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

December 2024 | A-18-22-03400

The Organ Procurement and Transplantation Network IT System's Cybersecurity Controls Were Partially Effective and Improvements Are Needed

REPORT HIGHLIGHTS

December 2024 | A-18-22-03400

The Organ Procurement and Transplantation Network IT System's Cybersecurity Controls Were Partially Effective and Improvements Are Needed

Why OIG Did This Audit

- HRSA oversees the contract for the Organ Procurement and Transplantation Network (OPTN) information technology (IT) system. The OPTN IT system contains data on every U.S. organ donor, transplant candidate, and recipient, as well as outcomes related to organ transplants. Securing the OPTN IT system with effective cybersecurity controls is important to the national organ transplantation system, its data, and the patients awaiting potentially life-saving organ donations.
- This audit examined (1) whether cybersecurity controls protecting the OPTN IT system were effective in preventing certain cyberattacks, (2) the likely level of sophistication or complexity an attacker needs to compromise the OPTN IT system or data, and (3) the OPTN IT system's ability to detect attacks and respond appropriately.

What OIG Found

- Cybersecurity controls protecting the OPTN IT system were effective in preventing certain simulated cyberattacks (e.g., phishing), but the network monitoring of the OPTN IT system was not able to detect or respond appropriately to most of our simulated cyberattacks.
- We determined that it would likely take an attacker with a moderate level of sophistication to be able to compromise the OPTN IT system or data and cause significant harm.
- We identified 22 vulnerabilities associated with 16 cybersecurity controls, mostly related to network monitoring. The vulnerabilities occurred because certain federally required cybersecurity controls had not been implemented or were not operating effectively to prevent, detect, or mitigate some of our simulated cyberattacks.

What OIG Recommends

We made 4 recommendations to HRSA, including that it: require the OPTN IT system contractor to remediate the 22 vulnerabilities identified during our audit, verify that the vulnerabilities were remediated, require the contractor to improve network monitoring of the OPTN IT system, and implement procedures to help ensure that the OPTN IT system contractor is adhering to federally required cybersecurity controls policies and standards on a continuing basis. The full recommendations are in the report.

HRSA concurred with all four of our recommendations.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS AUDIT

The Organ Procurement and Transplantation Network (OPTN) information technology (IT) system facilitates the allocation and distribution of donor organs to individuals waiting for an organ transplant through the Health Resources and Services Administration (HRSA), Health Systems Bureau's Organ Donation and Transplantation program. The OPTN IT system contains data on every U.S. organ donor, transplant candidate, and recipient, as well as outcomes related to organ transplants. Securing the OPTN IT system with effective cybersecurity controls is important to protecting the national organ transplantation system, its data, and the patients awaiting potentially life-saving organ donations.

OBJECTIVES

Our objectives were to determine: (1) whether cybersecurity controls protecting the OPTN IT system were effective in preventing certain cyberattacks, (2) the likely level of sophistication or complexity an attacker needs to compromise the OPTN IT system or data, and (3) the OPTN IT system's ability to detect attacks and respond appropriately.

