UNOS
UNITED NETWORK FOR ORGAN SHARING
Saving lives together

[redacted]
www.unos.org

Brian M. Shepard
Executive Director & CEO

March 2, 2022

VIA ELECTRONIC MAIL

The Hon. Ron Wyden, Chairman
The Hon. Charles Grassley
U.S. Senate Finance Committee
Washington, D.C. 20510

Dear Chairman Wyden and Senator Grassley,

We appreciated the opportunity to brief your staff regarding the issues raised in your January 31, 2022, letter concerning UNOS' IT security and technology infrastructure and practices. We are pleased to provide the following additional information and actions taken since our February 17, 2022 meeting, in addition to the presentation materials and requested root cause analysis submitted to HRSA on February 26, 2021.

Penetration Testing

Senate staff inquired about the role of external entities in conducting penetration testing. Below are clarifications about our most recent tests.

- A third-party commercial company conducted the 2021 tests. Penetration test was a web application test with and without credentials. Testing was conducted in our "production equivalent" environment.
    - The HHS Office of Inspector General (OIG) and HRSA accepted this test in lieu of performing their own penetration test for the 2021 Audit
    - No vulnerabilities were identified allowing escalation of privilege or ability for lateral movement
    - As promised, we are providing the results and remediations from the 2021 penetration test:
        - 0 Critical
        - 3 High: All closed immediately
        - 6 Medium: 5 Closed, 1 pending software update available in June 2022
        - 3 Low: 1 Closed, 2 pending closure with code roll-out May 2022
- A HRSA-selected vendor, Synack, will conduct the 2022 test. It will be a crowdsourced penetration test. The test will be in non-credentialed and credentialed format.

UNOS Relationship with Cybersecurity & Infrastructure Security Agency (CISA)

Senate staff recommended UNOS seek out free cybersecurity resources and services, such as the EINSTEIN sensor, offered by CISA to private sector organizations operating "critical infrastructure" for the nation. At this time, the OPTN system is categorized by HHS as a "high-value asset" and is ineligible for all services provided to infrastructures with this more elevated designation.

We appreciate, however, the suggestion to secure cybersecurity hygiene scans from CISA and have taken steps to request this important service.

UNOS established a relationship with CISA in 2015 and at that time registered for and participated in the Government Telecommunications Service (GETS), Wireless Priority Service (WPS), and Telecommunications Service Priority (TSP) programs. We have since sponsored numerous OPOs in support of their participation in the program.

Security Clearances and Classified Warnings

- [redacted]
- UNOS meets the contractual obligation as stated in the Position Sensitivity Designations requirements within the current OPTN contract, which states: "*All Contractor (and/or any subcontractor) employees must obtain a background investigation commensurate with their position sensitivity designation that complies with Parts 1400 and 731 of Title 5, Code of Federal Regulations (CFR).*"

Code Scanning and Review

- UNOS scans code throughout the software development lifecycle using [redacted] technology
- Snippets of code have been and will continue to be made available to HRSA for verification and closure of findings as needed
- Over the past several months, HRSA and UNOS have been working to establish a process for reviewing code. We estimate that HRSA will begin code reviews in Q2 of 2022.

Vulnerability Management

- Infrastructure vulnerability scanning is performed weekly using [redacted], and all results are provided to HRSA
- HRSA is provided access upon request and on a regular schedule to perform web applications scanning, using [redacted], against a production equivalent environment.

Offsite Backup Storage

- Offsite backup storage practices have been in place since the OPTN system's inception in 1999 and continue in the present.

2010 Modernization Project

- As a follow up to your question regarding the 2010 system modernization project:
    - A project called Chrysalis was terminated in 2012 after concluding that it would not go far enough to modernize and evolve the OPTN technology.
    - Following that decision, UNOS determined that the path forward needs to be centered on digital transformation of the OPTN System, embracing and practicing the Agile methodology, test automation, open-source frameworks, Application Programming Interfaces (APIs), mobile capabilities, elevated security practices, and cloud computing. As a result of this direction and culture, we have been able to –
        - React faster to the needs of the transplant community
        - Establish and maintain a consistent feedback loop with the users of OPTN system
        - Integrate cloud-based data analytics and machine learning capabilities
        - Implement a variety of open-source frameworks to deliver value
        - Enable members to benefit from our seamless integration with EHRs and EMRs
        - Empower members with secure mobile capabilities to perform work whenever and wherever
        - Reduce the threat landscape by implementing zero trust principles in conjunction with a defense-in-depth strategy
        - Maintain high quality of software, leveraging 24x7 automated testing
        - Deliver on the OPTN Board of Directors commitments
        - Retain and attract engineering talent

