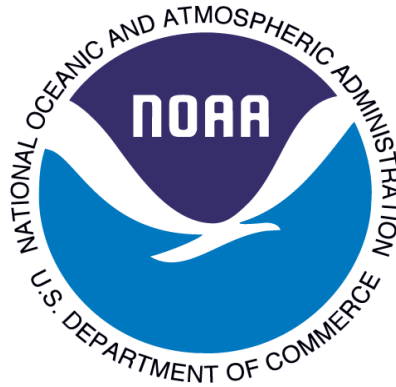# National Oceanic and Atmospheric Administration (NOAA)
Office of the Chief Information Officer (OCIO)

NOAA (N-Wave)

Service Catalog

Version 1.5
Q2 FY22

Track Changes

Version Number	Date	Description of Change/Revision	Section/Pages Affected	Changes Made by Name
1.2	Q4 FY20	Revised catalog for new format	all	R. Sears
1.3	Q2 FY21	Updated cloud services	page 5	R. Sears
1.4	Q2 FY21	Updated firewall services	page 6	A. Nemethy
1.5	Q2 FY22	Updated Multiple Services	All	A. Nemethy/A. Bogner

Table of Contents

I. N-Wave Provided Services

N-Wave offers key technical services as described in the N-Wave Service Catalog. The N-Wave Service Level Agreement further defines the expected service performance, metrics and delivery. The following technical service areas are offered. Costs for specific services are provided upon receipt of an N-Wave service request with required additional customer information.

- Enterprise Transport Services (Layer 0-3)
- Trusted Internet Connection Access Provider (TICAP)
- Enterprise Network Services
- Enterprise Cloud Services
- Network Operations
- Security Controls

II. *Subscribed Services*

Enterprise Transport Services (Layer 0-3)		
Service Type	**N-Wave Role**	**Customer Role**
Co-location	Provide racks for customer network assets at the specified co-location facility.	- Define a program representative as Point of Contact (POC) for this service.
Layer 1: Lit and Dark Fiber Services	Provide annual procurement and tracking of lit and dark fiber services.	- Define a program representative as POC for this service.
Layer 1: Optical Lambda transport over DWDM gear – 10G/ 100G	In specific regions, N-Wave may be able to provide optical engineering solutions.	- Define a program representative as Point of Contact (POC) for this service.
Layer 2: Virtual Local Area Network (VLAN) transport – 1G/10G/100G	N-Wave can provide private ethernet transport services, VLAN multi-point at 1G, 10G to 100G to support: - Wide area and metropolitan-area connectivity to NOAA campuses, laboratories, data centers and sites - Wide area and metropolitan-area transport for direct intra program connectivity. - Virtual Private LAN Service (VPLS) to provide ethernet-based multipoint to multipoint communication.	- Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process.

Layer 3: Internet, Internal-external routing 1G/10G /100G	N-Wave can provide private Layer 3 VPN multipoint IP routed services, Public Layer 3 transport to the NOAA TICAP (Internet, Internet2), NOAA-to-NOAA IP transit, 1G and 10G and up to 100G for R&E peering to support: - Wide area and metropolitan-area connectivity to NOAA campuses, laboratories, data centers and sites - Wide area and metropolitan-area transport for direct intra program connectivity. - Multiprotocol Label Switching (MPLS) allows for the creation of end-to-end circuits across any type of transport medium, using any protocol. - Both IPv4 and IPv6 transport. - Multicast communications. - Transport to NOAA TICAPs. - Internet and R&E providers. - Cloud services connectivity 1G VPN (any Cloud service provider). - Cloud broker connectivity service 2-10G (e.g., Azure, AWS, Google, Azure-AWS Gov, Oracle).	- Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process.
Trusted Internet Connection Access Provider (TICAP)	- High bandwidth and availability - Redundant TICAP infrastructure at sites in the D.C. metro, Denver, Seattle and Honolulu - TICAP sites in the contiguous U.S. are capable of failover within and between sites - Dedicated infrastructure in Honolulu reduces latency for customers at Hawaii sites - X-Wave ensures symmetric traffic flow through each TICAP - Service is compliant with Office of Management and Budget TIC requirements - 24x7 Tier 1 support and expert troubleshooting from a centrally managed and geographically dispersed team of Tier 2 and 3 engineers - Robust configuration management, monitoring, alerting and diagnostic tools TIC customers can inherit the following controls through CSAM: • SC-7.c, SC-7(3), SC-7(4).a, SC-7(4).b, SC-7(4).d, SC-7(4).e – Boundary Protection	- Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process.