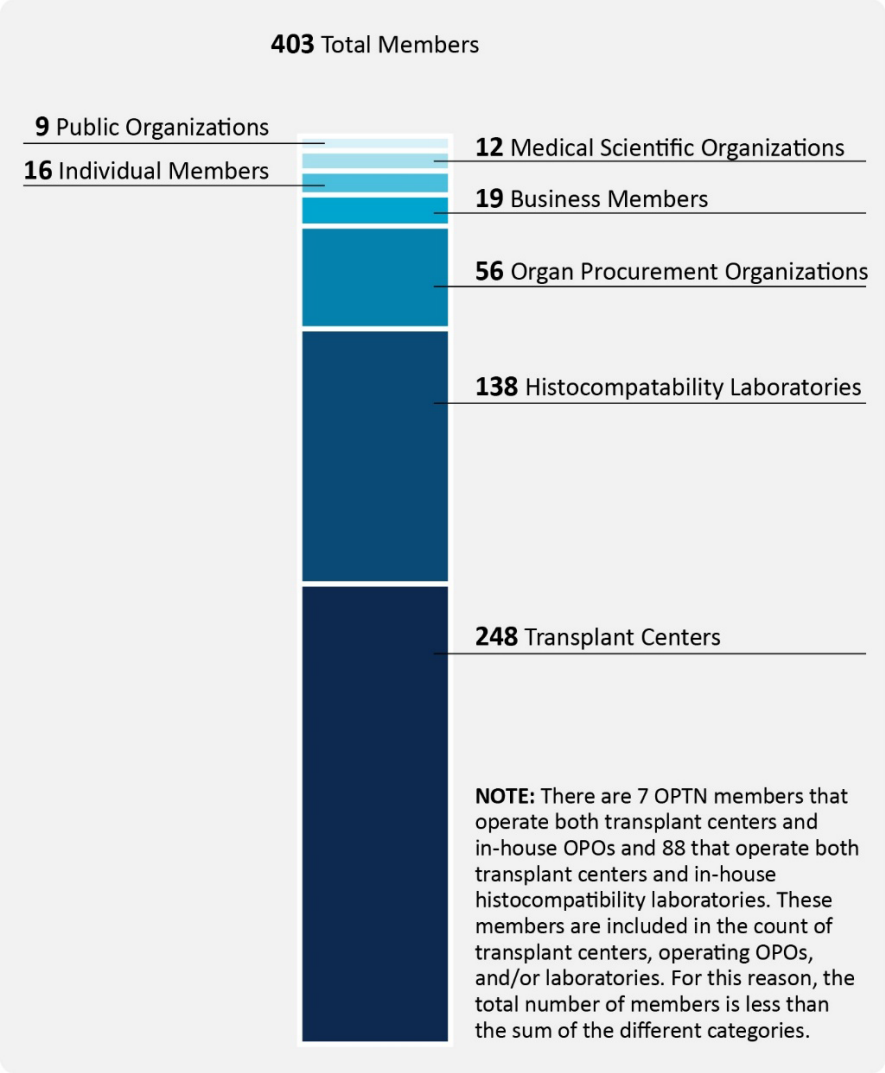
BACKGROUND

The Organ Procurement and Transplantation Network

The National Organ Transplant Act of 1984 (P.L. No. 98-507) established the OPTN to maintain a national registry for organ matching. The law also calls for the network to be operated by a private organization under Federal contract. The nonprofit organization United Network for Organ Sharing (UNOS) was awarded the OPTN contract by HRSA in 1986 and administered the OPTN during our audit period. HRSA's Health Systems Bureau provides oversight of the OPTN contract. The OPTN IT system is a key element of HRSA's Organ Donation and Transplantation program.

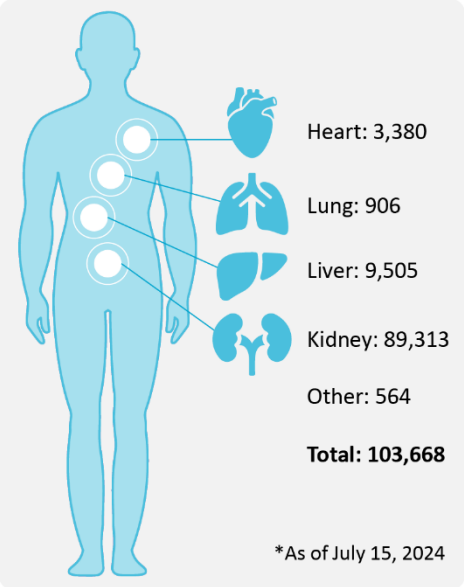
The OPTN maintains an organ allocation system for the more than 100,000 patients on the national transplant waiting list through: (1) data-driven organ allocation policy development and implementation; (2) promoting process quality improvement, by encouraging collaboration and the sharing of effective practices; and (3) technology, which is used to match donor organs to transplant candidates. Governed by a board of directors and managed by UNOS, the OPTN links public and private members who are engaged in activities related to transplants. Every transplant hospital program, organ procurement organization, and transplant histocompatibility laboratory in the United States is an OPTN member. As of July 15, 2024, the OPTN included 403 members from 7 different groups (see Figure 1 on the next page).

