OPTN

Briefing to the OPTN Board of Directors on

Establish Member System Access, Security Framework, and Incident Management and Reporting Requirements

OPTN Network Operations Oversight Committee

Prepared by: Courtney Jett and Terri Helfrich
UNOS Policy and Community Relations Department

Table of Contents

Establish Member System Access, Security Framework, and Incident Management and Reporting Requirements

Affected Policies:	*1.2: Definitions*
	3.1: Access to the OPTN Computer System
Sponsoring Committee:	*Network Operations Oversight*
Public Comment Period:	*January 19, 2023 – March 15, 2023*
Board of Directors Meeting:	*June 26, 2023*

Executive Summary

The OPTN Network Operations Oversight Committee (NOOC) aims to establish member system access and security framework requirements to enhance the security of the OPTN Computer System. These requirements will address the following:

- Security framework and controls for all members with access to the OPTN Computer System
- Self-attestation from members on the security framework in place
- Auditing and compliance monitoring for security requirements
- Security requests for information
- Development of an incident response plan, required actions for a security incident
- Establishment of an information security contact role
- Security training for all member organization staff

While the OPTN Computer System is already extremely secure, these additional measures will help address issues observed in the transplant community and achieve compliance with modifications to the OPTN Contract.

Purpose

The goal of this proposal is to enhance the security of the OPTN Computer System by reducing risk of member security incidents and to develop expectations in members' notification to the OPTN and resolution of security incidents. This proposal will increase accountability for securing the OPTN Computer System by creating OPTN member-level accountability for individual users' access. Increasing the security of the OPTN Computer System protects candidate, recipient, and donor data, and increases public trust. Furthermore, these additions are necessary to address modifications made to the OPTN Contract as required by Health Resources and Services Administration (HRSA).[1]

Background

In a survey of 381 healthcare IT professionals, there was a reported 94% increase in ransomware attacks on healthcare organizations between 2020 and 2021.[2] According to this survey, the healthcare industry saw both the highest increase in the volume and complexity of cyber-attacks. OPTN members are among those who have experienced cybersecurity incidents,[3,4] but the OPTN does not currently have a requirement for members to notify the OPTN of such incidents, nor a mechanism established for such a notification. Such a notification would allow for a faster response and a more in-depth evaluation of the members' recent interactions and the potential effect on the OPTN Computer System, to ensure the integrity of the data and availability of the system, which is critical for the process of organ allocation and transplantation.

The OPTN Contract includes strict vulnerability management requirements to maintain the OPTN Computer System, including adherence to Binding Operational Directives from the Cybersecurity and Infrastructure Security Agency (CISA), an agency of the United States Department of Homeland Security (DHS).[5] The CISA has a Coordinated Vulnerability Disclosure (CVD) process to disseminate information on such vulnerabilities and maintains a catalog of Known Exploited Vulnerabilities (KEV), which are vulnerabilities that are being actively exploited.[6] The CISA recommends that all stakeholders prioritize remediating these vulnerabilities, due to their higher level of risk. Historically, the OPTN has not developed member requirements for information security. Given recent changes in the healthcare cybersecurity landscape and modifications to the OPTN contract, the Committee submits this proposal.

---

[1] By contract with the Department of Health and Human Services, the OPTN Computer System is a contractor-owned, contractor-operated system. The OPTN contractor owns the computer system that is used as the OPTN Computer System. Requirements for the performance and maintenance of the OPTN Computer System are embedded in the OPTN contract (HHSH250201900001C). HHS recently modified the OPTN contract to require the OPTN Contractor to undertake additional security measures for the OPTN Computer System, including working with the NOOC to establish membership requirements for those members interacting with the OPTN Computer System.

[2] Rep. *The State of Ransomware in Healthcare 2022*. Abingdon, VA: Sophos, 2022.

[3] Dan Margolies. "Ransomware Attack on Midwest Transplant Network Affects More than 17,000". National Public Radio Kansas City, May 3, 2021. https://www.kcur.org/health/2021-05-03/ransomware-attack-on-midwest-transplant-network-affects-more-than-17-000 (Accessed December 9, 2022).

[4] Kat Jercich. "Nevada hospital ransomware attack could affect data of 1.3M patients". Healthcare IT News, August 23, 2021. https://www.healthcareitnews.com/news/nevada-hospital-ransomware-attack-could-affect-data-13m-patients (Accessed December 9, 2022).

[5] The OPTN Contractor must comply with the HHS Policy for the High Value Asset (HVA) Program, which includes compliance with CISA Binding Operational Directive 18-02 (https://www.cisa.gov/binding-operational-directive-18-02), which addresses remediation of identified vulnerabilities.

[6] https://www.cisa.gov/known-exploited-vulnerabilities. Accessed December 12, 2022.

OPTN members are critical stakeholders of the OPTN Computer System, and as such, it follows that the OPTN members should contribute to the reduction of risk to the security of the OPTN Computer System.

OPTN policies and bylaws do not define member organization requirements for security of the member environment that interacts with the OPTN Computer System. Individuals are bound by the OPTN Contractor's System Terms of Use,[7] but member organizations are not. The Systems Terms of Use does not cover broader security requirements that are more applicable to organizations than individuals. Throughout this proposal, "member" will refer to the OPTN member organization with access to the OPTN Computer System, and "individual" will refer to individuals within that member organization or that access the OPTN Computer System.

The Committee is proposing the initial security framework and controls be based on the National Institute of Standards and Technology (NIST) Special Publication 800-171: *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*.[8] NIST is an agency of the United States Department of Commerce that develops and distributes industry standards for technology and business. There are 110 controls, or measures which modify risk, in NIST Special Publication (SP) 800-171, covering the following categories:

- Access management
- Awareness and training
- Audit and accountability
- Configuration management
- Identification and authentication
- Incident response
- Maintenance
- Media protection
- Personnel security
- Physical protection
- Risk assessment
- Security assessment
- System and communications protection
- System and information integrity

In addition, recent modifications to the OPTN Contract require the OPTN Contractor to work with the NOOC to establish security frameworks for OPTN members, develop annual training requirements, and perform routine security audits. The modifications also require that the OPTN Contractor and the NOOC develop member requirements for response to security requests for information, notification to the OPTN of security incidents, and annual self-attestation to compliance with the security framework.[9]

[7] https://unos.org/wp-content/uploads/2018-UNOS-Systems-Terms-of-Use.pdf.
[8] National Institute of Standards and Technology (NIST). "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations". Special Publication. February 2020, https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final (Accessed December 11, 2022).
[9] OPTN Contract, HHSH250201900001C, Performance Work Statement (PWS) Task *3.2.5.5: OPTN BOD Network Operations Oversight Committee.*

Proposal for Board Consideration

This proposal is intended to enhance the overarching security of the OPTN Computer System and security of OPTN member organizations who use the OPTN Computer System through multiple proposed requirements. The requirements address the following:

- Security framework and controls for all members with access to OPTN Computer Systems
- Readiness assessment and self-attestation from members on the security framework in place
- Auditing and compliance monitoring for security requirements
- Security requests for information
- Development of an incident management response plan, as well as required actions for a security incident
- Establishment of an information security contact role
- Security training for all individuals with access to the OPTN Computer System

In addition, the Committee is proposing a transition period for the initial appointment of an information security contact and completion of the member's readiness assessment.

Third-party organizations that access the OPTN Computer System on a member's behalf will be addressed in a subsequent proposal.

