

Public Comment Proposal


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*

Contents

Executive Summary	2
Purpose	3
Background	3
Overview of Proposal	5
NOTA and Final Rule Analysis	11
Implementation Considerations	12
Post-implementation Monitoring	15
Conclusion	16
Considerations for the Community	16
Policy Language	17
Appendix A: NIST SP 800-171 Controls	20
Appendix B: Glossary of Terms	28



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

Affected Policies: 1.2: Definitions
3.1: Access to OPTN Computer System

Sponsoring Committee: Network Operations Oversight

Public Comment Period: January 19, 2023 – March 15, 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 at the request of 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.

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,⁵ 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*.⁶ NIST is an agency of the United

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 (HSH250201900001C). 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 <https://unos.org/wp-content/uploads/2018-UNOS-Systems-Terms-of-Use.pdf>.

⁶ National Institute of Standards and Technology (NIST). "Protecting Controlled Unclassified Information in Nonfederal Systems

States Department of Commerce that develops and distributes industry standards for technology and business. Among those standards is the NIST Cybersecurity Framework (CSF), which provides directions and guidance to improve organizational cybersecurity risk management.⁷ The NIST framework has five core pillars, or functions, which the Committee reviewed when developing this proposal:⁸

- Identify- Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- Protect- Develop and implement appropriate safeguards to ensure delivery of critical services.
- Detect- Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- Respond- Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- Recover- Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

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

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).⁹ 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.¹⁰ 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

and Organizations". Special Publication. February 2020, <https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final> (Accessed December 11, 2022).

⁷ <https://csrc.nist.gov/projects/risk-management>.

⁸ National Institute of Standards and Technology (NIST). "Framework for Improving Critical Infrastructure Cybersecurity". April 2018, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> (Accessed December 13, 2022).

⁹ 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.

¹⁰ <https://www.cisa.gov/known-exploited-vulnerabilities>. Accessed December 12, 2022.

cybersecurity landscape, the Committee has felt it necessary to begin to develop these requirements. OPTN members are critical stakeholders of the OPTN Computer System, and as such, it follows that the OPTN members should contribute to the minimization of risk to the security of the OPTN Computer System.

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.¹¹

Overview of Proposal

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
- 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, required actions for a security incident
- Establishment of an information security contact role
- Security training for all member organization staff

In addition, the Committee is proposing a transition period for the initial development of the security framework and control values.

Member Security Framework and Controls

All members will be expected to, at minimum, follow all of the NIST SP 800-171¹² 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 through 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 appendix also contains the initial proposed OPTN specified minimum control values. This list will be maintained by the OPTN and regularly reviewed by the Committee. The Committee intends this to be an iterative process with increasing maturity levels of information security capabilities over time. Members will be given notice prior to the change of any control values, with a transition period based on the increase in complexity of the control values.

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

¹¹ OPTN Contract, HHS250201900001C, Performance Work Statement (PWS) Task 3.2.5.5: *OPTN BOD Network Operations Oversight Committee*.

¹² <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf>.

- 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

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 third parties to whom they grant access for the purpose of assisting with OPTN functions on behalf of the member are compliant with 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, compliance reviews, 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 it an equivalent process would be necessary to ensure the capabilities are in place.

To ensure a system of checks and balances for 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.¹³ These roles are required to be approved by the Director or Transplant Administrator for the designated transplant program. Each individual granted access to the OPTN Computer System by one site security administrator will be required to be verified by a second site security administrator. This is in line with NIST SP 800-171

¹³ Based on OPTN data as of December 18, 2022.

control 3.1.4, separation of duties.¹⁴ Site security administrators are already required to review 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 information security training for all individuals who access the OPTN Computer System within the OPTN member organization. This training will be provided in the OPTN Contractor's Learning Management System, and will be required for new users to gain access, as well as required annually for all existing users.

This proposed requirement is in alignment with NIST SP 800-171 requirements for security awareness training.¹⁵ Required training will include content related to the need for information security, user actions to maintain security, and user actions to respond to suspected security incidents. At the end of the training, individuals will need to pass an exam in order to gain or maintain access to the OPTN Computer System.

Member 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 and OPTN specified minimum control values. Attestations must be provided prior to a new member joining, 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.

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 are and are not compliant with in the initial attestation and work with the OPTN Contractor's information security team to manage and remediate the risk of non-compliance. See the "Transition Period" section for more details around the implementation of this proposal.

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.

¹⁴ Id, page 23.

¹⁵ 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.

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.

Incident Response Plan

This proposal defines a security incident as “[a]n occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits.”¹⁶ 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
- 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, including on-site remediation with oversight by the OPTN Contractor and/or requiring the

¹⁶ 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.

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 will have 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.

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.