Figure 1: OPTN Membership by Group



During 2023, the OPTN IT system managed electronic protected health information (ePHI) associated with more than 23,000 organ donors. As of July 15, 2024, the OPTN IT system also maintained data on 103,668 waiting list candidates. See Figure 2 (next page).

Figure 2: Organ Transplant Candidate Counts



The Organ Procurement and Transplantation Network Information Technology System

The OPTN IT system, which is operated by UNOS, matches organs and individuals in accordance with OPTN policies.[1] OPTN members use the system to list patients for transplant, match patients with available donor organs, and submit required data. The OPTN IT system consists of subsystems that contain data on donated organs, organ transplant candidates, and transplantation.[2] These critical lifesaving subsystems and data are required to be protected by cybersecurity controls that mitigate various types of threats. The cybersecurity controls are designed to establish variable barriers across multiple layers such as web application firewalls to protect against internet-based cyberattacks and include network monitoring to detect and trigger responses to unusual network traffic.

HOW WE CONDUCTED THIS AUDIT

We conducted a penetration test of the OPTN IT system from April through June 2023 (audit period). The penetration test focused on the OPTN internal network and select public IP addresses. We also conducted a simulated phishing campaign that covered UNOS personnel in May 2023.

To assist us with the penetration test, we relied on the work of specialists. Specifically, OIG contracted with BreakPoint Labs, LLC (BPL), to assist in conducting the penetration test of the

[1] An IT system is a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, owned or operated on behalf of, and automated to support HHS's or an OpDiv's mission.

[2] The subsystems are used for specific functions (e.g., organ tracking).

OPTN IT system and providing subject matter expertise throughout the assessment of the system.

The penetration test consisted of authenticated and unauthenticated testing.[3] UNOS provided BPL with a system user login, as well as documentation on the system (e.g., the network's design and architecture). The goal of this testing was to emulate a real-world attacker in which the attacker has gained access to the internal network.

We performed testing in accordance with the agreed-upon Rules of Engagement document signed by OIG, BPL, HRSA and the OPTN IT system contractor. We provided detailed documentation about our preliminary findings to HRSA and the OPTN IT system contractor in advance of issuing our draft report to help enable timely remediation of the issues we identified.

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.

FINDING

During our audit period of April 2023 through June 2023, our testing revealed that cybersecurity controls protecting the OPTN IT system were effective in preventing certain simulated cyberattacks (e.g., phishing), but multiple federally required cybersecurity controls had not been implemented or were not operating effectively to prevent, detect, or mitigate some of our simulated cyberattacks. It would take an attacker with a moderate level of sophistication to compromise or cause significant harm to the OPTN IT system.[4]

We identified 22 vulnerabilities associated with 16 cybersecurity controls, mostly related to network monitoring, that if exploited could negatively impact the OPTN IT system's functionality and the security of its data. The OPTN IT system contractor did not effectively implement the following Federal National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, security controls, as described in Figure 3 (next page).

[3] Authenticated testing is when the tester has a valid system user login, which generally allows for deeper access resulting in a larger attack surface when compared to unauthenticated testing.

[4] The level of sophistication is based on MITRE's adversary threat levels (https://www.mitre.org/sites/default/files/pdf/10_2914.pdf). Moderate level is defined as the adversary having moderate resources, expertise, and opportunities to support multiple successful attacks.