Enterprise Network Services		
Service Type	**N-Wave Role**	**Customer Role**
Cable plant	- Provide cable plant standards, training and mechanism for tracking cable assets.	- Help adhere to cable plant standards. - Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process.
Managed Local Area Network (LAN)	- Provide network as a service. - Procure, install, configure, patch, scan and perform annual assessment and authorization on N-Wave managed network components. - Access layer is normal business hours with core layer 24/7.	- Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process. - Customer is responsible for patching end systems into switches.
Enterprise Wireless	- Design, deploy, manage and monitor the wireless network infrastructure within the campus. - Respond to Tier 2/3 system level issues from the campus. - Provide training for system administrators. - Normal business hours response.	- Report issues to their local Systems/IT administrator. - Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process.
Local N-Wave services engineer	- Provide onsite tier 2/3 N-Wave network engineers for direct campus support of N-Wave services. - N-Wave engineers will prioritize efforts to N-Wave campus provided services and N-Wave enterprise services in use at the campus (e.g.wireless, VPN). - Normal business hours response. - Onsite engineers will provide hands and eyes for N-Wave equipment and troubleshooting of N-Wave services. - Interface with local POCs on an ongoing basis to provide the site with a more personalized experience.	- Verify and troubleshoot connectivity from end device to N-Wave device. - Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process.
Enterprise Remote Access VPN (ERAV)	- Provide Client remote access VPN services for access to internal network resources. - Normal business hours response.	- Designate VPN admin to be the POC for VPN group. - VPN admin will triage user issues and, when needed, submit tickets to N-Wave. N-Wave will only accept tickets from designated VPN admins. - Users desktop support are

Service Type	N-Wave Role	Customer Role
		responsible for maintaining VPN profiles and Anyconnect versions.
Firewall services	- Provide firewalls as a service, including procurement, installation, configuration, monitoring, and management. - 24x7x365 management, monitoring and response.	- Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process. - Customers need to ensure the request is approved by the customer change management process prior to submission to N-Wave. N-Wave will only accept changes from approved submitters. - Customers will be responsible for defining security rules.

Enterprise Cloud Services		
Service Type	**N-Wave Role**	**Customer Role**
Azure commercial landing zone	- N-Wave provides hub and spoke topology. - N-Wave manages the hub consisting of load balancers and firewalls. - Options for private and public peerings. TICAP compliant.	- Manage spokes. - Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process.
Azure government landing zone	- N-Wave provides hub and spoke topology. - N-Wave manages the hub consisting of load balancers and firewalls. - Options for private and public peerings. TICAP compliant.	- Manage spokes. - Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process.
AWS landing zone	- TBD – Service in development.	
Google Cloud landing zone	- TBD – Service in development.	
1G VPN (Any Cloud service provider)	- Options for private and public peerings. TICAP compliant.	- Define a program representative as Point of Contact (POC) for this service. - Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process.
Broker connectivity service 2-10G	- Options for private and public peerings. TICAP compliant.	- Define a program representative as POC for this service.

Service Type	N-Wave Role	Customer Role
(Azure, AWS, Google, Azure-AWS Gov, Oracle)		- Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process.

Network Operations		
Service Type	**N-Wave Role**	**Customer Role**
Tier-1 service desk	- 24x7x365 response.	- Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process.
Tier 2-3 engineering	- See above per provided service.	- Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process.

