OPTN Network Operations Oversight Committee
Meeting Summary
May 26th, 2023
Webex

Edward Hollinger, MD, PhD, Chair

Introduction

The Network Operations Oversight Committee (NOOC) met via Webex on 05/26/2023 to discuss the following agenda items:

1. Welcome
2. Security Policy
    a. Proposed Transition Plan
    b. Education Requirement
3. Third Party Security Requirements to Access the OPTN Computer System Policy
4. Incorporation of NOOC into the OPTN Bylaws
5. February 15 OPTN Computer System Outage Root Cause Analysis
6. Closed Session

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

1. Welcome

Dr. Ed Hollinger, Chair of the Network Operations Oversight Committee (NOOC), welcomed committee members and provided an overview of the agenda.

2. Security Policy

Ms. Courtney Jett and Ms. Terri Helfrich presented the proposed transition plan for the security project and the education requirements associated with the project.

Proposed Transition Plan

Ms. Jett presented the proposed transition plan and noted the partnership with Accenture Federal on portions of the implementation plan. The NOOC is looking to solidify a plan for attestation and audits to prepare a standard process and documentation for the OPTN to operationalize. The committee will see the deliverables from Accenture Federal at a future meeting to ensure the timeline is in alignment with the rest of the project timeline.

The implementation requirements were divided into four main groups. The first requirement would be for members to report security incidents and for members to perform security data calls to ensure incidents are reported, as these likely have the biggest impact on the security posture of OPTN members. Members will be informed of this step once the proposal goes before the Board.

The next step would be for members to report information on their respective security contacts, with each member required to submit two site security administrators. The proposed timeline for members to submit this information is from July to December 2023, to allow members the ability to report this information on a rolling basis.

The third step would be for members to complete the initial readiness assessment and training requirements. This step would also be on a rolling basis, with a deadline of March 31, 2024. This deadline is dependent on members having identified and reported an information security contract. The rationale on the three to six months to complete their assessment was discussed, and the proposal of a rolling timeline was also discussed. Ms. Helfrich explained that when the assessments are submitted on a rolling basis, it leads to a more efficient process to ensure data is up to date. Resources and staffing capabilities must also be considered when discussing implementation timelines. During member's initial readiness assessment, the OPTN plans to address critical controls first.

The fourth step of implementation would be to begin the audit cycle, proposed to begin in July 2024. This step is dependent on a member's completion of the readiness assessment, thus allowing members time to begin enhancing their systems, before the OPTN begins auditing. The proposed frequency of audits would be once every three years; therefore, a third of members would be audited every year. The OPTN plans to collaborate with members on their assessments to improve their systems where noted.

Summary of Discussion

Multiple committee members commented that two site security administrators should be straightforward for members to obtain. They commented on the importance of having an information security contact established so the OPTN has a known point of contact. A committee member asked when notice would be sent to members, and Ms. Jett explained that the OPTN will send out notice ahead of the June 2023 Board Meeting to inform members of the project, and another notification will be sent to members immediately after the June 2023 Board Meeting. The committee member suggested allowing members 30 days after the Board meeting to submit their two site security administrators and multiple other committee members agreed with this suggestion. The committee discussed the feasibility of identifying site security administrators for different member types. A committee member voiced their concern that if this notification goes out to members ahead of the Board meeting, that the OPTN may get many questions ahead of time.

When the committee discussed the proposed timeline, a committee member suggested the policy be implemented immediately after it is approved by the Board. A committee advisor asked what typical guidance is utilized during policy implementation. Ms. Jett explained that during a phased implementation process, typically for non-programming requirements, the standard timeframe is three months after Board approval. However, if the policy requires programming, then the policy is implemented after programming is complete. Because this proposal is time sensitive, it is important for the NOOC to consider whether this timeline is appropriate. Ms. Jett explained that the OPTN will allow members at least 30 days' notice of a policy being implemented. A representative from HRSA commented that this is not a standard policy. They continued that the project has not followed a standard process but instead has followed an accelerated process, to implement the policy as soon as possible.