February 2021 Service Outage

- To clarify our response in our meeting, the February 2021 one-hour service outage occurred as the result of a failure within a high-availability redundant pair of internal firewalls, not a manual human error. The human error occurred during the service restoration effort. As requested during the meeting, the root cause analysis previously provided to HRSA is included as part of this response. Since this incident, further automation has been added to service restoration procedures to eliminate the need for human intervention.
- *Please note the graphic depicted in the provided RCA reflects the OPTN system architecture as of February 2021, while we were in transition to the current state architecture.* The OPTN system architecture today reflects what was presented to the staff during our call. It has additional built-in redundancies and security components, advanced use of public and private cloud, and automation.

Please do not hesitate to contact me if you have additional questions or require further clarifications.

Sincerely,

Brian Shepard, CEO
United Network for Organ Sharing

Attachments (2): *UNOS IT Security Presentation for Senate Finance (17 Feb. 2022); UNet Root Cause Analysis (6 Feb. 2021)*

[redacted]

OPTN Technology & Security Briefing

United Network for Organ Sharing

U.S. Senate Finance Committee Staff

February 17, 2022

[redacted]

Areas of Focus

- System modernization and reliability
- Sufficient backup systems
- Cloud utilization
- Security of the system from cyberattacks
- Basic features and security systems
- Ensuring that security flaws do not lead to preventable deaths
- Prevention of service interruptions due to ransomware attack, technical failure or inefficiency causing delays

[redacted]

System Modernization, Reliability & Cloud

- ✓ System modernization and reliability
- ✓ Cloud utilization
- ✓ Prevention of service interruptions due to ransomware attack, technical failure or inefficiency causing delays

Public Cloud Services (SaaS, PaaS, API)

[redacted]

System Backup & Recoverability

[redacted]

[redacted]

- ✓ System modernization and reliability
- ✓ Sufficient backup systems

Transfer Off-site

[redacted]

Continuous Data Replication
Intra- and Inter-site using high availability database clustering

Scheduled System Backups
Intervals ranging from every 15 minutes to once daily

Rapid Recoverability
Daily backups stored on-site for 3 weeks

Archival
Weekly, monthly, and annual backups stored off-site for 8 weeks, 2 years, and 4 years respectively

[redacted]

OPTN System Protections Are Working

- ✓ Security of the system from cyberattacks
- ✓ Basic features and security systems
- ✓ Prevention of service interruptions due to ransomware attack, technical failure, or inefficiency causing delays

Statistics

Websites blocked:	3,813,576
Inbound email blocks:	444,600
Emails quarantined:	33,806
Crowdstrike (End-Point Detection) alerts:	592
Refused connections:	1,204,258,768
Countries blocked	200 +
Events requiring follow-up by IS	286
Impactful incidents:	**0**

Click to add text

100% of staff trained annually and tested in security and privacy

Phishing Awareness and Response for 2021

4,539 phishing emails sent by Information Security
2,436 reported to Information Security
53% reporting rate
85 total clicks

