND FEDERAL REQUIREMENTS AND INDUSTRY BEST PRACTICES

FEDERAL REGULATIONS

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

> (1) ADP System Security Requirement.[7] State agencies are responsible for the security of all ADP projects under development, and operational systems involved in the administration of HHS programs. State agencies shall determine the appropriate ADP security requirements based on recognized industry standards or standards governing security of Federal ADP systems and information processing.

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

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

[7] 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.

appropriate compensating security controls or explicitly accept the additional risk.

SC-13 CRYPTOGRAPHIC PROTECTION (page F-196)

Control: The information system implements organization-defined cryptographic uses and type of cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Supplemental Guidance: Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography).

SI-4 INFORMATION SYSTEM MONITORING (Page F-219)

Control: The organization:

a. Monitors the information system to detect:
    1. Attacks and indicators of potential attacks in accordance with [*Assignment: organization-defined monitoring objectives*]; and
    2. Unauthorized local, network, and remote connections;
b. Identifies unauthorized use of the information system through [*Assignment: organization-defined techniques and methods*];
c. Deploys monitoring devices:
    1. Strategically within the information system to collect organization-determined essential information; and
    2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law

enforcement information, intelligence information, or other credible sources of information;

f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

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

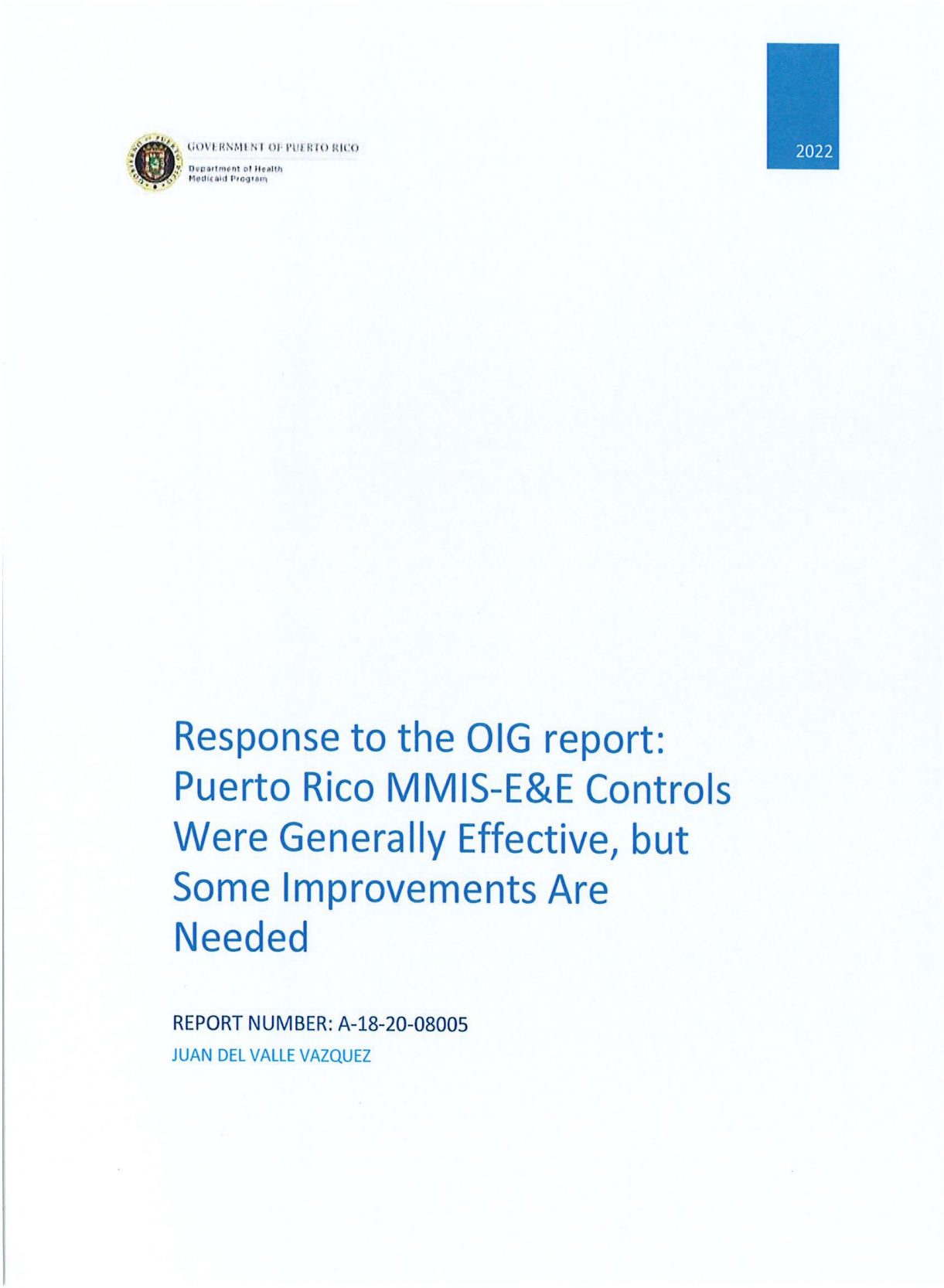
requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as 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.

INDUSTRY BEST PRACTICES

Google HSTS Preload Requirements, Submission Requirements, states:

Serve a HSTS header on the base domain for HTTPS requests:

- The max-age must be at least 31536000 seconds (1 year).
- The includeSubDomains directive must be specified.


GOVERNMENT OF PUERTO RICO
Department of Health
Medicaid Program
2022
Response to the OIG report:
Puerto Rico MMIS-E&E Controls Were Generally Effective, but Some Improvements Are Needed
REPORT NUMBER: A-18-20-08005
JUAN DEL VALLE VAZQUEZ

GOVERNMENT OF PUERTO RICO
Department of Health
Medicaid Program

Regarding the findings identified in the Pentest conducted at the end of 2020, the Puerto Rico Medicaid Program concurs with all the recommendations and confirms that they were addressed and remediated with the urgency they required. This was confirmed and validated with the different vendors maintaining and supporting the Puerto Rico Medicaid Program systems.

The Puerto Rico Medicaid Program takes the protection of the confidential information of our users and beneficiaries very seriously. As a result, we are constantly monitoring the compliance of our information systems' security and privacy controls, including those being managed and supported by our vendors.

Juan Del Valle Vazquez
Chief Information Security Officer
Puerto Rico Medicaid Program
Puerto Rico Department of Health
787-765-2929

Lcda. Dinorah Collazo Ortiz
Executive Program Director
Puerto Rico Medicaid Program
Puerto Rico Department of Health
787-765-2929

Juan Del Valle Vazquez