The representative from HRSA suggested that this proposal follow an implementation timeline similar to the proposal from the Kidney Transplantation Committee and Minority Affairs Committee to Modify Waiting Time for Candidates Affected by Race-Inclusive Estimated Glomerular Filtration Rate (eGFR) Calculations. The representative commented that this timeline was appropriate because it is the most recent OPTN policy that has been implemented on a quick timeline. The representative stated that the NOOC proposal should go into effect immediately. They commented that they did not think the proposed timeframe for members to submit security contacts, from July to December 2023, was quick enough. A committee advisor commented that if the OPTN provided notice to members of this change in timeline now, that it would be an onerous task for members to implement.

The committee discussed the proposed timeframe for members to submit readiness assessments to the OPTN on a three-month rolling timeline, ending March 31, 2024. A committee advisor commented that allowing members six to nine months is an adequate amount of time. A committee member commented that it is important to consider members who have little to no infrastructure in place to complete these assessments and to consider whether two to three weeks would not be enough time for them to complete the assessment. The committee member suggested the OPTN start with members who are considered higher risk, so they have more time to amend their systems after their assessments. The committee discussed the concern of having members submit their assessments all at once, because this would be too much data to process at once. After discussion, the committee landed on the decision that three months would be a better timeframe for members to submit their readiness assessments, rather than six or nine months. The committee agreed that this was a more appropriate way to measure members' initial readiness and would provide adequate time to assist members if necessary. The committee decided that the end of December 2023 was a better target for the transition plan.

When discussing the fourth phase of the proposed transition plan, a committee member suggested that the policy implementation language state when the earliest the audit cycle could begin. A representative from HRSA asked if the first round of audits could begin December 2023. However, when the audits can happen will depend on when the OPTN receives the readiness assessment results from members; it is important to evaluate members readiness assessments before establishing an audit timeline. A representative from HRSA asked if auditing members once every three years was an appropriate timeframe. A committee member responded that it was premature to figure out the audit cycle when the OPTN does not have any attestation data yet. When discussing when the audit would take place, Dale Smith, Chief Financial Officer, commented that the timing is pertinent to establish because this would fall on the cusp of either the FY2024 or FY2025 budget and would have a large impact on the OPTN budget. Mr. Smith explained that there is currently 2-2.5 million dollars allocated in the FY2024 budget for this audit work to be completed. Ms. Helfrich explained that the contractor has asked Accenture Federal for preliminary cost estimates for the first year and what ongoing costs may be. This cost will be based on decisions made by the committee on how much work the contractor should perform on audits annually. A committee member commented that the attestation was a good baseline to determine where members are with their security systems, and these initial attestations would help determine how frequently members should be audited.

Education Requirement

Ms. Jett presented the educational requirements for the member information security policy. An overview of the concerns about security training, expressed by Board members and HRSA, was provided to the committee. For example, a concern expressed by HRSA is whether members understand OPTN data protection obligations.

The committee was asked whether they share the same sentiments around member accountability and whether it is permissible for members to attest that they have completed information security training on an annual basis. The committee reviewed potential options if they were worried about accountability; the options presented to the committee were that they could include completion of user training in the annual attestation and audit every three years, or they could require user training be completed in the OPTN Contractor's learning management system and directly audit on a timeframe as determined by the NOOC.

The committee discussed OPTN data obligations members may have. Two potential options for them to explore would be to have members complete an educational program to test their knowledge. This training would span generic technology security data, to more specific transplant training. A second option for the committee to consider would be for members to provide their generic training in their

attestation, and then be required to complete a shorter version of the training to cover OPTN specific topics. This means that all members would have to take OPTN specific training in some respects, but these options mean that members would be able to avoid taking a generic training course multiple times.

Summary of Discussion

A representative from HRSA explained that based on feedback they have received, members already have security training in place and therefore members were interested in attesting to having completed the security training, rather than having to take an OPTN specific security training. HRSA expressed their concern that member institution trainings may not be OPTN focused enough and would not be an adequate alternative. A committee member explained that this was not an accurate representation of what the proposal was, and explained that members could attest to generic security pieces from their institution's training, but there would be specific training for members to address OPTN security components. The public comment feedback the proposal received was that members already complete multiple security trainings and they do not need another.

