Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

THE HEALTH RESOURCES AND SERVICES ADMINISTRATION SHOULD IMPROVE ITS OVERSIGHT OF THE CYBERSECURITY OF THE ORGAN PROCUREMENT AND TRANSPLANTATION NETWORK

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

Amy J. Frontz
Deputy Inspector General
for Audit Services

August 2022
A-18-21-11400

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: August 2022
Report No. A-18-21-11400

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

The Health Resources and Services Administration Should Improve Its Oversight of the Cybersecurity of the Organ Procurement and Transplantation Network

Why OIG Did This Audit

The Organ Procurement and Transplantation Network (OPTN) is part of the Health Resources and Services Administration (HRSA) national system that allocates and distributes donor organs to individuals waiting for an organ transplant. OPTN is a public-private partnership that links all professionals involved in the U.S. donation and transplantation system.

Our objective was to determine whether HRSA implemented selected cybersecurity controls over the OPTN to protect the confidentiality, integrity, and availability of transplant data, in accordance with Federal requirements.

How OIG Did This Audit

We reviewed a selected number of general information technology (IT) controls that the United Network for Organ Sharing (UNOS) had implemented for the OPTN and determined whether HRSA was providing adequate oversight to ensure the general IT controls were implemented in accordance with Federal requirements. To accomplish our objective, we requested and reviewed general IT controls documentation over OPTN provided by UNOS and HRSA for only the selected controls. In addition, we interviewed personnel from HRSA and UNOS and obtained demonstrations of those selected OPTN general IT controls.

What OIG Found

HRSA had ensured that most of the general IT controls that we selected to test were implemented for OPTN by UNOS to protect the confidentiality, integrity, and availability of transplant data in accordance with Federal requirements. However, we identified areas for which HRSA could improve its oversight of UNOS to ensure that all Federal cybersecurity requirements are being met in a timely manner. We noted that HRSA could improve its oversight of UNOS to ensure that UNOS performs adequate reviews of local user access of the OPTN, and that certain key cybersecurity policies and procedures were finalized and in place.

What OIG Recommends and HRSA's Comments

We recommend that HRSA develop additional oversight controls and procedures (e.g., deliverable schedules, compliance assessments, and monitoring) to ensure that the OPTN contractor complies with all Federal cybersecurity requirements and implements security controls over the OPTN in an effective and timely manner.

HRSA stated that it has made efforts to continuously strengthen its oversight and controls over OPTN. HRSA added a federal employee to serve as the OPTN Information System Security Officer to provide oversight of security controls, security procedures, security deliverable schedules, and security compliance assessments. In addition, HRSA indicated it has taken action to finalize the policies and procedures that were in draft during our audit and improve the access controls of OPTN.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS AUDIT

The Organ Procurement and Transplantation Network (OPTN) is part of the Health Resources and Services Administration (HRSA) national system that allocates and distributes donor organs to individuals waiting for an organ transplant. The United Network for Organ Sharing (UNOS), the contractor that administers the OPTN, is responsible for managing systems that contain data on every U.S. organ donor, transplant candidate, recipient, and outcome. The confidentiality, integrity, and availability of the systems for ensuring effective matching in a timely manner are critical to patients awaiting organ donation. The Department of Health and Human Services (HHS) designated OPTN as a High Value Asset.

OBJECTIVE

Our objective was to determine whether HRSA implemented selected cybersecurity controls over the OPTN to protect the confidentiality, integrity, and availability of transplant data, in accordance with Federal requirements.

BACKGROUND

Health Resources and Services Administration

HRSA is an agency within HHS. HRSA consists of 18 bureaus and offices; its programs support health care for people who are geographically isolated or economically or medically vulnerable. HRSA, through its Health Systems Bureau (HSB), oversees programs for facilitating organ, bone marrow, and cord blood transplantation. The HSB's Organ Donation and Transplantation program extends and enhances the lives of individuals with end-stage organ failure for whom an organ transplant is the most appropriate therapeutic treatment. The OPTN is a key element of the Organ Donation and Transplantation program.