Figure 3: Cybersecurity Control Findings Identified During Penetration Test

NIST SP 800-53, Revision 4, Security Control	Security Control Finding	Control No.*
Account Management	Failed to monitor the use of accounts and disable accounts that were no longer in use.	AC-2
Information Flow Enforcement	Failed to enforce approved authorizations for controlling the flow of information within the system.	AC-4
Least Privilege	Failed to prevent users from accessing portions of the information system and data that they were not authorized to have access.	AC-6
Audit Events	Failed to implement event-logging to help detect aberrant user behavior such as a user attempting to access portions of the system that the user doesn't normally access.	AU-2
Content of Audit Records	Failed to generate audit records containing information that establishes what type of event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	AU-3
Audit Review, Analysis, and Reporting	Failed to review and analyze information system audit records for indications of inappropriate, unusual, or unauthorized actions and report findings.	AU-6
Least Functionality	Failed to adhere to least functionality by allowing outdated protocols on the network.	CM-7
Identification and Authentication (Organizational Users)	Failed to require multi-factor authentication across all protocols.	IA-2
Authenticator Management	Failed to protect authenticator content from unauthorized disclosure or modification.	IA-5
Vulnerability Scanning	Failed to engage in regular vulnerability scanning on external resources.	RA-5

NIST SP 800-53, Revision 4, Security Control	Security Control Finding	Control No.*
Information in Shared System Resources	Failed to prevent unauthorized or unintended information transfer via shared system resources.	SC-4
Boundary Protection	Failed to have the information system monitor and control communications at the external boundary of the system and at key internal boundaries within the system.	SC-7
Transmission Confidentiality and Integrity	Failed to properly protect the integrity of transmitted information.	SC-8
Session Authenticity	Failed to protect the authenticity of communication sessions to protect against, for example, session theft or hijacking.	SC-23
Information System Monitoring	Failed to implement adequate network monitoring to detect unauthorized connections or to identify unauthorized use of the system.	SI-4
Information Input Validation	Failed to implement input validation for endpoint filetype uploads.	SI-10
*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.		

Additionally, HRSA's oversight procedures of the OPTN IT system contractor did not reveal the inadequately implemented or maintained federally required cybersecurity controls.

Organ Procurement and Transplantation Network Information Technology System Network Monitoring Was Not Effective Against Certain Simulated Cyberattacks

The OPTN IT system's cybersecurity controls were effective in preventing the successful execution of our phishing campaign. We executed a phishing campaign that consisted of sending an email to OPTN IT system users that contained a link to a fictitious website that would inappropriately capture a user's password when attempting to reset it. The phishing email was sent to over 500 UNOS employees who had access to the OPTN IT system. The phishing campaign did not result in successfully capturing any OPTN IT system user passwords. The OPTN IT system users who received the phishing email may have suspected that it was a

phishing email and did not click on the link or enter a password. Further, UNOS IT staff quarantined all of the emails shortly after we launched the phishing campaign.

The OPTN IT system's cybersecurity controls were also effective at preventing most of our simulated web application cyberattacks.[5] The web application security mechanisms successfully blocked our attempts to input malicious code. Conversely, our simulated web application cyberattacks uncovered 5 of the 22 vulnerabilities identified.

The OPTN IT system's networking monitoring was not effective in detecting and alerting security operators or system administrators of our execution of advanced threat actor techniques within the network in an "assumed breach scenario."[6] Our simulated cyberattacks demonstrated the potential to compromise the availability, integrity, and reliability of the OPTN IT system and its data. We identified 17 of the 22 vulnerabilities that a threat actor with authorized system user logins could exploit. For example, we were able to map out weaknesses in the identity access management environment, escalate privileges, and access sensitive personally identifiable information, source code, and system administrator credentials that gave us the ability to demonstrate a compromise of OPTN IT system functionality and data. Also, our expert-level penetration testers were able to successfully evade some protections, which demonstrated the need for the OPTN IT system to strengthen its "Defense-in-Depth" to detect and react timely to threats on the network.[7]

These vulnerabilities resulted from the OPTN IT system contractor not properly or fully implementing cybersecurity controls required by HHS and OPTN IT system contractor policies to reduce risk or mitigate threats. Further, HRSA did not identify the OPTN IT system contractor's lack of compliance with federally required cybersecurity controls that would have mitigated these vulnerabilities. The vulnerabilities we identified could have resulted in significant harm to the organ procurement and transplantation network which relies on the OPTN IT system to provide valuable life-saving services.