1.87% click rate*

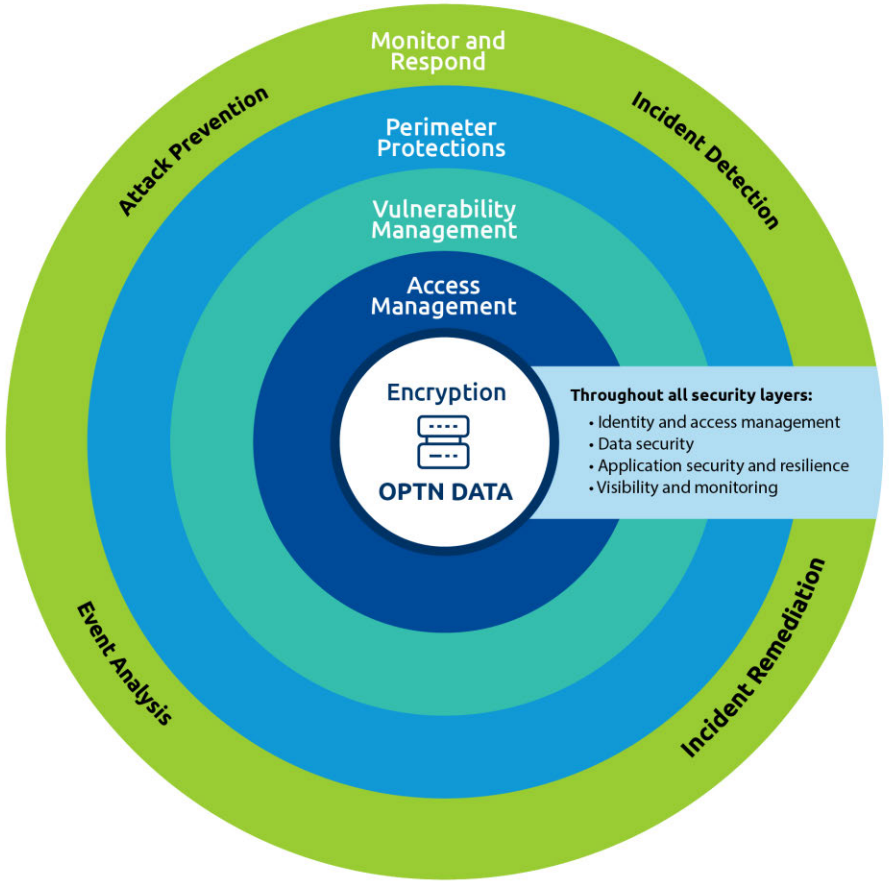
** KnowBe4 2021 Statistics for Healthcare: 3.7% click rate after training*

Security for the OPTN System

[redacted]

Defense-in-Depth

Application of fundamental security protections in a "layered" approach



[redacted]

Zero Trust Principles

Focus on data protection by applying granular access controls, continuous and comprehensive monitoring, and reliance on automation

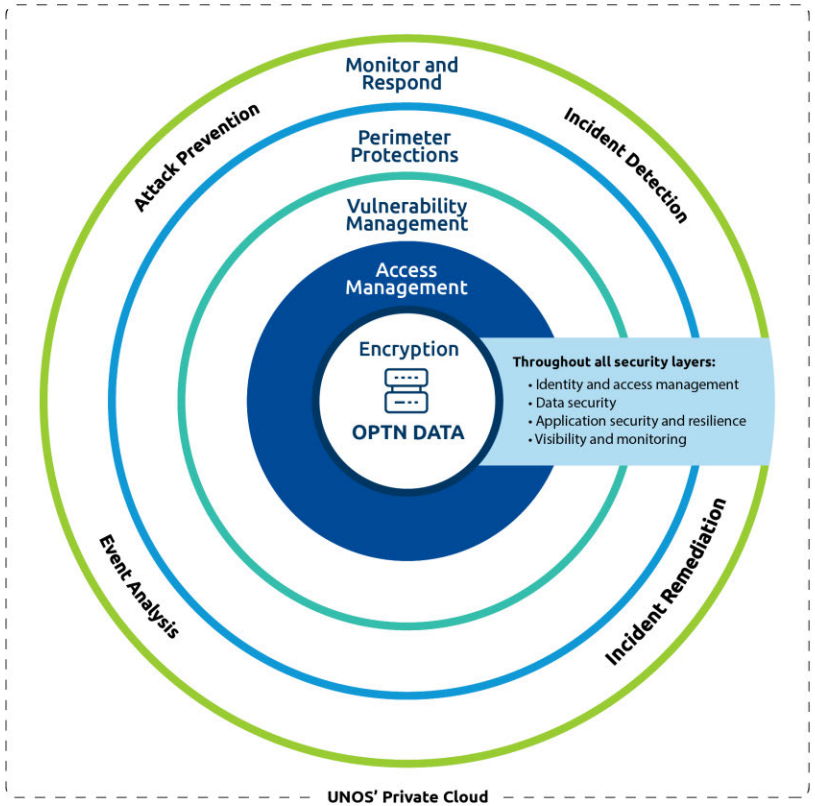
[redacted]