The HRSA Chief Information Security Officer (CISO) is responsible for ensuring that all federally required cybersecurity controls are in place for the OPTN. According to HRSA, before 2018, neither the OPTN contract nor the National Organ Transplant Act (NOTA) included cybersecurity requirements and standards, such as those included in National Institute of Standards and Technology (NIST) standards and the Federal Information Systems Modernization Act (FISMA). According to HRSA officials, because HRSA did not believe it could compel compliance with these requirements before 2018, it conducted only limited oversight of the OPTN's cybersecurity.

In 2018, HRSA modified the contract with UNOS to require that it follow FISMA and NIST, which allowed HRSA to increase its cybersecurity oversight of OPTN to include monitoring compliance with FISMA and NIST, in addition to the annual security assessments it said were being performed. HRSA said that it begins its security assessments by reviewing all controls that

require annual testing. Then it breaks up the remaining controls by thirds, grouping families with overlap and responsible parties together. In addition, HRSA tracks the selections in a spreadsheet to ensure that it tests all the annual controls annually and all the others at least every 3 years.

In 2020, the most recent assessment included 141 of the 385 NIST Special Publication (SP) 800-53 controls.[1] In addition, HRSA used a third party to conduct vulnerability scans of the OPTN.[2] HRSA provided support to show that it tracks the issues identified during assessments, scans, and other reviews of the OPTN, and that it worked with UNOS to resolve vulnerabilities.

National Organ Transplant Act

In 1984, Congress passed the NOTA to address the Nation's critical organ donation shortage and improve the organ-matching and -placement process. NOTA established the OPTN to maintain a national registry for organ matching. The NOTA also called for OPTN to be operated by a private, nonprofit organization under Federal contract. In 1986, HHS awarded the initial contract to UNOS, which continues to administer the OPTN.

Organ Procurement and Transplantation Network

The OPTN is owned by UNOS. The OPTN is a public-private partnership that links professionals involved in the U.S. donation and transplantation system, which includes transplant centers, organ procurement organizations, and labs. (Figure 1 on the next page shows the types of OPTN members.) In 2021, the OPTN maintained data associated with more than 20,400 donors. As of January 18, 2022, the OPTN maintained data on 106,500 waiting-list candidates (Figure 2, next page).

[1] A control family is a group of security controls related to the general security topic of the family. Control families are closely aligned with the 17 minimum security requirements for Federal information and information systems in the Federal Information Processing Standards Publication 200.

[2] Vulnerability scanning is the process of discovering, analyzing, and reporting on security flaws and vulnerabilities. Scans are conducted via automated vulnerability scanning tools to identify potential risk exposures and attack vectors across an organization's networks, hardware, software, and systems.