A representative from HRSA asked how the OPTN plans to train members who allow third-party access to the OPTN Computer System. The committee chair explained that this is a different issue than what the committee was discussing. They agreed that the NOOC and the OPTN needed to discuss what data use agreements should look like, but this is not something that every member needs to be trained on. The committee chair commented that this was a contract level discussion and not a discussion for the OPTN. The representative from HRSA stated that they wanted OPTN members who grant third-party users access to understand why they are granting these users access. They thought that members who are using the data should have some awareness of the need to protect it. The committee chair suggested that the NOOC make the training OPTN specific and have as little generic information in the training as possible. A committee advisor agreed and commented that members should be able to take their organizations generic security training and be able to attest to it, and then take a specialized OPTN security training.

The committee chair summarized the conversation and stated that the NOOC agreed members must complete their institutions IT security training, and the training must adhere to the parameters set by the OPTN. Members will attest to completing the training and attest that the training included the requirements noted by the OPTN. The committee decided that all members need to complete OPTN specific training that will be developed by the OPTN, and anyone who accesses the OPTN Computer System must also complete this training.

A committee member asked what frequency the OPTN should require members to complete their OPTN-specific security training. After discussion amongst the committee, the committee agreed that annually was appropriate. Ms. Jett explained that an OPTN contract modification also requires the attestation to be completed annually.

A representative from HRSA asked the committee if they thought there was specific training that security leaders within member institutions should be required to complete. The committee chair responded that it seemed appropriate to remind these users of their contractual obligations, but because this person could be different at different member institutions, it is not easy to decide on a single requirement for these leaders. The committee chair stated that this could be appropriate training for administrators who are not necessarily accessing the system through a user account. The committee chair thought that this was an important issue to discuss in the future with a legal viewpoint.

3. Third Party Security Requirements to Access the OPTN Computer System Policy

Ms. Kristine Althaus, Identity and Access Management Analyst, presented on third-party security requirements to access the OPTN Computer System and the current policy that is in place. Ms. Althaus explained that there is currently no direct accountability model for third-party organizations with the OPTN nor are there requirements at the organizational level for third parties. The committee was asked to determine what security requirements they believe should be in place for third parties at the organizational level. Two focus areas to determine the security requirements dealt with the requirements around accessing the OPTN Computer System, and requirements around incident management and reporting. Thus, the committee was asked to consider whether third-party users should be required to identify a security point of contact.

When discussing potential security requirements for systems accessing the OPTN Computer System, there were five options for the committee to consider. Option one was that third-party members must provide security for the computing environments and components. Option two was that third-party members must adhere to the most recent revision of the 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. Option three was that third-party members must attest to their adherence to their security framework through an OPTN attestation. Option four was that third-party members OPTN attestations must be submitted annually and upon request by the OPTN to maintain access to the OPTN Computer System. And option five for third-party members was that adherence to the security framework will be audited at least once every three years and third parties must also respond to OPTN requests for information within the timeframe stated by the OPTN.

Summary of discussion:

A committee member commented that it would be difficult for the OPTN to insert themselves into the contractual agreement between members and their third-party contractors. They commented that this could put the OPTN into complicated legal positions. A representative from HRSA agreed that it is complicated, however, it should not matter. They stated that if a third-party user, contracted through a member institution, is accessing OPTN Data then they should still be subject to OPTN requirements. The committee chair responded that the OPTN should provide OPTN members with the tools to be responsible for their own third-party users. Another committee member commented that whoever a member contracts with is responsible for their actions; it is not necessary to have separate requirements. A committee member stated that it is important for these members to understand the requirements they need to put in place for their third-party users when they are creating a contractual agreement with them.

Ms. Jett asked the committee whether they were concerned that the OPTN did not have a direct accountability model for third-party users or would the NOOC prefer to leave it at the member level, so members are responsible for their third-party users directly. The committee chair commented that this was too difficult to do and would make things more challenging. They stated that if a third-party user only has access to OPTN Data through a member, then the OPTN should hold the member accountable for their contracted users. Another committee member agreed with this suggestion and stated that all members are responsible for all the actions of whomever they choose to contract with.