[redacted]

Access Management

Access to systems and data provided to the right individuals, at the right time, for the right reason

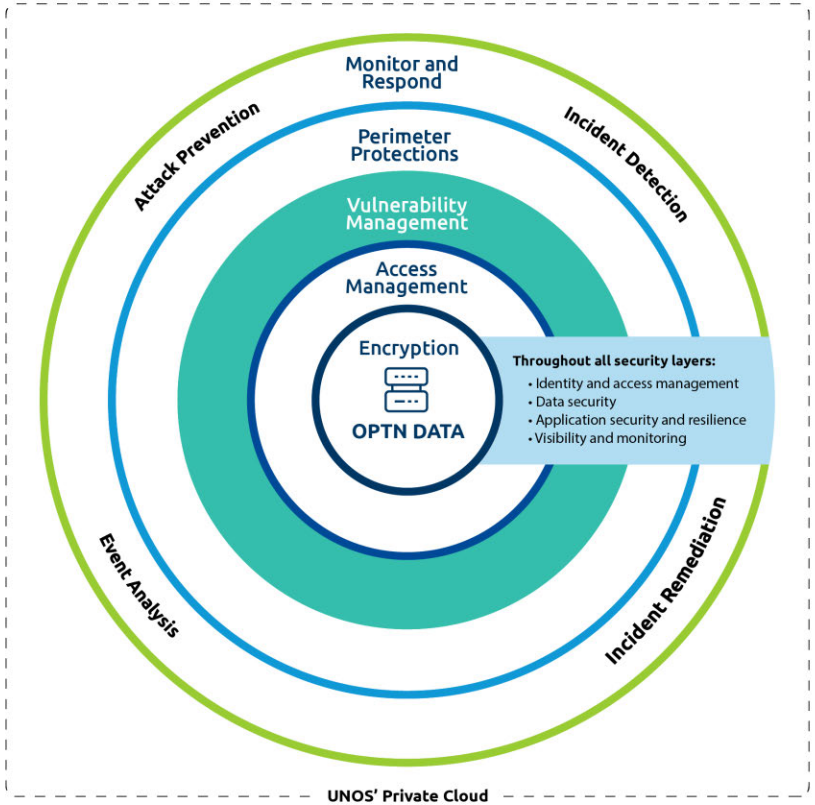
Areas of Focus	UNOS Capabilities
Basic features and security systems	✓ Role-Based Access Control (RBAC) ✓ Multi-factor authentication ✓ Encrypted data, channels and network drives
Ensuring that security flaws do not lead to preventable deaths	✓ Reduces risk of malware and ransomware propagation by preventing scope of administrator capabilities
Prevention of service interruptions due to ransomware attack, technical failure, or inefficiency causing delays	✓ Multi-factor authentication ✓ Reduce risk of malware and ransomware propagation by preventing scope of administrator capabilities



Vulnerability Management

Ensures doors are shut

Areas of Focus	UNOS Capabilities
System modernization and reliability	✓ Automated software code analysis
Basic features and security systems	✓ Continuous vulnerability scanning ✓ Automated patching and remediation ✓ Scanning to detect code and on-line vulnerabilities in web applications (SAST and DAST)
Ensuring that security flaws do not lead to preventable deaths	✓ Continuous vulnerability scanning ✓ Automated patching and remediation ✓ Scanning to detect code and on-line vulnerabilities in web applications ✓ Penetration testing to simulate cyber attacks