Figure 1: OPTN Membership

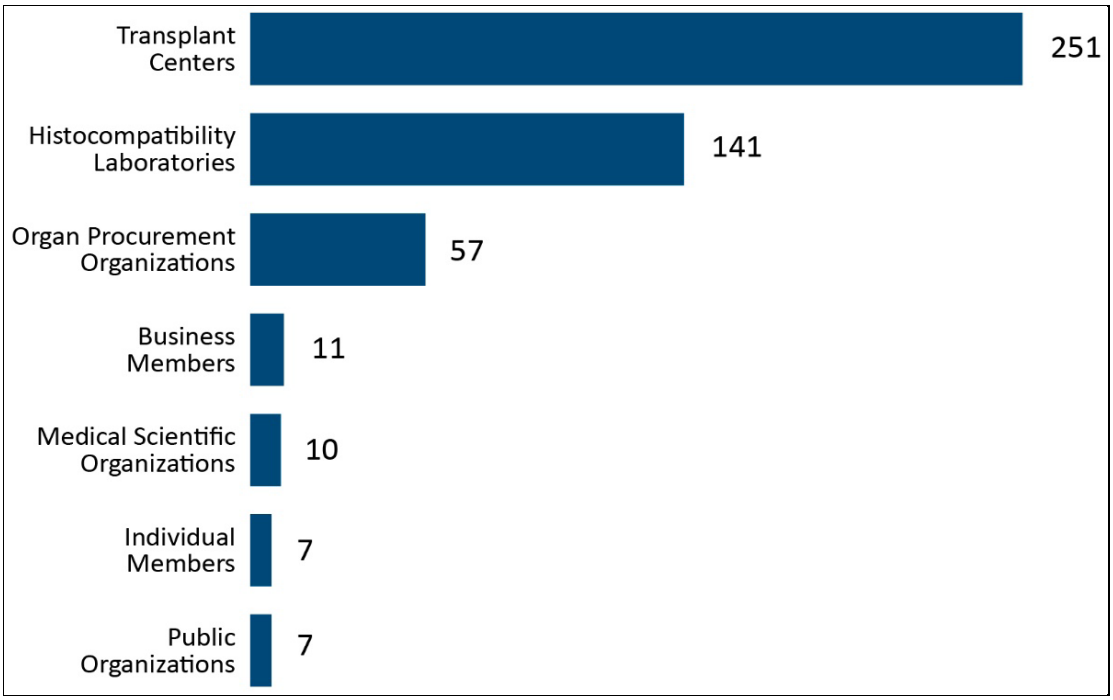
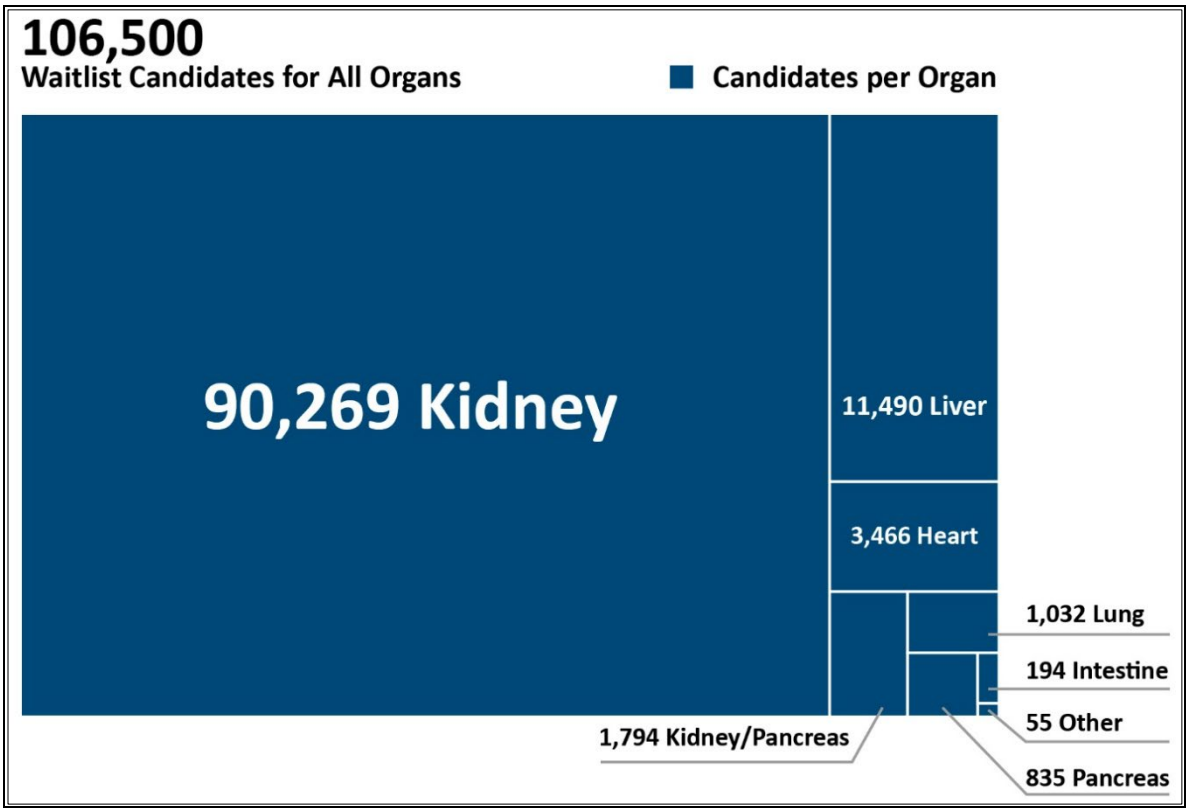


Figure 2: Waiting List Candidates by Organ[3]



[3] Donor and waiting list candidate data obtained from OPTN at https://optn.transplant.hrsa.gov/data/view-data-reports/national-data/. Accessed on Jan. 18, 2022.