Security Controls		
Service Type	**N-Wave Role**	**Customer Role**
Transport services (WAN/TICAP)	- N-Wave will provide common controls for network availability. - N-Wave will provide NOAA's Cyber Security Center with required logs, access to tools and other methods for initial triage of cyber incidents deemed sourced from the customer.	- Cyber incidents localized to FISMA users will be assigned to FISMA Information System Security Officer's via the NOAA Incident Response Reporting Application system.
Networking services wireless, VPN)	- N-Wave will provide common controls defined in the wireless service SLA. - N-Wave will provide NCSC with required logs, access to tools and other methods for initial triage of cyber incidents deemed sourced from wireless users.	- Cyber incidents localized to FISMA users will be assigned to FISMA Information System Security Officer's via the NOAA Incident Response Reporting Application system.

III. _Service Level Agreement_

Service levels are derived from historical data collected across various elements ranging from circuits and hardware to maintenance and engineering.

- SLA = Service Level Actual **-** based on historical data collection.
- SLO = Service Level Objective - target objective. This transitions to SLAs after a year of historical data is collected.

Service Element	SLA or SLO	Service Response*
Enterprise Transport Services		
N-Wave backbone	SLA= 99.999%	Tier 1-3 24x7x365
TICAP services**	SLA= 99.999%	Tier 1-3 24x7x365
Dual core connected site (includes Cloud transport)	SLA= 99.99%	Tier 1-3 24x7x365
Single core connected site	SLA= 99%	Tier 1-3 24x7x365
Enterprise Cloud transport VPN/broker	SLO= 99.99%	Tier 1-3 24x7x365
Enterprise Network Services		
Managed LAN core routing/ backbone	SLA = 99.99%	Tier 1-3 24x7x365
Managed LAN aggregation/access switching***	SLA= 99.9%	Tier 1, 24x7x365, Tier 2-3. 8x5xNBD
Enterprise Remote Access VPN (ERAV)***	SLA= 99.9%	Tier 1, 24x7x365, Tier 2-3. 8x5xNBD
Wireless***	SLA= 99.9%	Tier 1, 24x7x365, Tier 2-3. 8x5xNBD
Enterprise Cloud Services		
Landing zones all	SLO=99.9%	Tier 1-3 24x7x365
Refer to Appendix A - N-Wave NOC Response Time Agreement and Target Level of Service ***TICAP availability will be derived from a combination of network infrastructure resiliency coupled with TIC stack security component availability and stability* ****8x5xNBD = Support during regular business hours M-F with support beginning the next business day for after hours or weekends. (Critical escalations will follow the defined procedure in Appendix A: N-Wave NOC Response Time Agreement and Target Level of Service)*		

Engineering Services

N-Wave is committed to providing innovative, customer service driven engineering to support all transport capabilities and customer requirements through:

- Network assessments (WAN/LAN)
- Wireless network assessments
- Network design and strategy consulting
- Network deployment
- Special projects

Network Operations

N-Wave is committed to providing 24x7x365, highly available, world-class network operations with an emphasis on professional and customer service driven interaction delivered across Tier-1, 2 and 3 levels of engineering service, advanced monitoring, measurement, visualization and analysis tool sets. Network operations is provided to all N-Wave customers who utilize transport, network and cloud services; however, the following services can be leveraged to customize individual Line Office or program needs:

- NOC Service Desk (Tier-1)
- Tier-2 engineering support
- Tier-3 engineering support
- Custom tool development and systems support
- Advanced network measurement and visualization service
- Common Operating Picture Environment (COPE) dashboard
- Customer Grafana dashboards

Value-Added Services

Through direct customer engagement, requirements gathering, and active monitoring, N-Wave continually seeks options to enhance deployed-in-place services, improve technology and capability of the current N-Wave network infrastructure. N-Wave is also looking to the future with the design and engineering of the next generation of N-Wave infrastructure. At all levels, N-Wave collaborates and partners with NOAA, the research & education network community, commercial businesses and other federal agencies who are dedicated to exploring and implementing new and advanced networking technologies. The N-Wave program embodies a culture of networking and all N-Wave customers benefit from the program's involvement in:

Performance capacity planning	Dedicated program support
Diverse teams with strong SR&E collaboration and robust advanced tools	Recurring customer project & planning calls
Direct customer requirement gathering sessions	Test beds and proof of concepts
Technology exchanges/community workshops	Stakeholders/science engagement meetings

N-Wave NOC Response Time Agreement and Target Level of Service

The N-Wave NOC is a contractual agreement and partnership between N-Wave and the Global Network Operations Center (GlobalNOC) at Indiana University.