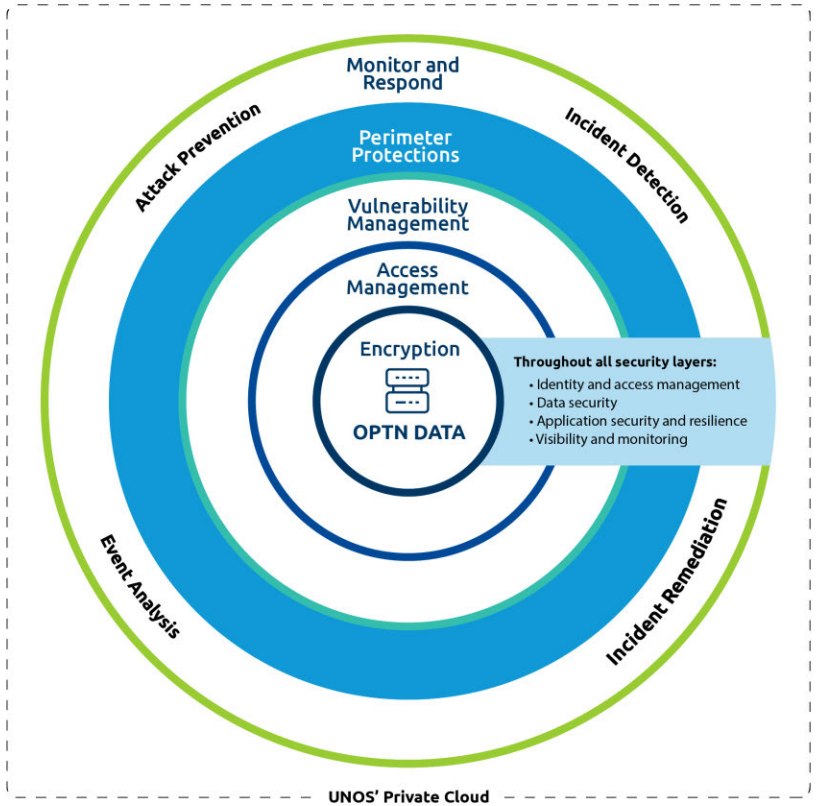


[redacted]

Perimeter Protections

Perimeter protections allow appropriate business activity

Areas of Focus	UNOS Capabilities
System modernization and reliability	✓ 5th generation firewalls ✓ End-point Detection and Response through Crowdstrike ✓ Canaries for early detection and alerting
Cloud utilization	✓ [redacted] cloud services to quickly update attack signatures, threat hunting and forensics ✓ 5th generation firewalls extended to Microsoft Azure
Security of the system from cyberattacks	✓ Intrusion detection and prevention to block attacks and suspicious traffic ✓ Attack identification and automated system containment to prevent spread of malware and ransomware
Prevention of service interruptions due to ransomware attack, technical failure, or inefficiency causing delays	✓ Intrusion detection and prevention to block attacks and suspicious traffic ✓ Attack identification and automated system containment to prevent spread of malware and ransomware ✓ Threat hunting to seek out signs of an intrusion

