OPTN Network Operations Oversight Committee
Meeting Summary
December 19, 2023
Webex

Daniel Yip, MD, Chair

Introduction

The Network Operations Oversight Committee (NOOC) met via Webex on 12/19/2023 to discuss the following agenda items:

1. Welcome
2. Revised Security Training
3. Revising Conditions for Access to the OPTN Computer System
4. 30 Day Update: Migrating the OPTN Computer System to the Public Cloud
5. Closed Session

The following is a summary of the committee's discussions.

1. Welcome

Dan Yip, Chair of the Network Operations Oversight Committee (NOOC), welcomed committee members and advisors, and provided an overview of the agenda.

2. Revised Security Training

Courtney Jett, Policy Analyst, provided an update on the revised security training to the committee. Ms. Jett explained that the NOOC was asked to review a revised security training for all OPTN Computer System users prior to the meeting. She noted that the training included revisions such as plainer and clearer language, migrating information and questions on security incidents into an Information Security Contact section, and replacing specific questions on security incidents from all user exams with questions on general access and use of the OPTN Computer System.

Ms. Jett asked the committee whether they supported the revisions made, if they had any other suggested revisions, and if 60 days would be an appropriate timeframe to require all users of the OPTN Computer System to complete the security training once it is implemented. Ms. Jett noted that the 60 day timeframe corresponds with the timeframe for deactivating inactive user accounts within the OPTN Computer System.

Summary of Discussion:

The committee discussed whether 60 days was an appropriate timeframe to require all users to complete the security training. After discussion, the committee decided 45 days was a more appropriate timeframe for members to complete the training. The committee also discussed how members would be notified of the training. A committee member suggested that the training notification be advertised in a unique manner to members to ensure the training stands out, and members are aware action is needed. A committee advisor suggested that the OPTN have a disciplined schedule on when to remind members of the training. A committee member commented that they thought the training module was succinct and user friendly.

The committee unanimously agreed on the endorsement of the security training and exam to be implemented in early 3034. The committee also agreed upon a 45 day timeframe in which users must complete their security trainings, once they are implemented.

3. Revising Conditions for Access to the OPTN Computer System

Ms. Jett explained that the committee must review the overarching project goals and questions in order to develop policy and bylaw language on the conditions for access to the OPTN Computer System. Ms. Jett recapped the goals that the committee had discussed in prior meetings:

- Require third-party/business member organizations meet the same security requirements as other OPTN members
- Require DUAs for all organizations who access the OPTN Computer System
- Revise reasons for access to the OPTN Computer System to exclude non-transplant functions/non-OPTN obligation functions
- Revise business membership bylaw to allow new members to join more easily.

Ms. Jett shared the committee's proposed additions to the policy and bylaw language on conditions for access. She noted that these additions included requiring both a primary representative and an alternate representative for business members, and to require interconnection security agreements (ISAs) for all organizations who interconnect with the OPTN Computer System. Ms. Jett noted that to require ISAs for all organizations who interconnect with the OPTN Computer System was a finding from HRSA and is similar to the finding related to data use agreements (DUAs). She noted that HRSA would need to review the proposed language for both the OPTN ISAs and DUAs, and the NOOC will also be asked to review the language of the two agreements.

Ms. Jett asked the committee to consider multiple questions when it came to policy and bylaw language. These questions included:

- How often should DUAs and ISAs be required to be renewed?
- Other than timing, the authorizing individual leaving, or requiring additional interconnections/changing system information, are there triggers for requiring an ISA be revised?
- Other than timing, the authorizing individual leaving, or new terms of data use by the OPTN, are there triggers that would require a DUA be revised?
- Should a DUA be required between two other member types (like a lab and a transplant hospital) who provide each other permissions?
- Should the OPTN require third-party/business member organizations to provide identity verification for users with OPTN Computer System Access?
- What would be a feasible way for the OPTN to identify/verify users with OPTN Computer System access?

When discussing whether the OPTN should require third-party users or business members to provide identity verification, Ms. Jett explained that third party users and business members have access to the OPTN Computer System through multiple member institutions, however these users may not have the same parameters and security measures to access the OPTN Computer System. She noted that this is different than the measures in place for members to access the OPTN Computer System, as certain security measures are required of members by CMS or state and local law.

<u>Summary of Discussion:</u>

A committee member asked about the role of an ISA. Contractor staff explained that an ISA explains what is needed from members in order to connect to the OPTN Computer System. They also noted that ISAs have connecting organizations affirm that they understand and will adhere to OPTN security requirements. They explained that some members will need both an ISA and a DUA in place because an ISA is necessary for members that want to connect to the system, and a DUA is necessary for members that want to access OPTN data.