HOW WE CONDUCTED THIS AUDIT

We designed our audit to determine whether HRSA provided adequate oversight over UNOS's implementation of cybersecurity; our audit was not an assessment of all organizational internal or general information technology (IT) controls and did not include technical testing. We reviewed a selected number of general IT controls that UNOS had implemented for OPTN and determined whether HRSA provided adequate oversight to ensure the general IT controls were implemented in accordance with Federal requirements. To accomplish our objective, we requested and reviewed general IT controls documentation over OPTN provided by UNOS and HRSA for only the selected controls. In addition, we interviewed personnel from HRSA and UNOS and observed demonstrations of those selected OPTN general IT controls.

We assessed selected general IT controls to determine whether HRSA ensured that UNOS complied with the requirements of the NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

The following are the general IT controls areas we selected; within these control areas, we reviewed specific actions taken for this audit:

- System security plan (SSP) – The formal document that provides an overview of the security requirements for an IT system and describes the security controls in place or planned for meeting those requirements.

- Risk assessment – The process of identifying and documenting the risks to an information system; it is part of risk management and incorporates threat and vulnerability analyses.

- Access controls – The process of granting or denying specific access requests to obtain data, use data, and/or view data.

- Configuration management – A collection of activities to maintain the integrity of the system.

- System monitoring – A review of cyber incidents that occur at the system boundary (i.e., the firewall).

- Flaw remediation – The identification, reporting, and correction of information system flaws (sometimes through patching).

- Vulnerability assessment – A systematic examination of an IT system or product to determine the adequacy of security measures; this examination often occurs through system scans.

In addition, we reviewed two penetration tests of OPTN. UNOS hired a third-party information security firm to perform a test in 2020 and hired another firm in 2021 of which the tests had a different scope of work.[4] We verified that the findings from these penetration tests were included in HRSA's plan of action and milestones (POA&Ms).[5, 6]

We also reviewed supporting documentation for selected OPTN controls described in the OPTN SSP to verify whether UNOS had described the implementation of those controls and whether HRSA adequately tested the controls during its annual security assessment to confirm they were in place and operating effectively.

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 scope and methodology, and Appendix B contains Federal requirements.

FINDINGS

HRSA had ensured that most of the general IT controls that we selected to test were implemented for OPTN by UNOS to protect the confidentiality, integrity, and availability of transplant data in accordance with Federal requirements. However, we identified areas for which HRSA could improve its oversight of UNOS to ensure that all Federal cybersecurity requirements are being met in a timely manner.

HRSA DID NOT ENSURE THAT SOME FEDERALLY REQUIRED CYBERSECURITY CONTROLS WERE IN PLACE FOR THE ORGAN PROCUREMENT AND TRANSPLANTATION NETWORK

HRSA could improve its oversight of UNOS to ensure that UNOS performs adequate reviews of local user access of the OPTN, and that certain key cybersecurity policies and procedures were finalized and in place. In addition, HRSA lacked adequate oversight procedures for UNOS to ensure that all Federal cybersecurity requirements were being met in a timely and effective

[4] 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.

[5] A POA&M is a document that identifies tasks that need to be accomplished to remediate a weakness or gap in controls. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

[6] The testing was conducted on UNOS's information systems, which included some areas that are outside of the OPTN boundary. Therefore, not all the findings noted in the summary of the penetration test are included in HRSA's POA&Ms because they addressed only the findings related to the OPTN.

manner. HRSA stated that there were limitations on and a lack of clarity of HRSA's responsibilities over OPTN in the previous and current contract and in the NOTA.
NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* requires that organizations develop, document, disseminate, review, and update policies and procedures for each security control family. The policies should address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The procedures should facilitate the implementation of the policies and the controls associated with the control family. NIST gave the policy and procedure controls the highest priority code, which means that an organization should implement the policy and procedure controls first.