Member Security Framework and Controls

All members will be expected to, at minimum, follow all of the NIST SP 800-171[10] framework controls and the OPTN specified minimum control values. Members who are compliant with other security frameworks must show that all 110 controls required by NIST SP 800-171 are covered though a crosswalk between frameworks. **Appendix A** contains an overview of the controls outlined in NIST SP 800-171, which can be found in more detail in the special publication. The Committee initially proposed OPTN minimum control values, maintained by the OPTN and regularly reviewed by the Committee. However, upon further discussion the Committee decided that determining members' current levels of information security would be the first step prior to determining minimum control values.

When developing policies and procedures in alignment with these controls, members will need to consider factors such as:

- How to evaluate the system against the security framework, identify gaps, and work towards remediation
- How to reduce risk when individuals are accessing the member environment or OPTN Computer System via personal devices
- How to reduce risk when individuals are accessing the member environment or OPTN Computer System via remote locations or networks, such as donor hospitals
- How to operationalize notification of security incidents to the OPTN
- How to continue secure access in the event of a security incident
- How to operationalize the notification of security incidents from software vendors, Electronic Medical Record (EMR) or Laboratory Informatics System (LIS) vendors, and others

[10] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

Due to the vast array of potential solutions for each requirement, this proposal does not dictate how to operationalize these controls. Each member will develop their solution based on their current level of information security maturity and their own functional needs. For example, one member may have already issued work devices for all individuals within the organization, and so may require all staff to access the member's environment and OPTN Computer System solely through the provided devices. Another member may choose to compartmentalize personal devices, with additional security provided in the compartmentalized portion of the device through which the user can access the necessary systems. Both options provide the additional required security, and this proposal does not seek to require one method of operationalizing these requirements over another.

Members are responsible for ensuring that all individuals to whom they grant access for the purpose of assisting with OPTN functions on behalf of the member adhere to these security requirements.

Information Security Personnel

This proposal requires members to identify an Information Security Contact. This role is intended to be the individual responsible for compliance with the requirements set forth within this proposal, as well as the point of contact for the OPTN for self-attestation, audits, security requests for information, and security incident reporting. The member must also have internal policies to ensure that the Information Security Contact is notified of declared security incidents. This proposal does not require a second individual to back up the point of contact, but in the event the point of contact is not available an equivalent process would be necessary to ensure the capabilities are in place.

To ensure a system of checks and balances for individual user access assignment and validation, members must also designate two site security administrators, and for transplant hospital members, this means two per designated transplant program. Members are already required to have at least one site security administrator, including one per designated transplant program at transplant hospitals. Currently 66% of labs, 96% of OPOs and 96% of transplant programs already have at least two site security administrators.[11] These roles are required to be approved by the OPTN Representative. This is in line with NIST SP 800-171 control 3.1.4, separation of duties.[12] Site security administrators are already required to review individual user accounts and permission levels when a user is no longer associated with the member as well as when a user's roles or responsibilities have changed such that a different level of permission is necessitated. Review will also be required at the request of the OPTN Contractor.

Required Training

This proposal includes required annual information security training for all individuals who access the OPTN Computer System within the OPTN member organization. Mindful of the community's concerns regarding possible duplication of training, the Committee determined that the training will be specific to OPTN security requirements. This training will be provided in the OPTN Contractor's Learning Management System and will cover individual and member responsibilities related to securing the OPTN Computer System and OPTN data.

[11] Based on OPTN data as of December 18, 2022.

[12] NIST SP 800-171 "Control 3.1.4: Separate the duties of individuals to reduce the risk of malevolent activity without collusion." Page 11. Accessed May 15, 2023.

This proposed requirement is in alignment with NIST SP 800-171 requirements for security awareness training.[13] Required training will include content related to the need for information security, individual user actions to maintain security, and individual user actions to respond to suspected security incidents. Individuals will need to pass an exam in order to gain or maintain access to the OPTN Computer System.

Member Readiness Assessment/Attestation

This proposal includes a requirement for all OPTN members to submit an annual self-attestation stating their compliance with the NIST SP 800-171 security framework or equivalent. Attestations must be provided prior to a new member gaining access to the OPTN Computer System, and annually thereafter or upon request by the OPTN Contractor. Calls for attestation will be distributed by the OPTN Contractor to the Information Security Contact with instructions for completion and return of the attestation.

The initial self-attestation will be a readiness assessment, determining the current state of member systems and identifying any gaps. Members may not be immediately able to attest to full compliance with all security controls upon implementation of this proposal. Members would be expected to specify which controls they do and do not adhere to in the initial attestation and work with the OPTN Contractor's information security team to manage and remediate the risk of non-compliance.

Routine Audits

Members will be subject to security audits every three years. The OPTN Contractor may contract with a third-party information security company to perform the audits. The auditing criteria will be compliance with the controls from NIST SP 800-171 and the OPTN-specified control values. These audits will begin after sufficient time for members to implement a security framework and take action on their Plans of Action and Milestones (POAMs).

Security Requests for Information

In order to ensure that known exploited vulnerabilities with the potential to affect the OPTN Computer System have been addressed by members, the OPTN Contractor may perform security requests for information. These requests for information inform the OPTN Contractor of the state and remediation status of the vulnerability within the member's environment. These requests will be distributed by the OPTN Contractor after CISA notification of a high or critical known exploited vulnerability, to ensure that the risk has been addressed. The timing for required response to these requests for information will be based on the level of threat of the vulnerability, as defined by the Department of Homeland Security.

The OPTN Contractor may also contract with third party information security company to perform the requests for information.

[13] NIST SP 800-171 "Control 3.2.1: Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems." Page 16. Accessed December 12, 2022.

Incident Response Plan

This proposal defines a security incident as "[a]n event that is declared as jeopardizing the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits."[14] It is only intended to encompass declared security incidents, not every potential incident under investigation by a member. It is also only intended to encompass security incidents involving the member's computing environment and limited to those machines and devices that are used to access the OPTN Computer System. That would be computing environments used to connect to the OPTN Computer System; associated environments used to manage or interface with said computing environment; and systems used to transmit or receive information and data from the OPTN Computer System. It is not intended to encompass machines or devices that are not used to access the OPTN Computer System.

All members must develop and comply with an incident response plan, to be available to the OPTN upon request. This plan must include the following:

- Notification of declared security incidents to the Information Security Contact from the member's information security staff.
- Notification to the OPTN Contractor of declared security incidents occurring on any device that connects to the OPTN Computer System or by which the member provides information to the OPTN as soon as possible, but within 24 hours of the Information Security Contact becoming aware of the declared incident if the affected users or impacted systems are not disconnected from the OPTN Computer System
- Provision of updates of the remediation status on the agreed upon schedule until the OPTN Contractor deems no longer necessary
- Process for acquiring third party validation of proper containment, eradication, and successful recovery, upon request by the OPTN Contractor
- Provision of final incident report

In the event of a security incident, members may be required to take specific actions to appropriately ensure risk to the OPTN Computer System is managed and balanced with the need to ensure transplants continue. This may include on-site remediation with oversight by the OPTN Contractor and/or requiring the member to disconnect from the OPTN Computer System until the OPTN Contractor has determined the risk is mitigated. Members will be required to meet control and verification requirements as provided by the OPTN Contractor based on the type of security incident. These requirements will be communicated directly to the member through the information security points of contact established in the member's incident response plan.