[5] A web application attack is an attempt by malicious actors to exploit vulnerabilities and weaknesses in web applications or mobile applications created during the software development process, with the goal of disrupting business or gaining access to an organization's IT ecosystem.

[6] The "assumed breach scenario" operates under the premise that a breach has already occurred or that an attacker has compromised the network. In this scenario, security teams simulate an attacker who operates within the context of an authorized user.

[7] "Defense-in-Depth" is an information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

RECOMMENDATIONS

We recommend that the Health Resources and Services Administration:

- require the OPTN IT system contractor to remediate the 22 vulnerabilities identified;
- verify that the 22 vulnerabilities identified were remediated;
- require the OPTN IT system contractor to improve network monitoring by implementing NIST SP 800-53, Revision 5, for the OPTN IT system, to include data loss prevention technology to prevent unauthorized exfiltration of information (Control SC-7(10)) and red-team exercises to simulate attempts by adversaries to compromise organizational systems (Control CA-8(2)); and
- implement procedures to help ensure that the OPTN IT system contractor maintains compliance with federally required cybersecurity controls policies and standards on a continuing basis.

HRSA COMMENTS

In written comments on our draft report, HRSA concurred with all four of our recommendations and described actions it has taken and plans to take to address them.

In response to our first and second recommendations, HRSA stated that it is working with the OPTN IT contractor to remediate the 22 vulnerabilities we identified. HRSA stated that it is reviewing the evidence of remediation submitted by the contractor for 17 of the vulnerabilities and expects that the remaining 5 will be remediated no later than the end of 2024.

In response to our third recommendation, HRSA stated that the contractor will resolve the related finding no later than the end of 2024. Since the penetration test, the contractor has enabled additional alerts for unauthorized exfiltration of information and implemented additional port blocks on its firewall.

In response to our fourth recommendation, HRSA stated that it hired a Federal OPTN Information System Security Officer that reports to the agency to provide oversight of security controls. In addition, the HRSA Information System Security Officer regularly monitors contractor compliance with federally required cybersecurity controls and will continue to enhance oversight.

HRSA's comments are included in their entirety as Appendix D.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

The penetration test was conducted from April 2023 through June 2023 and included:

- OPTN IT system and non-production IT system operated by UNOS,
- publicly accessible URLs identified in the agreed-upon Rules of Engagement (RoE), and
- UNOS's enterprise network/identity access management environment.

The phishing campaign was executed on May 1, 2023, and was designed to send a phishing email to over 500 UNOS staff members with OPTN IT system access.

We conducted our audit from October 2022 through August 2024.

METHODOLOGY

To accomplish our objectives, we contracted with BPL to conduct the penetration test of the OPTN IT system and the phishing campaign.

For the penetration test, the testing included the IT systems identified in the agreed-upon RoE, as well as OPTN IT system's internal network, shared resources, identity access management environment, and anything that could result in compromise over the systems listed in the RoE and the general OPTN IT system network. All tested devices were operated or maintained by UNOS or UNOS contractors. Certain simulated cyberattacks were conducted against a replica or functioning copy of the UNOS portal (i.e., non-production system) that is not used for operational work to not jeopardize the functionality of the UNOS Portal that is used for operations or the integrity of the data. UNOS provided BPL with a system user login, as well as documentation on the system, like the network's design and architecture. The goal of this scenario, known as gray-box testing, was to emulate a real-world attacker in which the attacker has gained access to the internal network. Testing of the non-production system began May 15, 2023, and concluded June 2, 2023. Limited testing of the OPTN IT system operational environment began May 1, 2023, and concluded June 2, 2023. Like the non-production system testing, BPL was granted system user logins on the internal OPTN IT system network.

The phishing campaign was conducted on May 1, 2023. BPL was provided a UNOS-created email account from which the phishing email would be sent. UNOS provided a target list of over 500 recipients. BPL sent a phishing email to the users disguised as an internal UNOS email requesting users to reset their passwords. The email included a link to a website that mimicked the UNOS portal and asked the users to input their password.