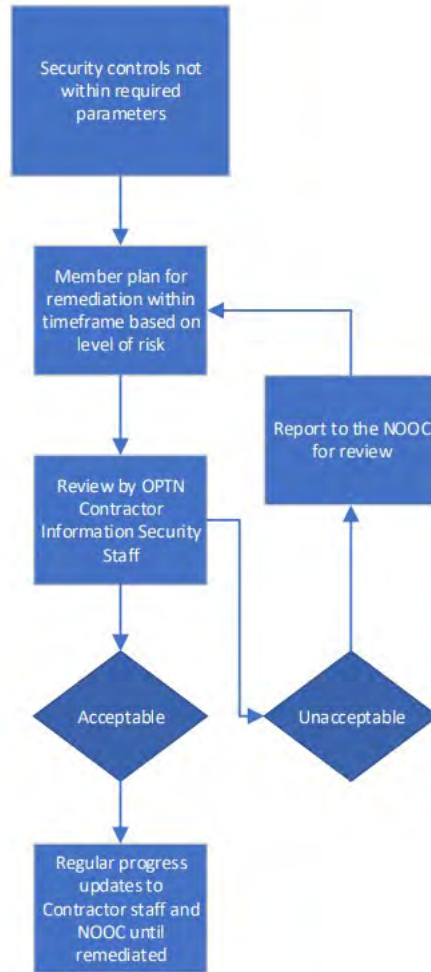
The OPTN Contractor has existing security incident notification requirements, which will not be impacted by this proposal. The OPTN Contractor is required to notify HRSA within one hour of a declared security incident, and to follow HRSA's instruction regarding any additional notifications.¹⁷

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.

¹⁷ OPTN Contract, HHS250201900001C, Performance Work Statement (PWS) Task 3.20.4: *Incident Response*.

Figure 1: Process for Remediation of Security Controls



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 (POA&M) 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

The OPTN Contractor, in collaboration with the member, will actively manage the risk of non-compliance with the security requirements developed within this proposal. However, this proposal does include the potential for members to lose access to the OPTN Computer System if a member does not adopt security measures or comply with requests for remediation such that the 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 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 is necessary for risk management for the security of the OPTN Computer System.

In the case of loss of access, the OPTN Contractor's staff may be required to work with the member to perform 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 before the member is permitted to re-connect to the OPTN Computer System. The member would be responsible for establishing a secure systems access, and the Committee is interested in feedback on other potential secure access options beyond the response procedures.

Transition Period

The Committee recognizes that compliance with these new requirements will require a transition period for many members. The Committee is proposing a six-month transition for members to perform an initial assessment and attestation of current status in relation to the required security controls. Plans associated with full remediation must be completed and provided to the OPTN within a mutually agreed upon timeframe. All security requirements will be required to be remediated by the end of the specified timeframe, with documentation provided to the OPTN for review by the OPTN Contractor Information Security staff and the Committee.

Members will be expected to have established an information security point of contact upon implementation of this proposal. Members will receive notice between approval and implementation, and the Committee is seeking feedback on a feasible timeframe to establish this role.

NOTA and Final Rule Analysis

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..."¹⁸ and the OPTN Final Rule, which

¹⁸ 42 USC §274(b)(2)(A)(ii)

requires the OPTN to develop “Policies on such other matters as the Secretary directs.”¹⁹ 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

Member and OPTN Operations

This proposal will impact all members with access to the OPTN Computer Systems and may require a significant transition period for some members.

Operations affecting Histocompatibility Laboratories

All members will need:

- A security framework that meets or exceeds the controls in NIST Special Publication 800-171
- To establish an Information Security Contact, which may require the hiring of new staff for information security
- All staff to complete required training
- To complete the initial attestation within six months of policy implementation
- To complete annual self-attestations as well as an audit at a minimum of every three years
- To complete security requests for information within the specified timeframes, which will be based on the level of threat to information security
- To notify and update the OPTN when managing a security incident

Hospital-based histocompatibility labs may be able to utilize information security frameworks and controls existing within the hospital. OPTN membership includes 92 hospital-based lab members, and 49 independent or OPO-based lab members.²⁰

Operations affecting Organ Procurement Organizations

All members will need:

- A security framework that meets or exceeds the controls in NIST Special Publication 800-171
- To establish an Information Security Contact, which may require the hiring of new staff for information security
- All staff to complete required training
- To complete the initial attestation within six months of policy implementation
- To complete annual self-attestations as well as an audit at a minimum of every three years
- To complete security requests for information within the specified timeframes, which will be based on the level of threat to information security
- To notify and update the OPTN when managing a security incident

Hospital-based OPOs may be able to utilize information security frameworks and controls existing within the hospital. OPTN membership includes seven hospital based OPOs and 50 independent OPOs.²¹

¹⁹ 42 CFR §121.4(a)(6).

²⁰ Based on active OPTN members as of December 11, 2022.

²¹ Based on active OPTN members as of December 11, 2022.