The OPTN Contractor has response procedures in place and will need to investigate the scope of the compromise to determine potential impacts to other members and determine if there is any indication of compromise to OPTN systems. The response to the incident will be based on the type of security incident and level of compromise. Mitigation and containment will prioritize ensuring minimal impact to transplantation, through new secure systems access if endpoints are compromised at the member institution.

[14] Definition developed from NIST *Special Publication 800-12 Revision 1: An Introduction to Information Security.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf. Accessed December 20, 2022.

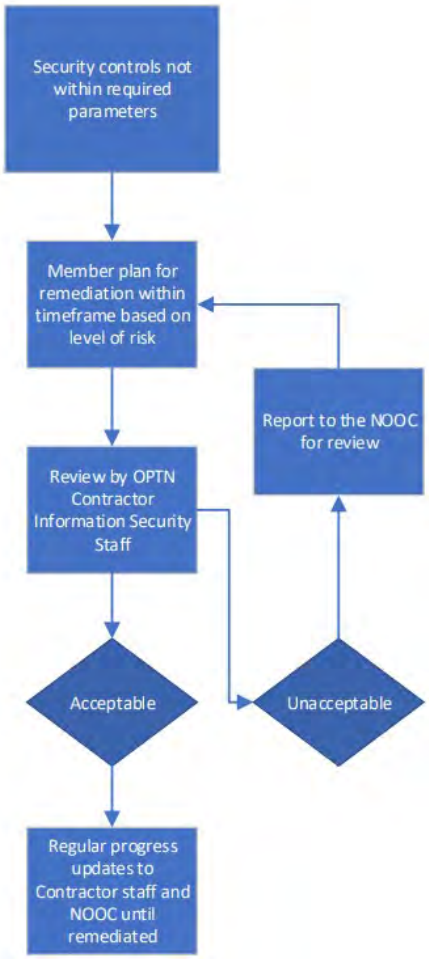
The Committee understands that security incidents can happen even if the member follows all security controls, and that it is not possible to completely remove risk. Information provided in incident response is used to help members maintain critical transplantation-related functions and to ensure security of the OPTN Computer System.

The OPTN Contractor has existing security incident notification requirements, which will not be impacted by this proposal. The OPTN Contractor is required to notify HRSA within one hour of a declared security incident, and to follow HRSA's instruction regarding any additional notifications.[15]

Risk Remediation and Compliance Monitoring

When either member attestation or auditing reveals security controls that are not within the required parameters, the Committee is proposing that the OPTN Contractor's Information Security staff and the Committee to work with the member to manage the risk and develop a remediation plan, see **Figure 1** for a draft process this review would take.

Figure 1: Process for Remediation of Security Controls



[15] OPTN Contract, HHSH250201900001C, Performance Work Statement (PWS) Task *3.20.4: Incident Response*.

The drafted process involves the OPTN Contractor's Information Security team assessing risk alongside the member, which would be documented in a Risk Management Tool. Members would have the option to respond to risk through a Plan of Actions and Milestones (POAM) or Risk Based Decision (RBD). Members would be expected to provide progress updates at regular intervals based on the level of risk. This process is intended to help both the member and the OPTN Contractor's information security team understand security implications and level of risk. The focus of these reviews is meant to focus on risk remediation, and not specifically on compliance with OPTN policy.

Members who refuse remediation may be referred to the MPSC for review under OPTN *Bylaws Appendix L: Reviews and Actions*.

Loss of Access to OPTN Computer System

This proposal does include the potential for members to lose access to the OPTN Computer System if a member's continued access to the OPTN Computer System poses a risk to the security of the OPTN Computer System that outweighs the risk of pausing a member's access to the OPTN Computer System. This may occur due to a security incident at a member institution, a member not adopting security measures, or a member not complying with requests for remediation for critical vulnerabilities. Temporary loss of access to the OPTN Computer System may happen stepwise, based on the level of risk the member's security presents. This could include the removal of access to Application Programming Interfaces (APIs), data entry capabilities, and ultimately the entire computer system. This loss of access would only occur if it is deemed necessary for risk management for the security of the OPTN Computer System.

In the case of loss of access, members should have a business continuity plan to maintain critical functions. This is already required by the Centers for Medicare and Medicaid Services' (CMS's) Emergency Preparedness Rule.[16] The OPTN Contractor's staff may work with the member to perform some OPTN functions typically performed by the member, such as entering data into the OPTN Computer System, and allocating organs on behalf of the member. The OPTN Contractor will have response procedures in place for security incidents related to OPTN members with access to the OPTN Computer System. The procedure, once finalized, will include the types of member incidents reportable to the OPTN, communication and response requirements, and roles and responsibilities of OPTN members when an incident is identified. The procedure will also include the key response phases: investigation, mitigation and containment, and recovery from the event which may include a third-party verification that there are no further indicators of system compromise.

The OPTN Contractor's staff will work with the member, following the response procedure, to re-establish access as quickly as possible, to ensure vital transplantation related functions are able to be maintained. Members may be required to establish a secure virtual local area network (VLAN) or connect only via new and isolated devices connected only to a mobile network and not the member's environment. The member may be required to provide proof that the member's environment is secured

[16] The Centers for Medicare and Medicaid Services. *Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers Final Rule.* (Federal Register) Effective November 16, 2016. Available at https://www.federalregister.gov/documents/2016/09/16/2016-21404/medicare-and-medicaid-programs-emergency-preparedness-requirements-for-medicare-and-medicaid. Accessed May 15, 2023.

before the member is permitted to re-connect to the OPTN Computer System. The member would be responsible for establishing a secure systems access.

Transition Period

The Committee recognizes that these new requirements will require a transition period for members. The Committee is proposing that members begin by reporting information security contacts and appointing a second site administrator, followed by reporting of security incidents and responding to information security requests for information. Members are encouraged to report security incidents prior to the implementation of this portion of the proposal, but it is not required. Members will then submit their readiness assessments, work with the Committee and OPTN Contractor on their POAMs and RBDs, and then the audit cycle will begin. The full details on proposed timing of the transition period can be found in the "Timing of Implementation" section.

Overall Sentiment from Public Comment

Sentiment is collected on public comment proposals and is measured on a 5-point Likert scale from strongly oppose to strongly support (1-5). These reports are helpful to spot high-level trends, but they are not meant as public opinion polls or to replace the substantive analysis below. Generally, public comment sentiment has been supportive of this proposal, as indicated by the total sentiment score of 3.5. **Figure 2** shows sentiment received from all respondents (regional meeting, online, and email) by their stated member type. Transplant hospitals were slightly less supportive of the proposal, with a sentiment score of 3.4, and patients were more supportive of the proposal, with a sentiment score of 4.1.