We oversaw BPL's work to ensure that all objectives were met, and that testing was performed in accordance with government auditing standards and the RoE. We also interviewed personnel from HRSA to discuss the OPTN IT system's security controls and HRSA's oversight of UNOS. We discussed the results of the penetration test and the audit with HRSA.

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[8]

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 allow users to add functionality as new exploits and tools are released.

GoPhish

GoPhish is an open-source phishing framework that can 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.

Nmap

Nmap is a free, open-source utility for vulnerability assessments, port scanning, and network mapping. For penetration testing, Nmap is primarily used as a port scanner to identify the state of any port in the environment, which can reveal the best areas to focus an attack.

[8] The identification of the tools in this appendix do not constitute or imply endorsement or recommendation by HHS OIG or its employees.

APPENDIX C: FEDERAL REQUIREMENTS

Federal Information Security Modernization Act of 2014, section 2 added section 3554 to title 41 of the U.S. Code. Section 3554 requires Federal agencies to comply with the policies, procedures, standards, and guidelines promulgated under title 40, section 11331 of the Act, which requires that Federal information systems meet the minimum information security system requirements described under section 20(b) of the National Institute of Standards and Technology Act (NIST) (15 U.S.C. 278g-3). Section 3554(a)(1)(A) states that the requirements also apply to:

‘‘(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

> ‘‘(i) information collected or maintained by or on behalf of the agency; and
>
> ‘‘(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;”

Federal Information Processing Standards, Publication 200: *Minimum Security Requirements for Federal Information and Information Systems.* These standards require that organizations apply an appropriately tailored set of baseline security controls from NIST SP 800-53, Revision 4*, Security and Privacy Controls for Federal Information Systems and Organizations*.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.* This publication covers the recommended security controls and associated assessment procedures for Federal information systems and organizations. Security controls are listed by control family.

Access Control (AC)

- AC-2 Account Management (Page F-7)
  Control: The organization:
  a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];
  b. Assigns account managers for information system accounts;
  c. Establishes conditions for group and role membership;
  d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
  e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;
  f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or

conditions];
g. Monitors the use of information system accounts;
h. Notifies account managers:
1. When accounts are no longer required;
2. When users are terminated or transferred; and
3. When individual information system usage or need-to-know changes;
i. Authorizes access to the information system based on:
1. A valid access authorization;
2. Intended system usage; and
3. Other attributes as required by the organization or associated missions/business functions;
j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

- AC-4 Information Flow Enforcement (Page F-14)
  Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].

- AC-6 Least Privilege (Pages F-18)
  Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Audit and Accountability (AU)

- AU-2 Audit Events (Page F-41)
  Control: The organization:
  a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];
  b. Coordinates the security audit function with other organizational entities requiring audit related information to enhance mutual support and to help guide the selection of auditable events;
  c. Provides a rationale for why the auditable events are deemed to be adequate to support after the fact investigations of security incidents; and
  d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].

- AU-3 Content of Audit Records (Page F-42)
  Control: The information system generates audit records containing information that

establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

- AU-6 Audit Review, Analysis, and Reporting (Page F-45)
  Control: The organization:
  a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and
  b. Reports findings to [Assignment: organization-defined personnel or roles]

Configuration Management (CM)

- 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].

Identification and Authentication (IA)

- IA-2 Identification and Authentication (Organizational Users) (Page F-90)
  Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

- IA-5 Authenticator Management (Page F-95)
  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 authenticators prior to information system installation;
  f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
  g. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type];
  h. Protecting authenticator content from unauthorized disclosure and modification;
  i. Requiring individuals to take, and having devices implement, specific security

safeguards to protect authenticators; and

j. Changing authenticators for group/role accounts when membership to those accounts changes.