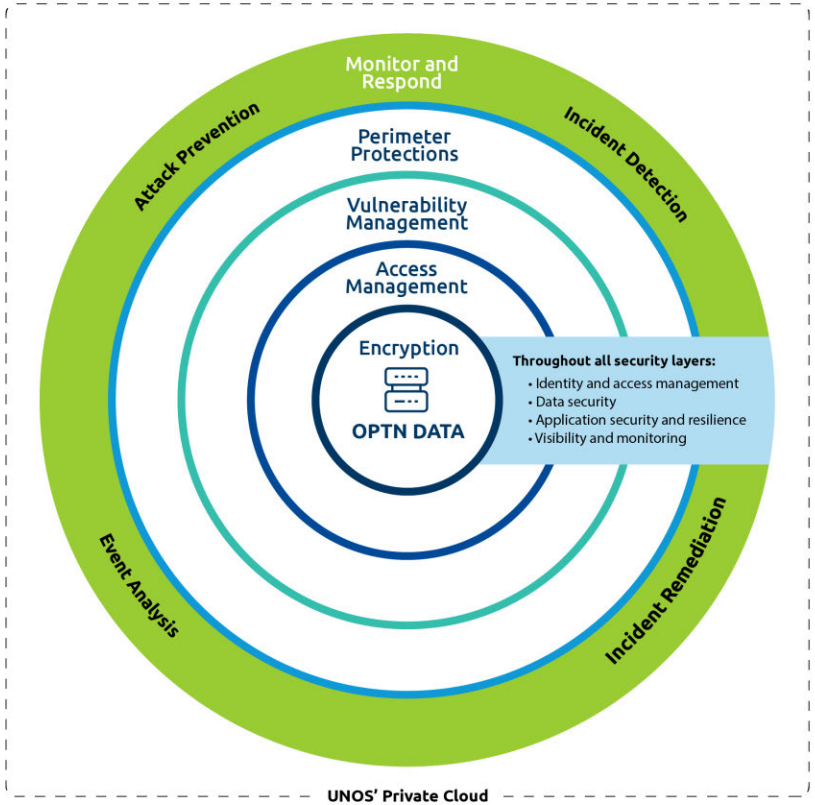


[redacted]

Monitor and Respond

Continuously identify and respond to potential threats

Areas of Focus	UNOS Capabilities
System modernization and reliability	✓ Monitoring of server-to-server traffic within a virtual machine ✓ Industry leading Security Information and Event Management System (SIEM)
Cloud utilization	✓ Cloud implementations for up-to-date capabilities and threat detections
Basic features and security systems	✓ Latest in logging and correlation ✓ File integrity monitoring and alerting ✓ Data leak identification and prevention
Prevention of service interruptions due to ransomware attack, technical failure, or inefficiency causing delays	✓ Monitoring of server-to-server traffic within a virtual machine ✓ Security information and event management system ✓ Cloud implementations for up-to-date capabilities and threat detections ✓ Advanced data correlation and alerting



[redacted]

Thank you!

[redacted]

[redacted]

Appendix

[redacted]

UNOS Information Security Team

- More than 112 years of combined IT and Information Security Experience
- Holds 27 industry recognized certifications including:
  - Certified Ethical Hacker (CEH)
  - Certified Cloud Security Professional (CCSP)
  - Certified Detection Analyst (CDA)
  - Certified Incident Handler (CIH)
  - Certified Information Systems Security Professional (CISSP)
  - Certified Penetration Tester (GPEN)

UNOS UNITED NETWORK FOR ORGAN SHARING

IT Operations RCA Report

Incident: Periodic UNet℠ Access Impact

Date & Duration of Incident: 2021-02-06 8:10PM EST - 11:00 PM EST

Incident Summary

Starting around 2021-02-06 8:15PM EST, users began to experience periodic latency and errors in UNet functions

Root Cause

East Region 1 (ER1) Computing Environment experienced a Network Equipment failure

Detailed Description

UNet users experienced periodic latency or errors as a result of ER1 Networking Equipment failure.

Between 08:10pm and 08:15PM EST, one node of a clustered pair of internal [redacted] firewalls experienced an interface failure which cascaded to the other firewall node, resulting in a total failure of the internal firewall cluster.

This failure, in turn, caused interruption to internal network traffic in ER1. [redacted] technical support confirmed that the issue was caused by a defect in the [redacted] firewall's firmware.

Continued on Next Page

Issue resolution actions consisted of transitioning impacted workloads from ER1 to ER2 computing environment, as well as taking the ER1 internal firewall cluster offline and bypassing internal network traffic.

Additional Information

Throughout the incident some workloads running in ER1 remained there. Periodically, between 08:25 and 09:25PM EST, ER1 was not accessible to UNet users. Procedural errors made in the process of transitioning some workloads from ER1 to ER2 contributed to this incident. All other steps taken (manual and automated) during this incident were accomplished without any errors.

The equipment in question has not been put back in service.

Since the incident, ER1 has been and continues to be fully operational. All normal workloads/activities have been and are functioning there.