Figure 2: Sentiment by Member Type

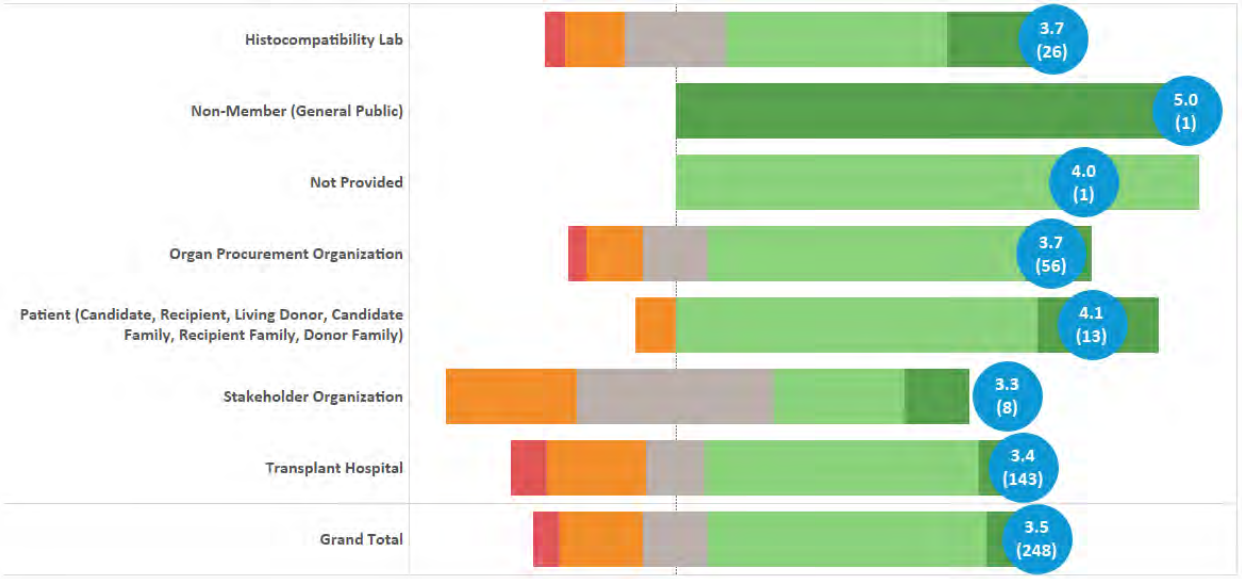
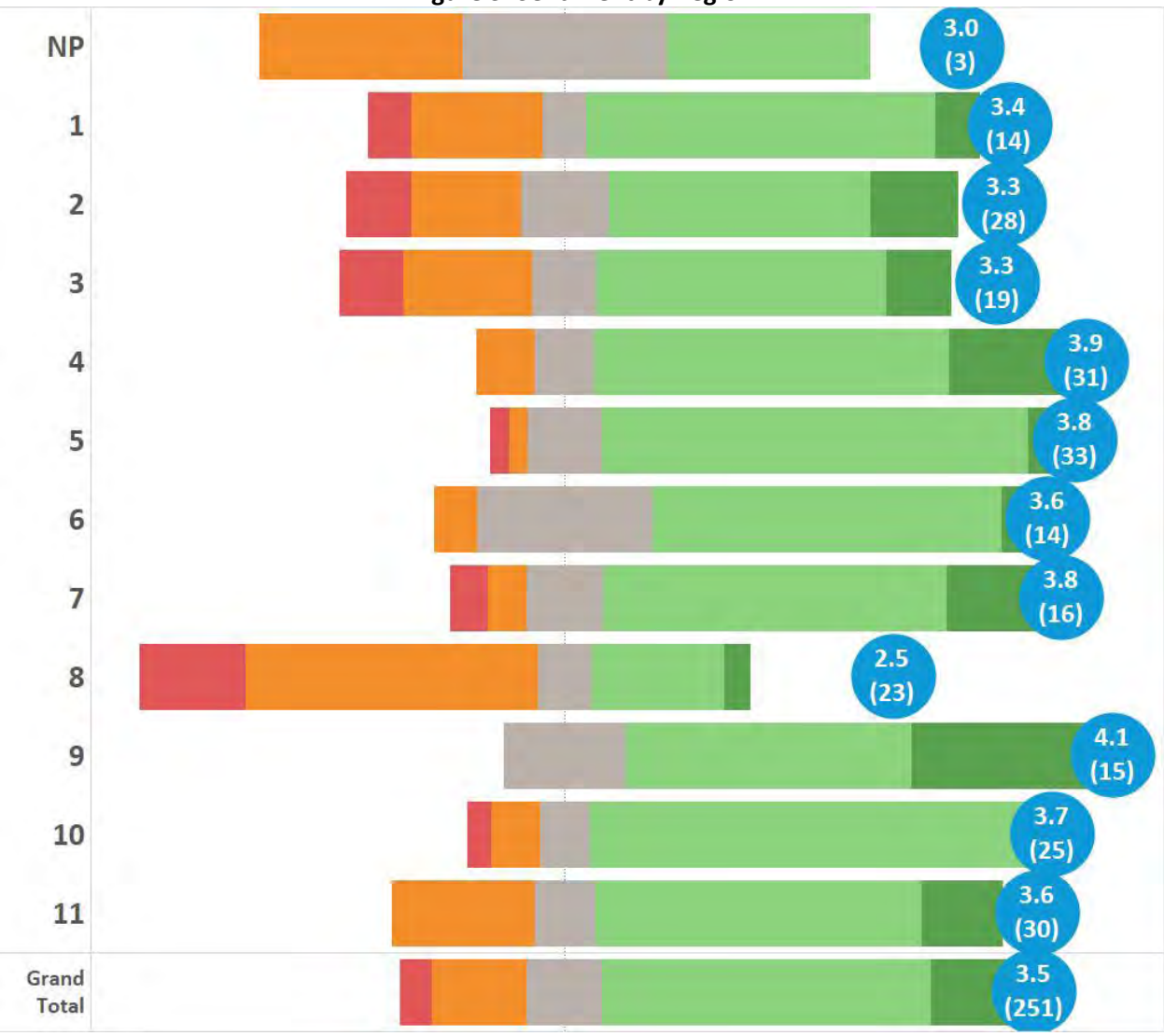


Figure 3 shows sentiment received by region, with "NP" representing sentiment for commenters whose location was not provided. Again, overall sentiment was supportive, as indicated by a total sentiment score of 3.5. Opposition was raised in all regions, mostly under the theme of end-user burden. Commenters in Region 8 expressed the most concern of any region, with a sentiment of 2.5.

Figure 3: Sentiment by Region



In addition to the sentiment score, items out for public comment also provide the opportunity for respondents to submit a substantive written comment. Responses are submitted by members of the public at large, as well as on behalf of regions and committees.[17] In addition to comments from regional meetings, eight OPTN committees, eight stakeholder organizations, and 24 individual commenters provided substantive comments. Major themes raised by commenters included the scope of the proposal, considerations for the security framework, access to the computer system, considerations for

[17] For comments submitted on behalf of the region or committees, the public comment item is discussed at the meeting, OPTN staff draft a summary of the discussion, and the Regional Councillor or Committee leadership review the comment, confirming it is an accurate representation of the discussion that occurred.

end-user burden and cost, timing of implementation, incident response, member data sensitivity, compliance monitoring, and additions to consider.

Scope of the Proposal

Multiple commenters expressed that the scope of the NIST 800-171 requirements applying to every aspect of the member computing environment, not just those that directly interface with the OPTN, would be a substantial burden. In order to address these concerns, the Committee reduced the scope of the security framework and incident reporting requirements from every aspect of a members' computing environment and interfacing environments to only portions of a member's environment used to access or manage access to the OPTN Computer System. This would reduce scope from all machines on a member's environment that access the internet, including devices such as medication dispensing machines and cardiac monitors, to only those directly accessing or managing access to the OPTN Computer System.

This reduction in scope is low risk for the OPTN Computer System, as while these additional portions of a member's environment can still contain exploitable vulnerabilities that can spread to other portions of a member's system, the member is still required to provide a robust security framework for portions accessing the OPTN Computer System and notify the OPTN if those portions of the member's environment are impacted.