UNOS's policies and procedures for the following controls were either in draft or did not exist:

- Access controls – Policies and procedures were in draft and going through the approval process.

- Risk assessment – Policies and procedures were in draft and were estimated to be finalized by the end of third quarter 2022.

- System monitoring – There were no policies or procedures.

During our audit, HRSA took a proactive step by creating a POA&M to address the lack of policy and procedure documentation for certain security control families, including the controls that we identified.

We also found that there is a high risk of local site administrators not deactivating local site user accounts in a timely manner. The only assurance that site administrators deactivated local site user accounts was an annual user account audit that was conducted by the local site administrator. Therefore, a terminated user's account could still be active and used to access the OPTN for up to a year after termination, which would not be considered a timely deactivation, especially considering that bad actors leverage dormant but still active accounts to improperly access systems and data.

Without finalized, written policies and procedures, there is a high risk that UNOS staff may not fully understand or perform as intended their roles and responsibilities as they pertain to certain cybersecurity controls, or that the OPTN will not comply with NIST controls as required by the FISMA. A lack of finalized, written policies and procedures could result in essential cybersecurity controls not being implemented properly or at all. Some of the controls assist in the timely detection of a cybersecurity attack or verify that access is restricted and the integrity of the organ matching process is maintained. In addition, because of the critical role of the OPTN and the sensitive data it contains, a security breach could have significant consequences for vulnerable patients.

RECOMMENDATION

We recommend that HRSA develop additional oversight controls and procedures (e.g., deliverable schedules, compliance assessments, and monitoring) to ensure that the OPTN contractor complies with all Federal cybersecurity requirements and implements security controls over the OPTN in an effective and timely manner.

HRSA COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments on our draft report, HRSA stated that it has taken the following actions as part of its efforts to continuously strengthen its oversight and controls over OPTN. HRSA added a Federal employee to serve as the OPTN Information System Security Officer (ISSO) to provide oversight of security controls, security procedures, security deliverable schedules, and security compliance assessments. The HRSA OPTN ISSO is responsible for working with UNOS to ensure that the OPTN system maintains the SSP and other security documents, mitigates findings, implements POA&Ms, performs security updates, and continuously monitors security controls for the system. In addition, HRSA indicated that it has taken action to finalize the policies and procedures that were in draft during our audit and improve the access controls of OPTN.

We are encouraged that HRSA has taken steps to improve its oversight controls and procedures of the OPTN and the OPTN contractor.

HRSA's comments are included in their entirety in Appendix C.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We tested the following general IT controls of the OPTN:

- System security plan – Determined whether the SSP included the IT security controls required for a high-risk system.

- Risk assessment – Reviewed policies and procedures for conducting risk assessments and determined whether UNOS had conducted risk assessments of the OPTN.

- Access controls – Reviewed policies and procedures related to access controls and observed demonstrations of select access controls that were in place over the OPTN for UNOS personnel and local site users.

- Configuration management – Reviewed policies and procedures related to configuration management and determined whether a configuration management plan that included current configuration baselines[7] for its operating systems was maintained.

- System monitoring – Determined whether UNOS had policies and procedures related to system monitoring and had system monitoring tools in place for the OPTN.

- Flaw remediation – Reviewed the policies and procedures for addressing system flaws and determined whether tools were being used for flaw remediation.

- Vulnerability assessments – Determined whether there were vulnerability assessment processes, including vulnerability scans being performed on a set schedule, and whether POA&Ms were created for identified weaknesses.

We conducted our audit work from March 2021 through May 2022.

METHODOLOGY

To accomplish our objective:

- We reviewed:

    - IT security documentation related to OPTN to determine whether selected controls were implemented in accordance with Federal requirements;

[7] Configuration baselines are a documented set of specifications for a system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.