Action steps taken during incident:

08:12PM EST	Initial [redacted] alerts received
08:25PM	Organ Center (OC) receiving Members Calls
	IT On-call responding engineer informs On-call manager and begins to evaluate the issue
08:33PM	Conference Bridge initiated
08:56PM	ER1 Networking Equipment failure identified as triggering event
	Systems Engineer enroute to ER1
09:10PM	Decision is made to move some UNet functions to ER2. Leverage external Transition Plan (TP) in [redacted]
	Additional Systems Engineers are brought into the Conference Bridge to assist
09:23P	TP procedures to ER2 are initiated
09:40P	TP procedures to ER2 are completed Reviewing periodic ThousandEyes.com alerts reported in operational logs
09:45P	UNet functions to add candidate or register donor are functional
10:01P	Some functions transitioned from ER1 to ER2 generating periodic alerts
10:22P	Issues in executing TP procedures to ER2 identified on the Conference Bridge: 1) External Plan not up to date 2) Human data entry errors
10:30P	Corrective Actions identified to address issues in TP procedures
10:58P	UNet functions accessible both internally and externally

Continued on Next Page

Corrective Action:

We have completed our detailed investigation and compiled our corrective actions to prevent future incidents of this kind:

● All procedural documentation will be updated in Attainium.net first then synchronized with on premises copy. Attainium.net has no dependency to internal infrastructure. (Completed 2/8/21).

● Transition Plan (TP) procedures training will be updated to accommodate all scenarios. Staff retraining has commenced, and will be required for all new team members. Training will be ongoing as procedures are updated, and a quarterly review of all procedure documentation will be conducted.

● Continue with additional automation (scripting) to further reduce manual TP tasks, avoiding potential for human error and resulting in faster transitions. (2/28/21)

● [redacted]

UNet℠ Operating Environment: April 2021

[redacted]

OPTN ORGAN PROCUREMENT AND TRANSPLANTATION NETWORK UNOS Confidential

Continued on Next Page

UNOS UNITED NETWORK FOR ORGAN SHARING

● Provide continuous updates to HRSA (2/9 and 2/11/21) and NOOC (2/19/21) on UNet availability to maintain confidence in the system

UNet℠ Availability last 12 months

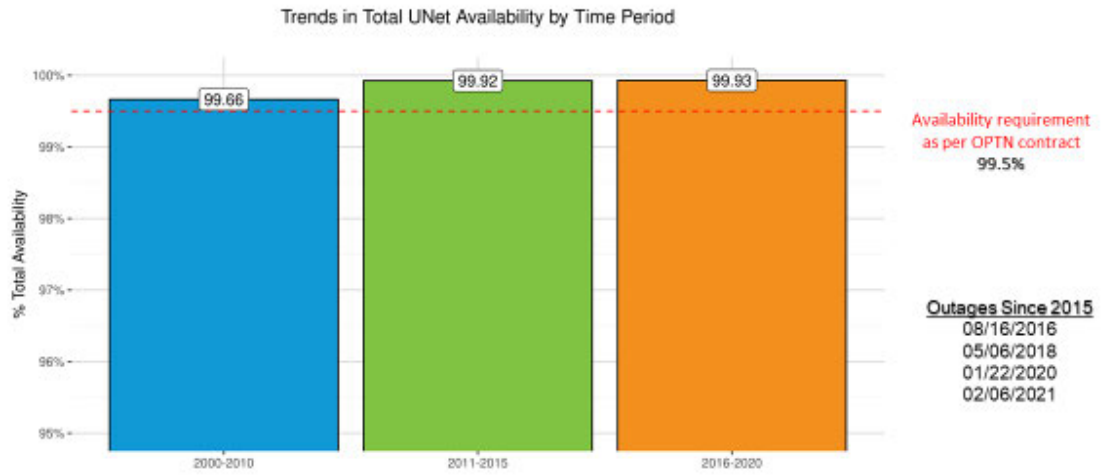
Month	UNet Availability
Feb 2020	99.81%
Mar 2020	100.00%
Apr 2020	100.00%
May 2020	99.75%
Jun 2020	99.94%
Jul 2020	99.78%
Aug 2020	99.95%
Sep2020	100.00%
Oct 2020	100.00%
Nov 2020	100.00%
Dec 2020	99.83%
Jan 2021	100.00%

Availability during this period
99.92%

Availability requirement as per OPTN contract ***99.5%***

OPTN ORGAN PROCUREMENT AND TRANSPLANTATION NETWORK 6

UNet℠ Availability last 20 years



OPTN ORGAN PROCUREMENT AND TRANSPLANTATION NETWORK 7