Security Framework Considerations

Multiple commenters recommended alternative security frameworks for the Committee to consider, such as HITRUST, 405(d), Healthcare Industry Cybersecurity Practices (HICP), and others. The Committee had chosen NIST as the security controls are more easily mapped to other frameworks than most other existing security frameworks. The Committee had felt that a more rigid system that is less mappable to other frameworks would restrict members' existing information security implementations, and that large hospital systems would be unlikely to change their existing information security implementations for transplantation alone.

Access to the Computer System

Multiple commenters expressed concerns about the potential for this proposal to increase barriers to accessing the system and emphasized the need for flexibility in transplantation due to the many geographic locations members would need access. Many commenters also emphasized the need to access the OPTN Computer System from personal devices. One commenter stated that if organizational security requirements were too onerous, individual users may be more likely to access the OPTN Computer System through unsecured personal devices to avoid the compliance burdens.

Although restricting the use of personal devices was a common concern that arose from the community, the Committee did not place any restrictions on the use of personal devices in the proposal. Members will be required to develop policies on the secure use of personal devices under NIST 800-171 control 3.1.18, but those policies are able to be implemented in a way that allows the use of mobile devices to ensure flexible user access to the OPTN Computer System.

Considerations for End-User Burden and Cost

Multiple commenters expressed concerns about OPTN information security being duplicative of existing institutional requirements, and one commented that the OPTN could instead require trainings meet certain standards to reduce redundant trainings. Mindful of the community's concerns regarding possible duplication of training, the Committee determined that the training will be specific to OPTN security requirements. This training will be provided in the OPTN Contractor's Learning Management System and will cover individual and member responsibilities related to securing the OPTN Computer System and OPTN data.

One commenter recommended that based on significant costs, organizations should be given the opportunity to address additional needs within standard budget cycles and identify priorities within compliance if budgets do not allow for it all to be completed at once. The Committee intends to work with members to increase information security maturity over time, and not to require members to implement all controls immediately. After the initial readiness assessment, the Committee will focus on addressing the highest risk controls with members with a combination of a Plan of Actions and Milestones (POAM) and Risk-Based Decisions (RBD). This is a cooperative process to increase security capabilities by focusing on how to feasibly implement the highest risk controls as well as risk mitigation procedures for lower risk controls.

One recipient parent/information security professional stated that while this could increase overhead, the system exists for the benefit of recipients and should protect them and the processes that support them.

Timing of Implementation

The Committee had initially proposed six months for the appointment of the information security contact and the completion of the initial readiness assessment. Multiple commenters expressed that the implementation timeframe was too aggressive for the proposal, some stating that this timeframe would disproportionately affect smaller organizations. Multiple commenters had expressed concerns that they would not be able to have the controls fully implemented in this timeframe, but the proposed timeframe was for a readiness assessment, not a full information security framework implementation. Due to concerns about the need for a point of contact for security incidents, the Committee decided that one months' timeframe for reporting an information security contact to the OPTN would be appropriate. This contact can always be updated by the member if the member chooses to hire new or additional staff to fulfill this requirement.

The Committee recognizes the feedback on attestations, and wants to ensure the completion of the initial readiness assessment helps members begin identifying their information security gaps. The OPTN Contractor will work with members to help them recognize and begin remediating security gaps. This is not intended as a punitive process, nor are all controls required to be fully implemented prior to completion of the readiness assessment. Initial readiness assessments will not be issued until members have identified an information security contact, and members will have a minimum of three months to complete the assessment. The Committee had felt that would be sufficient time, as members are not required to implement controls in that time period, and instead simply respond to the current state of their systems. The OPTN Contractor will educate members on the completion of the readiness assessment prior to its release. After members submit their readiness assessments, members will work with the Committee on POAMs to determine how to feasibly implement higher risk controls and

increase their information security maturity, as well as RBDs to determine how to mitigate risk for lower risk controls. Members will be required to adhere to a security framework, but the Committee has not set thresholds for minimum performance and will determine if that is necessary or appropriate after review of member readiness assessment data.

The Committee has discussed the cadence of audits as a portion of the timing of implementation as well. Due to the work members will be completing as a part of their initial readiness assessments, the Committee has decided to begin audits in Quarter 3 of 2024 at the earliest. The Committee will monitor the timing of readiness assessments and remediations prior to implementing this requirement. This would allow members additional time to work on their information security maturity before an outside assessment is performed. The Committee felt that audits may not be as beneficial until members have had time to begin work to increase their information security maturity. See **Figure 4** for the proposed implementation timeline of this proposal. The Committee will evaluate the readiness of the community at each step of implementation to determine if the timeline remains appropriate, and there is a potential that this timeline may be lengthened.

Figure 4: Proposed Implementation Timeline

Incident Response

Multiple commenters stated that the timeframe of 24 hours to notify the OPTN of an incident would be aggressive and inconsistent with reporting requirements of other agencies. The Committee also discussed that in the first 24 hours of an incident, the member may have broader concerns in large incidents, such as ensuring electronic doors can be accessed. The Committee evaluated other federal requirements as a part of their evaluation of this concern. The Committee reviewed the required reporting for federally insured banks, which is 36 hours,[18] the Cyber Incident Reporting for Critical Infrastructure Act of 2022, which is 72 hours,[19] and the Securities and Exchange Commission (SEC) draft

[18] Dept. of the Treasury, Federal Reserve System, Federal Deposit Insurance Corp., Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, Final Rule (November 18, 2021), available at https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211118a1.pdf.
[19] Public Law No. 117-103 (03/15/2022)

regulation for reporting to shareholders, which is four business days.[20] Based on public comment feedback and alignment with other regulatory requirements, the Committee determined that 72 hours was an appropriate maximum timeframe for reporting if a member disconnects affected users and impacted systems from the OPTN Computer System. If a member does not disconnect affected users and impacted systems from the OPTN Computer System, the timeframe for reporting will remain at 24 hours. The Committee still encourages members to report incidents as soon as possible.

One commenter expressed concerns with the definition of a security incident including the phrase "potentially", and that it would require disproportionate effort to the potential risks. The Committee agreed that the language was overly broad and revised the definition of a security incident based on this feedback to "an event that is declared as jeopardizing the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits."

Multiple commenters stated that each member should address breach or loss of access to the OPTN Computer System as part of its emergency preparedness plan, identifying alternative means based on the type of access necessary for its operations. Another commenter expressed concern about how members will provide transplant services if access to the Computer System is temporarily removed. The Committee will provide educational materials to the community about business continuity planning to maintain transplant operations in the event of a security incident.

Member Data Sensitivity

One commenter stated that if the OPTN were to collect detailed information on member controls, it would be a central repository of information that could be used to compromise members.

Some of the member information will be confidential matters related to potential security vulnerabilities of individual systems. Only aggregated and de-identified information will be provided in open session meetings, which will first be evaluated to ensure it does not expose system-wide vulnerabilities in members. Review of member attestations, risk remediations, or other security-related information will be conducted in closed session meetings per OPTN *Bylaws 1.1.C: Meetings* in order to protect member security, as these details are confidential and impact the security posture of members.

Compliance Monitoring

One commenter stated that the Committee needs to develop a process for holding members accountable if they fail their information security audit, and that the correct body to discuss member accountability would need IT expertise. The Membership and Professional Standards Committee (MPSC) commented that they would like more information on how they would be involved in member non-compliance with these requirements, as well as what the consequences of members not being able to meet these requirements would be.