A representative from HRSA asked how the committee thought the OPTN should handle situations where there are multiple members contracted with a single third-party user. The committee chair thought that this went back to the importance of educating members and explaining that they are responsible for their third-party users and members should have this language in their data use agreements with any third-party users.

A representative from HRSA asked if there was any information about data aggregation when it came to third-party access. They suggested that when the project undergoes its next round of the policymaking process, that the committee consider whether they would like to include information about data aggregation. A committee advisor stated that in the long term, the OPTN will likely need to categorically change the membership of the OPTN and expand to ensure there is a spot for third-party entities to allow the OPTN some oversight of these third-party users.

Next Steps:

The committee agreed that this is an important conversation that should be revisited in a future meeting.

4. Incorporation of NOOC into the OPTN Bylaws

Ms. Rebecca Murdock, Senior Policy Counsel, presented the proposal to incorporate the NOOC into the OPTN Bylaws. Ms. Murdock explained that the NOOC is not currently in OPTN Bylaws and including it would ensure that it stays within the governance structure of the OPTN. The proposed language to include in the OPTN Bylaws to incorporate the NOOC was presented to the committee as open and broad to ensure flexibility to the committee and allow the committee to adjust based on the committee's needs. Including the committee into the OPTN Bylaws ensures that there is a referring body of delegation when it comes to potential authority making decisions from the Board to the NOOC.

Summary of discussion:

There were no questions or comments.

Vote:

The committee voted unanimously to recommend that the Board incorporate the OPTN Network Operations Oversight Committee into the OPTN Bylaws.

5. February 15 OPTN Computer System Outage Root Cause Analysis

Mr. Tiwan Nicholson, Senior Director IT Operations, presented an update on the February 15 OPTN Computer System outage and an update on the root cause analysis (RCA) of the outage. The RCA of the outage was provided to the committee ahead of time in their materials and has also been submitted to HRSA. Mr. Nicholson explained that more conversations between the OPTN and HRSA will likely take place in the future about the details of the RCA and to discuss potential corrective actions.

A summary of the RCA was provided to the committee. Mr. Nicholson explained that the OPTN was able to recreate the event in a controlled environment to better understand what happened. It was explained that a series of innocuous events came together and caused a degradation on the file repository, which bled into the interaction with the database server, and because the database server is the primary database node, then it could not perform its normal synchronization within the cluster, therefore leading to a cluster failure.

Many actions have been taken since the outage, and changes have been made with the vendor to reconfigure the backup. The OPTN has also made recommended changes to their database configuration, based on recommendations from Microsoft. Other actions that have been taken since the outage include general health and optimization changes on the process schedule of the system and analyzing if this is the appropriate schedule for the system.

Summary of discussion:

There were no questions or comments from the committee.

6. Closed Session

The committee met in a closed session.

Attendance

- **Committee Members and Advisors**
  - Adam Frank
  - Bruno Mastroianni
  - Daniel Yip
  - Edward Hollinger
  - James Pittman
  - Kelley Hitchman
  - Maryjane Farr
  - Melissa McQueen
  - Paul Connelly
- **HRSA Representatives**
  - Adriana Martinez
  - Arjun Naik
  - Christopher McLaughlin
  - Nick Lewis
  - Vanessa Arriola
  - Vinay Vuyyuru
- **UNOS Staff**
  - Alex Tulchinsky
  - Amy Putnam
  - Anna Messmer
  - Bonnie Felice
  - Courtney Jett
  - Dale Smith
  - Julie Nolan
  - Krissy Laurie
  - Kristine Althaus
  - Laura Schmitt
  - Liz Robbins Callahan
  - Lloyd Board
  - Marty Crenlon
  - Matt Belton
  - Michael Ferguson
  - Michael Ghaffari
  - Morgan Jupe
  - Rachel Hippchen
  - Rebecca Murdock
  - Rob McTier
  - Robert Emerson
  - Roger Vacovsky
  - Terri Helfrich
  - Tiwan Nicholson
  - Tynisha Smith
- **Other Attendees**
  - Nathan Kottkamp