Operations affecting Transplant Hospitals

All members will need:

- A security framework that meets or exceeds the controls in NIST Special Publication 800-171
- To establish an Information Security Contact, which may require the hiring of new staff for information security
- All staff to complete required training
- To complete the initial attestation within six months of policy implementation
- To complete annual self-attestations as well as an audit at a minimum of every three years
- To complete security requests for information within the specified timeframes, which will be based on the level of threat to information security
- To notify and update the OPTN when managing a security incident

Transplant programs may be within larger hospital or healthcare systems with existing information security frameworks and controls. 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.

Operations affecting the OPTN

This proposal will significantly impact OPTN operations. The OPTN Contractor will need to:

- Perform audits independently or through a third-party contractor, initially and at a minimum of every 3 years, of all members with access to the OPTN Computer System
- Review member attestations and work with members to remediate any security controls that are not compliant with OPTN requirements. This process will involve participation in risk assessments and plans of action, as well as review of regular updates from the members.
- Perform and review requests for information from members when a high or critical vulnerability is detected
- Manage incident response in the event of a member security incident, and investigate potential compromise to other OPTN members and the OPTN Computer System

Projected Fiscal Impact

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

Projected Impact on 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 attestation within six months of policy implementation. 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 (POA&M) or Risk Based Decision (RBD) with the OPTN Contractor's information security staff. This would require regular 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.²²

Projected Impact on 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 attestation within six months of policy implementation. 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 (POA&M) 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 50 independent OPOs.²³

Projected Impact on Transplant Hospitals

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

²² Based on active OPTN members as of December 11, 2022.

²³ Based on active OPTN members as of December 11, 2022.

complete and pass required training, as well as complete the initial attestation within six months of policy implementation. 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 (POA&M) 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.

Projected Impact on the OPTN

This proposal will require additional information security personnel to review attestations, work with members on Plans of Actions and Milestones (POA&M) 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 and routine audits.

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 compliance with required controls, 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 staff

In addition, the Committee is proposing a transition period for initial compliance.

Considerations for the Community

The Committee requests feedback on the following questions:

- Are the initial proposed NIST SP 800-171 control values outlined in Appendix A feasible for members?
- Should a member environment accessing the OPTN Computer System include personal devices?
 - Should members be required to notify the OPTN Contractor every time that there is a security incident involving a personal device?
- What is a feasible timeframe for members to have an information security contact established?
- Do you support the development of an alternative pathway for managing noncompliance with security policies?
- What factors should institutions consider in developing a plan to maintain operations in the case of a breach and loss of access to the OPTN Computer System is necessary?

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 1.2 Definitions

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

3

4 **OPTN Computer System**

5 The software platform operated by the OPTN contractor in performance of the OPTN Contract. This
6 platform includes, but is not limited to, the OPTN Data System, the OPTN Waiting List, the OPTN Donor
7 Data and Matching System, the OPTN organ labeling, packaging, and tracking system, the OPTN Patient
8 Safety Reporting Portal, and OPTN KPDPP.

9

10 **Security incident**

11 An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an
12 information system or the information the system processes, stores, or transmits.

13

14 **3.1 Access to OPTN Computer System Security Requirements for Systems Connecting to the OPTN** 15 **Computer System**

16

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

18

- 19 1. ~~Transplant hospitals~~
- 20 2. ~~Organ procurement organizations (OPO)~~
- 21 3. ~~Histocompatibility laboratories~~

22

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

25

26 Transplant hospital, organ procurement organization, and histocompatibility laboratory members must
27 provide security for: the computing environments used to connect to the OPTN Computer System;
28 associated environments used to manage or interface with said computing environment; and systems
29 used to transmit or receive information and data from the OPTN Computer System.

30

31 Transplant hospital, organ procurement organization, and histocompatibility laboratory members must
32 demonstrate through attestation that these environments are in compliance with the most recent
33 revision of either a National Institute of Standards in Technology (NIST) information security framework
34 or a NIST equivalent security framework, including adoption of OPTN minimum security control values.
35 Attestations using the templates provided by the OPTN Contractor must be submitted annually and
36 upon request by the OPTN contractor to maintain access to the OPTN Computer System.

37

38 Compliance with the security framework will be monitored by the OPTN Contractor, including by, but
39 not limited to, an audit to occur at least once every three years. Transplant hospital, organ procurement
40 organization, and histocompatibility laboratory members must also respond to OPTN information
41 security requests for information within the stated timeframe communicated by the OPTN Contractor.



42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88

3.1.A ~~Non-member Access~~ Access to the OPTN Computer System

Transplant hospital, OPO, and histocompatibility laboratory members are provided access to the OPTN Computer System as members of the OPTN. Transplant hospital, OPO, and histocompatibility laboratory members with access to the OPTN Computer System may authorize user access to the OPTN Computer System through contract or other agreement with approval of the OPTN Contractor. Members who authorize such access must ensure that those to whom they grant access are compliant with OPTN Policy 3.1: Security Requirements for Systems Connecting 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.