At this time, the Committee does not have established thresholds for member performance in information security maturity. The Committee feels that they cannot make a data-driven decision about minimum thresholds for information security maturity at this time, without reviewing the current state of information security in member systems. Audits would not be pass or fail but would recommend areas for improvement based on the level of the members' information security maturity. In addition,

[20] Securities and Exchange Commission, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Proposed Rule (March 9, 2022), available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

members will not be required to have all controls implemented at the time of the initial policy implementation. Members will be required to adhere to a NIST or equivalent security framework, which includes a process for mitigating risk and maturing over time.

Following public comment the Committee also removed the requirement for members to adhere to specific OPTN minimum control values, as they felt it may be premature prior to evaluating member systems. The Committee proposes to first collect members' readiness assessments and then prioritize which values, if any, should be implemented based on data related to level of risk of controls and current member statuses.

Additions to Consider

Multiple commenters recommended that the Committee publish technical guidance focusing on these groups of controls and make it available to member organizations. The Committee will prioritize providing educational materials to members using both existing industry resources and developing transplant-specific resources.

Compliance Analysis

NOTA and OPTN Final Rule

This proposal is provided under the authority of the National Organ Transplant Act of 1984 (NOTA) and the OPTN Final Rule. NOTA requires the Organ Procurement and Transplantation Network (OPTN) to establish "a national system, through the use of computers and in accordance with established medical criteria, to match organs and individuals included in the list…,"[21] and the OPTN Final Rule, which requires the OPTN to develop "Policies on such other matters as the Secretary directs."[22] Though modifications to the OPTN Contract, the Secretary has directed the OPTN Contractor, in coordination with the OPTN NOOC, to develop policies to enhance the security of the OPTN Computer System.

Implementation Considerations

This proposal will impact all members with access to the OPTN Computer Systems and may require additional personnel to handle information security.

Histocompatibility Laboratories

All members will need to develop a security framework that meets or exceeds controls in NIST SP 800-171, if they do not have such a framework already. This may take significant time and new personnel, depending on the members' current information security status. All members will need all staff to complete and pass required training, as well as complete the initial readiness assessment. Depending on the state of the member's information security by the initial attestation, members may need to respond to noncompliance and the level of risk through a Plan of Actions and Milestones (POAM) or Risk Based Decision (RBD) with the OPTN Contractor's information security staff. This would require regular

[21] 42 USC §274(b)(2)(A)(ii)
[22] 42 CFR §121.4(a)(6).

updates to the OPTN, and remediation the agreed upon timeframe.

All members will be required to complete attestations annually, and audits at a minimum of every three years. Required requests for information will be dependent on the cybersecurity landscape, as it is not possible to predict the number of high and critical known exploited vulnerabilities that will be discovered.

Management of a security incident will now need to involve OPTN notification and updates. Members may require third party incident response teams to assist with incident containment and recovery, as well as to verify to the OPTN that the recovery was performed in such a way that access can be securely re-established to the OPTN Computer System.

Hospital-based histocompatibility labs may be able to utilize information security resources existing within the hospital. OPTN membership includes 92 hospital-based lab members, and 49 independent or OPO-based lab members.[23]

Organ Procurement Organizations

All members will need to develop a security framework that meets or exceeds controls in NIST SP 800-171, if they do not have such a framework already. This may take significant time and new personnel, depending on the members' current information security status. All members will need all staff to complete and pass required training, as well as complete the initial readiness assessment. Depending on the state of the member's information security by the initial attestation, members may need to respond to noncompliance and the level of risk through a Plan of Actions and Milestones (POAM) or Risk Based Decision (RBD) with the OPTN Contractor's information security staff. This would require regular updates to the OPTN, and remediation within the agreed upon timeframe.

All members will be required to complete attestations annually, and audits at a minimum of every three years. Required requests for information will be dependent on the cybersecurity landscape, as it is not possible to predict the number of high and critical known exploited vulnerabilities that will be discovered.

Management of a security incident will now need to involve OPTN notification and updates. Members may require third party incident response teams to assist with incident containment and recovery, as well as to verify to the OPTN that the recovery was performed in such a way that access can be securely re-established to the OPTN Computer System.

Hospital-based OPOs may be able to utilize information security resources existing within the hospital. OPTN membership includes seven hospital based OPOs and 49 independent OPOs.[24]

Transplant Programs

All members will need to develop a security framework that meets or exceeds controls in NIST SP 800-171 if they do not have such a framework already. This may take significant time and new personnel, depending on the members' current information security status. All members will need all staff to

[23] Based on active OPTN members as of December 11, 2022.
[24] Based on active OPTN members as of May 15, 2023.

complete and pass required training, as well as complete the initial readiness assessment. Depending on the state of the member's information security by the initial attestation, members may need to respond to noncompliance and the level of risk through a Plan of Actions and Milestones (POAM) or Risk Based Decision (RBD) with the OPTN Contractor's information security staff. This would require regular updates to the OPTN, and remediation within the agreed upon timeframe.

All members will be required to complete attestations annually, and audits at a minimum of every three years. Required requests for information will be dependent on the cybersecurity landscape, as it is not possible to predict the number of high and critical known exploited vulnerabilities that will be discovered.

Management of a security incident will now need to involve OPTN notification and updates. Members may require third party incident response teams to assist with incident containment and recovery, as well as to verify to the OPTN that the recovery was performed in such a way that access can be securely re-established to the OPTN Computer System.

Transplant programs may be within larger hospital or healthcare systems with existing information security resources. Members will still need to provide documentation of the framework and controls, and develop an Information Security Contact, but may have fewer security needs to address.

OPTN

Operational Considerations

This proposal will require additional information security personnel to review attestations, work with members on Plans of Actions and Milestones (POAM) and Risk Based Decisions (RBD), complete security requests for information, and audit members every three years. The OPTN Contractor may utilize third parties for requests for information, attestation review, and routine audits. The OPTN Contractor will work closely with the NOOC to ensure an effective and efficient implementation of this policy.

Resource Estimates

The OPTN Contractor estimates 3,270 hours for implementation. Implementation will involve creating an automated submission capability for the information security contact, automating the annual attestation, and developing educational resources to the community about the changes. The OPTN Contractor estimates 22,135 hours for ongoing support. Ongoing support includes reviewing and processing completed attestations, working with members to develop POAMs and RBDs, and routine audits. Some of the work related to attestation review and audits may be completed by a third-party contractor. The work related to attestations and audits is included in the OPTN Fiscal Year 2024 budget with an estimate of $2.7 million, with a hybrid approach of third party contracting and increased internal staffing. Current staffing has been able to respond to member incidents at single institutions to date. There is a possibility for an increase in the resource requirements related to managing member security incidents. Member security incidents can vary in size and scope, and therefore resources may be needed to respond accordingly, particularly if multiple members have simultaneous security incidents.

Post-implementation Monitoring

Member Compliance

Members will be expected to comply with requirements in the proposed policy language. In addition to the compliance monitoring outlined above, all elements required by policy may be subject to OPTN review, and members are required to provide documentation as requested.

This proposal includes member monitoring and compliance through the NOOC and OPTN Contractor's information security staff. Member self-attestations will be reviewed for security controls implementation, and members will receive information security audits every three years.