I. **Expected Service Desk Response Time – 15 Minutes**
    N-Wave NOC Service Desk is staffed 24 hours a day, seven days a week, all year long (24x7x365) and responds immediately to all incidents reported to the N-Wave NOC or when alarms are noticed on monitoring systems. Service Desk technicians will begin immediate problem assessment and analysis to identify the severity of the issue to include the following:

    ● Initial Problem Assessment
        ○ Collect customer contact information
        ○ Collect circuit, network device, customer/network impact information, service(s) affected information
        ○ Check monitoring tools
        ○ Reconcile scheduled maintenances
        ○ Collect traceroute, ping, router information, ect.
    ● Create and assign trouble ticket to engineering
    ● Contact is assigned round-robin style through either the on-call engineer or Network Planning Team (NPT) engineer

    NOTE: Since critical issues require faster response times for notifying engineers, some of the information above may be added to the ticket after initial ticket assignment.

II. **Expected N-Wave NOC Engineer Response Times**
    Below are the priority and severity impact level guidelines for how soon after a ticket has been created and assigned to an engineer that investigation must begin. All tickets are worked based on criticality, and ongoing major incidents may affect actual response times.

N-Wave NOC Support - Customer Impact Guidelines (PRIORITY)	
Customer Impact is a subjective scale of measure used to quantify the current impact of a problem or maintenance on the customer's operations, performance, and usability. Set in conjunction with the customer, it may change as the ticket progresses and is used for ticket escalation. Customer Impact seeks to answer, "How high of a priority is the problem/maintenance to the customer?"	
	Impact Level (Priority) - Investigation (Response Time)
● A problem or issue for which the customer needs immediate, undivided attention from NOC staff until resolved. ● The customer is expected to be available immediately to commit full-time resources until the situation is resolved. ● The NOC uses this by default when the network is monitored to have an outage of a non-redundant core network element.	**Critical (1) - 10 minutes**
● A problem or issue for which the customer needs resolution within one business day.	**High (2) - 1 hour**

● The customer is expected to commit resources to resolve the situation between the hours of 1300 and 0100 UTC (1200 and 0000 UTC when Daylight Saving Time is in effect). ● The NOC uses this by default when the network is monitored to have an outage of a redundant core network element.	
● A problem or issue for which the customer does not need immediate resolution, but needs NOC attention within three business days. ● The customer is expected to be available to provide information or assistance when available during normal business hours. ● The NOC uses this by default when a customer connection or session is monitored to have a problem or outage. This is also used by default for maintenance which is both NOC initiated and customer impacting.	**Moderate (3) - 1 day**
● No impact to the customer's operations, performance and usability. ● Non-urgent customer service requests. ● Routine installation/provisioning tickets, non-customer impacting maintenance and customer initiated maintenance.	**Low (4) - 3 days**
N-Wave NOC Support - Network Impact Guidelines (SEVERITY)	
Network Impact is an objective scale of measure used internally to quantify the highest level of impact to the network that occurred throughout the duration of a problem or maintenance. Network Impact seeks to answer, "How severe is the problem/maintenance to the network?"	
	Impact Level (Severity) - Investigation (Response Time)
● The network, a portion of the network, or a key network resource fails, causing an outage of service. ● The network, a portion of the network, or a key network resource, is severely degraded rendering the network nearly unusable.	**Critical (1) - 10 minutes**
● The network, a portion of the network, or a key network resource, fails or is severely degraded, but service has not been affected due to redundant resources. ● The network, a portion of the network, or a key network resource, is experiencing mild-to-moderate degradation, and service is affected. ● Security requests and incidents.	**High (2) - 1 hour**
● Network problems or maintenances of limited scope that pose no risk to the network as a whole. ● Direct connectivity to a single entity (peer, connector, lambda) has been lost.	**Moderate (3) - 1 day**
● No network impact	**Low (4) - 3 days**