A committee advisor asked if an ISA is necessary for member institutions and third-party users that access the OPTN Computer System. Contractor staff explained that ISAs are necessary for each and that ISAs will be between OPTN members and the OPTN when the OPTN becomes its own entity. The committee advisor asked if an ISA would replace attestations for members that are currently in place. Ms. Jett explained that the attestations in place apply to every member that accesses the OPTN Computer System and are specific to access, and an ISA is specific to a members' interconnection with the OPTN Computer System. A representative from HRSA noted that member attestations allow them to assess the condition of the OPTN environment, whereas ISAs pertain to the connection between the members' system and the OPTN Computer System.

When discussing policy language, a representative from HRSA noted that some of the questions the NOOC discussed cannot be changed and must be included in policy. A representative from HRSA stated that some of the requirements noted are requirements of the NIST 800-47 framework and pertain to information on ISAs and DUAs.

Next Steps:

Ms. Jett shared that contractor staff will provide draft policy and bylaw language to the NOOC for their review, and that they will discuss the language at a future meeting. Ms. Jett asked that the committee review draft ISA and DUA templates before their next meeting. She noted that the templates are currently under review with HRSA.

4. 30 Day Update: Migrating the OPTN Computer System to the Public Cloud

Dale Smith, Chief Financial Officer, shared that the OPTN contractor and HRSA's scheduled meeting to discuss migrating the OPTN Computer System to the public cloud had been cancelled the day prior, and there was no update to provide to the committee. During the NOOC's meeting on November 15, the committee voted to recommend the OPTN contractor, HRSA, and United States Digital Services (USDS) collaborate and provide a recommendation to the committee on the best way to migrate the OPTN Computer System to the public cloud.

Christopher McLaughlin, representative from HRSA, shared that although the committee asked HRSA to collaborate with the OPTN contractor to move the OPTN Computer System to the public cloud, HRSA is unable to participate in this kind of communication. Mr. McLaughlin stated that because the OPTN Computer System is a proprietary system owned by the OPTN contractor, HRSA is unable to provide guidance or advice in the development or revision of a contractor system. He shared that the OPTN contractor can continue to share suggestions on migrating the OPTN Computer System to the cloud with the NOOC for their consideration. Mr. McLaughlin shared that HRSA is not supportive of any activity to move the OPTN Computer System to the public cloud. Mr. McLaughlin stated that HRSA believes the OPTN Computer System should focus on improving identified vulnerabilities instead.

Mr. McLaughlin was asked to clarify whether he was speaking on behalf of HRSA or on behalf of HRSA and USDS. Mr. McLaughlin shared that he was speaking on behalf of HRSA and cannot speak on behalf of USDS. HRSA agreed to provide more clarity on USDS's stance.

Dr. Yip commented that the NOOC requests the OPTN Computer System prepare for any changes and advances that might be made in the future and agrees that the current capabilities of the OPTN Computer System need to be solidified, however it is important that the system is not standing still.

Summary of Discussion:

A committee advisor asked that since the Board approved of the Finance Committee's recommendation to fund the migration of the OPTN Computer System to the public cloud, is HRSA able to stop the migration. A representative from HRSA stated that HRSA does not support OPTN resources being used in for the migration of the OPTN Computer System to the public cloud.

A committee advisor asked if these vulnerabilities of the system are addressed, will HRSA then support the migration of the OPTN Computer System to the public cloud. Mr. McLaughlin stated that HRSA would like to focus on the vulnerabilities of the system and then once those are addressed, then they may consider next steps. A committee member asked why the OPTN Computer System cannot address identified vulnerabilities and migrate to the public cloud at the same time. Mr. McLaughlin shared that HRSA is unsure the OPTN contractor has the capacity to do both at once.

Mr. Smith asked if HRSA supports the componentized approach the OPTN contractor has suggested for the migration of the OPTN Computer System to the public cloud. Mr. McLaughlin shared that HRSA would need to review a proposal from the OPTN contractor on this componentized approach in order to answer the question.

A committee member asked if HRSA could make a statement on their disapproval of migrating the OPTN Computer System to the public cloud. The committee member shared that as a patient, it seems as if the OPTN is not embracing innovation or moving the OPTN Computer System forward. Mr. McLaughlin directed the committee member to HRSA's modernization effort information and that he would inquire further on whether HRSA is able to provide a statement on their reasons for not wanting to migrate to the public cloud.

5. Closed Session

The committee met in a closed session.

Attendance

- **Committee Members and Advisors**
  - Andrew Kao
  - Colleen McCarthy
  - Daniel Yip
  - Edward Hollinger
  - James Pittman
  - Kelley Hitchman
  - Melissa McQueen
  - Paul Connelly
- **HRSA Representatives**
  - Adriane Burton
  - Christopher McLaughlin
  - Cliff Myers
  - Daniel Thompson
  - Nick Lewis
  - Suma Nair
  - Vinay Vuyyuru
- **UNOS Staff**
  - Anna Messmer
  - Courtney Jett
  - Julie Chatman
  - Kristine Althaus
  - Lauren Mauk
  - Morgan Jupe
  - Roger Vacovsky
  - Steve Mohring
  - Terry Doolittle
  - Tynisha Smith