Conclusion

This proposal is intended to enhance overarching information security of the OPTN Computer System and security of OPTN member organizations who use the OPTN Computer System through multiple proposed requirements. The requirements address the following:

- Security framework and controls for all members with access to OPTN Computer Systems
- Self-attestation from members on the security framework in place
- Auditing and compliance monitoring for security requirements
- Security requests for information
- Development of an incident response plan, required actions for a security incident
- Establishment of an information security contact role
- Security training for all member organization individuals with access to the OPTN Computer System
- Transition period for initial compliance

The Committee has modified the scope of the required security framework, the requirements for security training, and the timing of implementation, and the minimum control value requirements in response to public comment.

Policy Language

Proposed new language is underlined (example) and language that is proposed for removal is struck through (~~example~~). Heading numbers, table and figure captions, and cross-references affected by the numbering of these policies will be updated as necessary.

1.2 Definitions

The definitions that follow are used to define terms specific to the OPTN Policies.

OPTN Computer System

The software platform operated by the OPTN Contractor in performance of the OPTN Contract. This platform includes, but is not limited to, the OPTN Data System, the OPTN Waiting List, the OPTN Donor Data and Matching System, the OPTN Organ Labeling, Packaging, and Tracking system, the OPTN Patient Safety Reporting Portal, and OPTN Kidney Paired Donation Pilot Program (KPDPP).

Security incident

An event that is declared as jeopardizing the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits.

3.1 Access to the OPTN Computer System~~s~~

~~Only the following categories of members may access the match system:~~

1. ~~Transplant hospitals~~
2. ~~Organ procurement organizations (OPO)~~
3. ~~Histocompatibility laboratories~~

~~The waiting list may only be accessed by members, and members may not use the match system for non-members or add candidates to the waiting list on behalf of non-member transplant hospitals.~~

Transplant hospital, organ procurement organization, and histocompatibility laboratory members are provided access to the OPTN Computer System as members of the OPTN. Transplant hospital, organ procurement organization, and histocompatibility laboratory members with access to the OPTN Computer System may authorize user access to the OPTN Computer System.

Representatives of HRSA, HHS, and other components of the federal government are provided access to the OPTN Computer System as requested by the HRSA COR.

Members must ensure that all users meet OPTN training requirements prior to establishing a user's access to the OPTN computer system and yearly thereafter. Members must also ensure that all users comply with the OPTN Contractor's system terms of use for the OPTN Computer System.

3.1.A Security Requirements for Systems Accessing the OPTN Computer System

Transplant hospital, organ procurement organization, and histocompatibility laboratory members must provide security for the computing environments and components thereof

which are used access the OPTN Computer System and the associated environments used to manage the member's computing environment used to access the OPTN Computer System.

Transplant hospital, organ procurement organization, and histocompatibility laboratory members must ensure that these environments adhere to a security framework that is either:

- the most recent revision of a National Institute of Standards in Technology (NIST) information security framework or
- a security framework with equivalent controls provided by the member and approved by the OPTN.

Transplant hospital, organ procurement organization, and histocompatibility laboratory members who authorize access to users must ensure that the user agrees to access the OPTN Computer System through computing environments that adhere to either the most recent revision of a NIST information security framework or a security framework with equivalent controls.

Transplant hospital, organ procurement organization, and histocompatibility laboratory members must attest to their adherence to their security framework through an OPTN attestation. OPTN attestations must be submitted annually and upon request by the OPTN to maintain access to the OPTN Computer System.

Adherence to the security framework will be audited at least once every three years. Transplant hospital, organ procurement organization, and histocompatibility laboratory members must also respond to OPTN requests for information within the timeframe stated by the OPTN.

3.1.B Site Security Administrators

Organ procurement organization and histocompatibility laboratory members with access to the OPTN Computer System must designate at least two site security administrators to maintain access to the OPTN Computer System. Transplant hospital members with access to the OPTN Computer System must designate at least two site security administrators for each of its designated transplant programs.

Site security administrators are responsible for maintaining an accurate and current list of users and permissions, specific to the role of the user in its performance of duties related to OPTN Obligations. Permission levels must be granted according to the NIST principle of least privilege.

Site security administrators must review user accounts and permission levels:

- When a user is no longer associated with the member organization
- When the user's roles or responsibilities have changed, such that a different level of permission is necessitated
- As directed by the OPTN

3.1.C Security Incident Management and Reporting

Transplant hospital, organ procurement organization, and histocompatibility laboratory members with access to the OPTN Computer System must develop and comply with an incident

response plan designed to identify, prioritize, contain and eradicate security incidents. The incident response plan must include *all* of the following:

- Appointment of an information security contact, as detailed in OPTN *Policy 3.1.C.i: Information Security Contact*
- Notification to the OPTN Contractor of security incidents occurring in any environment outlined in *Policy 3.1.A: Security Requirements for Systems Accessing the OPTN Computer System*, as soon as possible, but no later than:
    - 24 hours following the information security contact becoming aware of the security incident if a member does not disconnect the affected users and any impacted systems from the OPTN Computer System
    - 72 hours following the information security contact becoming aware of the security incident if the member does disconnect the affected users and any impacted systems from the OPTN Computer System
- Process for acquiring third party validation of proper containment, eradication, and successful recovery

Portions of the incident response plan involving access to the OPTN Computer System must be made available to the OPTN on request and will be considered confidential.

In the event of a security incident, members will be required to provide status updates to the OPTN on the security incident on an agreed upon schedule and to meet control and verification requirements as provided by the OPTN based on the type of security incident. These requirements will be communicated directly to the member through the information security contact established in the member's incident response plan. Members may also be required to provide a final incident report.

Members may be required to take specific actions to appropriately ensure risk to the OPTN Computer System is managed and balanced with the need to ensure transplants continue. Specific actions may include on-site remediation, requiring the member's access to the OPTN Computer System be temporarily removed until the OPTN has determined the risk is mitigated, or other containment and recovery actions with oversight by the OPTN.

Any action that temporarily removes the member's access to the OPTN Computer System must be directed by the OPTN or the Secretary of HHS. The OPTN Contractor may take other actions necessary to secure the OPTN Computer System on behalf of the OPTN. Any actions taken by the OPTN Contractor to secure the OPTN Computer System on behalf of the OPTN must be reported to the OPTN within 48 hours.

3.1.C.i Information Security Contact

Transplant hospital, organ procurement organization, and histocompatibility laboratory members with access to the OPTN Computer System must identify an information security contact, who is responsible for maintaining and complying with a written protocol that includes how an information security contact will:

1. Provide 24/7 capability for incident response and communications

a. Receive relevant notifications of security incidents from the member's information security staff
b. Communicate information regarding security incidents to the OPTN
c. Facilitate development and fulfillment of OPTN Obligations outlined in OPTN *Policy 3.1.A: Security Requirements for Systems Accessing the OPTN Computer System*

#

Appendix A: NIST SP 800-171 Controls

Below are the NIST SP 800-171 Revision 2 controls. A full description of each control is provided in the special publication.[25] The Committee is proposing that every member must have policies or procedures to address each control within this publication.

Access Control	
Control Number	**Description**
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.
3.1.3	Control the flow of Controlled Unclassified Information (CUI) in accordance with approved authorizations.
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
3.1.8	Limit unsuccessful logon attempts.
3.1.9	Provide privacy and security notices consistent with applicable Controlled Unclassified Information (CUI) rules.
3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
3.1.11	Terminate (automatically) a user session after a defined condition.
3.1.12	Monitor and control remote access sessions.
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
3.1.14	Route remote access via managed access control points.
3.1.15	Authorize remote execution of privileged non commands and remote access to security-relevant information.
3.1.16	Authorize wireless access prior to allowing such connections.
3.1.17	Protect wireless access using authentication and encryption.
3.1.18	Control connection of mobile devices.