Risk Assessment (RA)

- RA-5 Vulnerability Scanning (Page F-153)
  Control: The organization:
  a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported;
  b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
     1. Enumerating platforms, software flaws, and improper configurations;
     2. Formatting checklists and test procedures; and
     3. Measuring vulnerability impact;
  c. Analyzes vulnerability scan reports and results from security control assessments;
  d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and
  e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

System and Communications Protection (SC)

- SC-4 Information in Shared Resources (Page F-186)
  Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

- SC-7 Boundary Protection (Page F-188)
  Control: The information system:
  a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
  b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
  c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

- SC-8 Transmission Confidentiality and Integrity (Page F-193)
  Control: The information system protects the [Selection (one or more):

confidentiality; integrity] of transmitted information.

- SC-23 Session Authenticity (Page F-201)
  Control: The information system protects the authenticity of communications sessions.

System and Information Integrity (SI)

- 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

- SI-10 Information Input Validation (Page F-229)
  Control: The information system checks the validity of [Assignment: organization-defined information inputs].

APPENDIX D: HRSA COMMENTS

HRSA
Health Resources & Services Administration
Office of Federal Assistance and Acquisition Management
5600 Fishers Lane
Rockville, MD 20857

DATE: October 1, 2024

TO: Amy J. Fontz
Deputy Inspector General for Audit Services

FROM: Cynthia Baugh
Associate Administrator

CYNTHIA R. BAUGH -S
Digitally signed by CYNTHIA R. BAUGH -S
Date: 2024.10.01 12:58:04 -04'00'

SUBJECT: Office of Inspector General Draft Report: A-18-22-03400

Attached is the Health Resources and Services Administration's response to the above subject report. If you have any questions, please contact Sandy Seaton in the Health Resources and Services Administration's Office of Federal Assistance and Acquisition Management at (301) 443-2432.

Attachments

OIG Draft Report A-18-22-03400

Below please find the Health Resources and Services Administration's (HRSA) response to the Office of Inspector General's (OIG) draft report on the Organ Procurement and Transplantation Network (OPTN) Information Technology System.

OIG RECOMMENDATION #1 and #2

- Require the OPTN IT system contractor to remediate the 22 vulnerabilities identified; and
- Verify that the 22 vulnerabilities identified were remediated.

HRSA RESPONSE

Concur.

Status: Partially Complete.

HRSA promptly worked with the OPTN IT contractor on these findings and the contractor reported remediation of 17 of the 22 findings. HRSA is actively reviewing the evidence of the remediation submitted by the OPTN contractor for compliance. Further findings are expected to be remediated by no later than the end of the year. As part of HRSA's OPTN Modernization Initiative, HRSA is focused on developing a modernized OPTN IT system, while strengthening the legacy system during the transition.

OIG RECOMMENDATION #3

- Require the OPTN IT system contractor to improve network monitoring by implementing NIST SP 800-53, Revision 5, for the OPTN IT system, to include data loss prevention technology to prevent unauthorized exfiltration of information (Control SC-7(10)) and red-team exercises to simulate attempts by adversaries to compromise organizational (Control CA-8(2)).

HRSA RESPONSE

Concur.

Status: Partially Complete.

The contractor will resolve this finding by no later than December 30, 2024. On February 16, 2024, HRSA completed its evaluation of the OPTN system under NIST SP 800-53, Revision 5 security controls. Since the OIG penetration test, the OPTN contractor enabled additional alerts for unauthorized exfiltration of information (Control SC-7(10)) which are monitored by the contractor's staff. The contractor has also implemented additional port blocks on its firewall.

Annual penetration tests of the OPTN system are conducted by HRSA using the HHS provided service (Control CA-8(2)).

OIG RECOMMENDATION #4

Implement procedures to help ensure that the OPTN IT system contractor maintains compliance with federally required cybersecurity controls policies and standards on a continuing basis.

HRSA RESPONSE

Concur.

Status: Complete.

HRSA is committed to protecting the security of organ transplantation data. HRSA hired a federal OPTN Information System Security Officer reporting to the agency, to provide oversight of security controls, security procedures, security deliverable schedules, and security compliance assessments. The HRSA Information System Security Officer regularly monitors contractor compliance with federally required cybersecurity controls policies and standards and will continue to enhance oversight as part of the agency's OPTN Modernization Initiative.

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