3.1.B Site Security Administrators

Transplant hospital, OPO, 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 employees 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 least privileged principles of access.

Prior to establishing a user’s access, site security administrators must verify that the potential user has completed OPTN required training. Once a user has access, site security administrators must verify that approved users continue to complete yearly OPTN required training and comply with the OPTN Contractor’s system terms of use.

Site security administrators must review user accounts and permission levels:

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

3.1.C Security Incident Management and Reporting

Transplant hospital, OPO, 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. This plan must be made available to the OPTN Contractor on request, and 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 declared security incidents occurring in any environment outlined in Policy 3.1: Security Requirements for Systems Connecting to the OPTN Computer System, as soon as possible, but no later than 24 hours following the information security contact becoming aware of the incident

- 89 • Provision to the OPTN Contractor of status updates on the security incident on an agreed upon
- 90 schedule
- 91 • Process for acquiring third party validation of proper containment, eradication, and successful
- 92 recovery, upon request by the OPTN Contractor
- 93 • Provision of the final incident report to the OPTN Contractor

94

95 In the event of a security incident, members may be required to take specific action(s) to appropriately

96 ensure risk to the OPTN Computer System is managed and balanced with the need to ensure transplants

97 continue. Specific actions may include on-site remediation, requiring the member to be disconnected

98 from the OPTN Computer System until the OPTN Contractor has determined the risk is mitigated, or

99 other containment and recovery actions with oversight by the OPTN Contractor.

100

101 Members will be required to meet control and verification requirements as provided by the OPTN

102 Contractor based on the type of security incident. These requirements will be communicated directly to

103 the member through the information security contact established in the member’s incident response

104 plan.

105 **3.1.C.i Information Security Contact**

106 Transplant hospital, OPO, and histocompatibility laboratory members with access to the OPTN

107 Computer System must identify an information security contact, who is responsible for

108 maintaining and complying with a written protocol that includes how an information security

109 contact will:

- 110
- 111
- 112 1. Provide 24/7 capability for incident response and communications
- 113 2. Receive relevant notifications of security incidents from the member’s information security
- 114 staff
- 115 3. Communicate information regarding declared security incidents to the OPTN
- 116 4. Facilitate development and fulfillment of OPTN Obligations outlined in OPTN Policy 3.1:
- 117 Security Requirements for Systems Connecting to the OPTN Computer System

#

Appendix A: NIST SP 800-171 Controls

Below are the NIST SP 800-171 controls. A full description of each control is provided in the special publication.²⁴ The Committee is proposing that every member must have policies or procedures to address each control within this publication.

Access Control		
Control Number	Description	OPTN Proposed Minimum Control Value
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.	5 login 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.	60 minutes
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 noncommands 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.	

²⁴ 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	OPTN Proposed Minimum Control Value
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.	

Awareness and Training		
Control Number	Description	Proposed Minimum Control Value
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.	Required annually

Audit and Accountability		
Control Number	Description	Proposed Minimum Control Value
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	

Audit and Accountability		
Control Number	Description	Proposed Minimum Control Value
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	Proposed Minimum Control Value
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	Proposed Minimum Control Value
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.	

Identification and Authentication		
Control Number	Description	Proposed Minimum Control Value
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.	60 days of inactivity
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	15 characters (consult NIST SP 800-63B ²⁵ for additional requirements)
3.5.8	Prohibit password reuse for a specified number of generations.	24 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	Proposed Minimum Control Value
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.	

Maintenance		
Control Number	Description	Proposed Minimum Control Value
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.	

²⁵ <https://pages.nist.gov/800-63-3/sp800-63b.html>. Accessed December 15, 2022.

Maintenance		
Control Number	Description	Proposed Minimum Control Value
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.	

Media Protection		
Control Number	Description	Proposed Minimum Control Value
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.	

Personnel Security		
Control Number	Description	Proposed Control Value
3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	

Personnel Security		
Control Number	Description	Proposed Control Value
3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers	

Physical Protection		
Control Number	Description	Proposed Minimum Control Value
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.	

Risk Assessment		
Control Number	Description	Proposed Minimum Control Value
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.	

Security Assessment		
Control Number	Description	Proposed Minimum Control Value
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.	

Security Assessment		
Control Number	Description	Proposed Minimum Control Value
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	Proposed Minimum Control Value
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.	

System and Communications Protection		
Control Number	Description	Proposed Minimum Control Value
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	Proposed Minimum Control Value
3.14.1	Identify, report, and correct system flaws in a timely manner.	Remediation timeframe: High risk - 30 days Moderate risk - 90 days Low risk - 180 days
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.	
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.	

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.