- two OPTN penetration test reports, which were completed for UNOS by third parties in 2020 and 2021, to determine whether any vulnerabilities were identified;

- supporting documentation from HRSA for selected cybersecurity controls in the 2019 OPTN SSP that HRSA reviewed in its 2019 and 2020 security assessments; and

- documentation from UNOS for selected controls listed in the 2019 OPTN SSP that were not part of HRSA's recent security assessments.

- We interviewed personnel from HRSA to discuss cybersecurity controls over OPTN and their oversight of UNOS.

- We interviewed UNOS personnel and observed demonstrations of selected OPTN cybersecurity controls.

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: FEDERAL REQUIREMENTS

Federal Information Security Modernization Act of 2014, Section 3554. Agencies must 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 (15 U.S.C. 278g-3).

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 covers the recommended security controls and associated assessment procedures for Federal information systems and organizations. Security controls are listed by control family.

Control families include but are not limited to:

- access control,
- configuration management,
- identification and authentication,
- incident response,
- personnel security,
- risk assessment,
- security assessment and authorization, and
- system and information integrity.

Agencies are required to have written policies and procedures for the minimum-security controls, which are determined by the impact baseline of the information system. The first security control in each family generates requirements for specific policies and procedures that are needed for the effective implementation of the other security controls in the family.

APPENDIX C: HRSA COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Health Resources and Services Administration

Rockville, MD 20857

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

FROM: HRSA Administrator

DATE: July 22, 2022

SUBJECT: Office of Inspector General Draft Report titled, "The Health Resources and Services Administration Should Improve Its Oversight of the Cybersecurity of the Organ Procurement and Transplantation Network, A-18-21-11400"

Attached is the Health Resources and Services Administration's (HRSA) response to the Office of Inspector General draft report titled, "The Health Resources and Services Administration Should Improve Its Oversight of the Cybersecurity of the Organ Procurement and Transplantation Network, A-18-21-11400." If you have any questions, please contact Sandy Seaton in HRSA's Office of Federal Assistance Management at (301) 443-2432.

Carole Johnson, HRSA Administrator

Health Resources and Services Administration's Comments on the OIG Draft Report – *The Health Resources and Services Administration Should Improve Its Oversight of the Cybersecurity of the Organ Procurement and Transplantation Network* (A-18-21-11400)

The Health Resources and Services Administration (HRSA) appreciates the opportunity to respond to the above draft report. HRSA's response to the Office of Inspector General (OIG) draft recommendation is as follows:

OIG Recommendation

We recommend that HRSA develops additional oversight controls and procedures (e.g., deliverable schedules, compliance assessments, and monitoring) to ensure that the OPTN contractor complies with all Federal cybersecurity requirements and implements security controls over the OPTN in an effective and timely manner.

HRSA Response

HRSA is committed to protecting the confidentiality, integrity, and availability of transplant data, in accordance with all federal requirements. As the draft report notes, HRSA ensured that most of the cybersecurity controls selected by the OIG to test were implemented for the OPTN by UNOS to protect the confidentiality, integrity, and availability of transplant data in accordance with federal requirements. HRSA has taken the following actions as part of the Agency's efforts to continuously strengthen oversight and controls:

- On March 26, 2022, HRSA added a federal employee to serve as OPTN Information System Security Officer (ISSO) to provide oversight of security controls, security procedures, security deliverable schedules, and security compliance assessments. The HRSA OPTN ISSO is responsible for working with UNOS to ensure that the OPTN system maintains the System Security Plan and other security documents, mitigates findings, implements Plans of Action and Milestones (POAMs), performs security updates, and continuously monitors security controls for the system.
- Where specific policies and procedures noted in the draft report existed in draft form, HRSA has taken action to finalize these documents.

HRSA also has ensured that for the OPTN, UNOS implemented two factor authentication for all users. Multifactor authentication was added to the onboarding process, which includes verification of the account owner by UNOS and the OPTN member organization representative. Finally, HRSA will create POAMs to ensure the offboarding process disables and remove inactive user accounts from the OPTN system within an appropriate timeline.