[25] National Institute of Standards and Technology (NIST). "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations". Special Publication. February 2020, https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final (Accessed December 11, 2022).

Access Control	
Control Number	**Description**
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.
3.1.20	Verify and control/limit connections to and use of external systems.
3.1.21	Limit use of portable storage devices on external systems.
3.1.22	Control CUI posted or processed on publicly accessible systems.

142
143

Awareness and Training	
Control Number	**Description**
3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.
3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.

144

Audit and Accountability	
Control Number	**Description**
3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.
3.3.3	Review and update logged events.
3.3.4	Alert in the event of an audit logging process failure.
3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.
3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.
3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
3.3.9	Limit management of audit logging functionality to a subset of privileged users.

Configuration Management	
Control Number	**Description**
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.
3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.
3.4.4	Analyze the security impact of changes prior to implementation.
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.
3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
3.4.9	Control and monitor user-installed software.

Identification and Authentication	
Control Number	**Description**
3.5.1	Identify system users, processes acting on behalf of users, and devices.
3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
3.5.5	Prevent reuse of identifiers for a defined period.
3.5.6	Disable identifiers after a defined period of inactivity.
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.
3.5.8	Prohibit password reuse for a specified number of generations.
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.
3.5.10	Store and transmit only cryptographically protected passwords.
3.5.11	Obscure feedback of authentication information.

Incident Response	
Control Number	**Description**
3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.
3.6.3	Test the organizational incident response capability.

148

Maintenance	
Control Number	**Description**
3.7.1	Perform maintenance on organizational systems.
3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.
3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.

149

Media Protection	
Control Number	**Description**
3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
3.8.2	Limit access to CUI on system media to authorized users.
3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse.
3.8.4	Mark media with necessary CUI markings and distribution limitations.
3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
3.8.7	Control the use of removable media on system components.
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.
3.8.9	Protect the confidentiality of backup CUI at storage locations.

150

Personnel Security	
Control Number	**Description**
3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.
3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

151

Physical Protection	
Control Number	**Description**
3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.
3.10.3	Escort visitors and monitor visitor activity.
3.10.4	Maintain audit logs of physical access.
3.10.5	Control and manage physical access devices.
3.10.6	Enforce safeguarding measures for CUI at alternate work sites.

152

Risk Assessment	
Control Number	**Description**
3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.
3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
3.11.3	Remediate vulnerabilities in accordance with risk assessments.

153

Security Assessment	
Control Number	**Description**
3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

System and Communications Protection	
Control Number	**Description**
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
3.13.3	Separate user functionality from system management functionality.
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.
3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.
3.13.13	Control and monitor the use of mobile code.
3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.
3.13.15	Protect the authenticity of communications sessions.
3.13.16	Protect the confidentiality of CUI at rest.

System and Information Security	
Control Number	**Description**
3.14.1	Identify, report, and correct system flaws in a timely manner.
3.14.2	Provide protection from malicious code at designated locations within organizational systems.
3.14.3	Monitor system security alerts and advisories and take action in response.
3.14.4	Update malicious code protection mechanisms when new releases are available.

System and Information Security	
Control Number	**Description**
3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
3.14.7	Identify unauthorized use of organizational systems.

156

Appendix B: Glossary of Terms

The following terms are used throughout the proposal.

Audit log: A record of system access and security events (see "Security events") that can be both physical and electronic.

Audit record reduction: A process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts.

Audit report generation: Reports generated through audit record reduction.

Authoritative source: A synchronized time reference to allow uniformity of time stamps for systems with multiple system clocks and systems connected over a network.

Baseline configuration: Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems and serve as a basis for future builds, releases, and changes to systems. These include information about system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and update and patch information on operating systems and applications; and configuration settings and parameters), network topology, and the logical placement of those components within the system architecture.

Controls: See "Security Controls".

Controlled Unclassified Information (CUI): Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

Controlled Unclassified Information (CUI) at rest: Information at rest refers to the state of information when it is not in process or in transit and is located on storage devices as specific components of systems.

Cryptographic keys: A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm.

Cryptographic mechanisms: An element of a cryptographic application, process, module or device that provides a cryptographic service, such as confidentiality, integrity, source authentication, and access control.

Deny-all, permit by exception policy (whitelisting): The process used to identify software programs that are authorized to execute on systems.

Deny-by-exception policy (blacklisting): The process used to identify software programs that are not authorized to execute on systems.

FIPS-validated cryptography: A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS Publication 140-3 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP). See NSA-approved cryptography.

Known Exploited Vulnerability: A vulnerability that is known to be exploited. A catalog of Known Exploited Vulnerabilities is maintained by the Cybersecurity and Infrastructure Security Agency (CISA).[26] **Insider threat:** A security threat originating from within the system. Potential indicators and possible precursors of insider threat include behaviors such as: inordinate, long-term job dissatisfaction; attempts to gain access to information that is not required for job performance;

[26] https://www.cisa.gov/known-exploited-vulnerabilities-catalog. Accessed December 16, 2022.

unexplained access to financial resources; bullying or sexual harassment of fellow employees; workplace violence; and other serious violations of the policies, procedures, directives, rules, or practices of organizations.

Logged events: The list of security events logged in the audit log.

Logging process failure: Includes software and hardware errors, failures in the audit record capturing mechanisms, and audit record storage capacity being reached or exceeded.

Managed access control points:

Mobile code: Technologies including Java, JavaScript, ActiveX, Postscript, PDF, Flash animations, and VBScript. Decisions regarding the use of mobile code in organizational systems are based on the potential for the code to cause damage to the systems if used maliciously.

Mobile computing platforms: Devices accessing the system in a mobile format, including tablets and smartphones.

Multifactor authentication: Requires the use of two or more different factors to authenticate. The factors are defined as something you know (e.g., password, personal identification number [PIN]); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). Multifactor authentication solutions that feature physical authenticators include hardware authenticators providing time-based or challenge-response authenticators and smart cards.

Network traffic: Computer network communications that are carried over wired or wireless networks between hosts.

Nonlocal maintenance sessions: Those activities conducted by individuals communicating through an external network.

Portable storage devices: Portable devices on which system information is stored, including USB memory sticks, digital video disks, compact discs, and external or removable hard disk drives.

Principle of least functionality: Configuring organizational systems by limiting component functionality to a single function per component.

Principle of Least Privilege: Providing users with authorized privileges no higher than necessary to accomplish required organizational missions or business functions.

Privileged accounts: An information system account with approved authorizations of a privileged user.

Privileged commands: A human-initiated (interactively or via a process operating on behalf of the human) command executed on a system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information.

Replay-resistant authentication mechanisms: Include protocols that use nonces or challenges such as time synchronous or challenge-response one-time authenticators.

Security Controls (Controls): Measures which modify risk. These can include any process, policy, device, practice, or other actions that modify risk.

Split tunneling: Simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks. Split tunneling might be desirable by remote users to communicate with local system resources such as printers or file servers. However, split tunneling allows unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information.

System boundaries: Boundary components include gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a system security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks).

System development life cycle: A formal or informal methodology for designing, creating, and maintaining software (including code built into hardware).

System environment: The unique technical and operating characteristics of an IT system and its associated environment, including the hardware, software, firmware, communications capability, organization, and physical location.

Voice over Internet Protocol: A term used to describe the transmission of packetized voice using the internet protocol (IP) and consists of both signaling and media protocols.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.