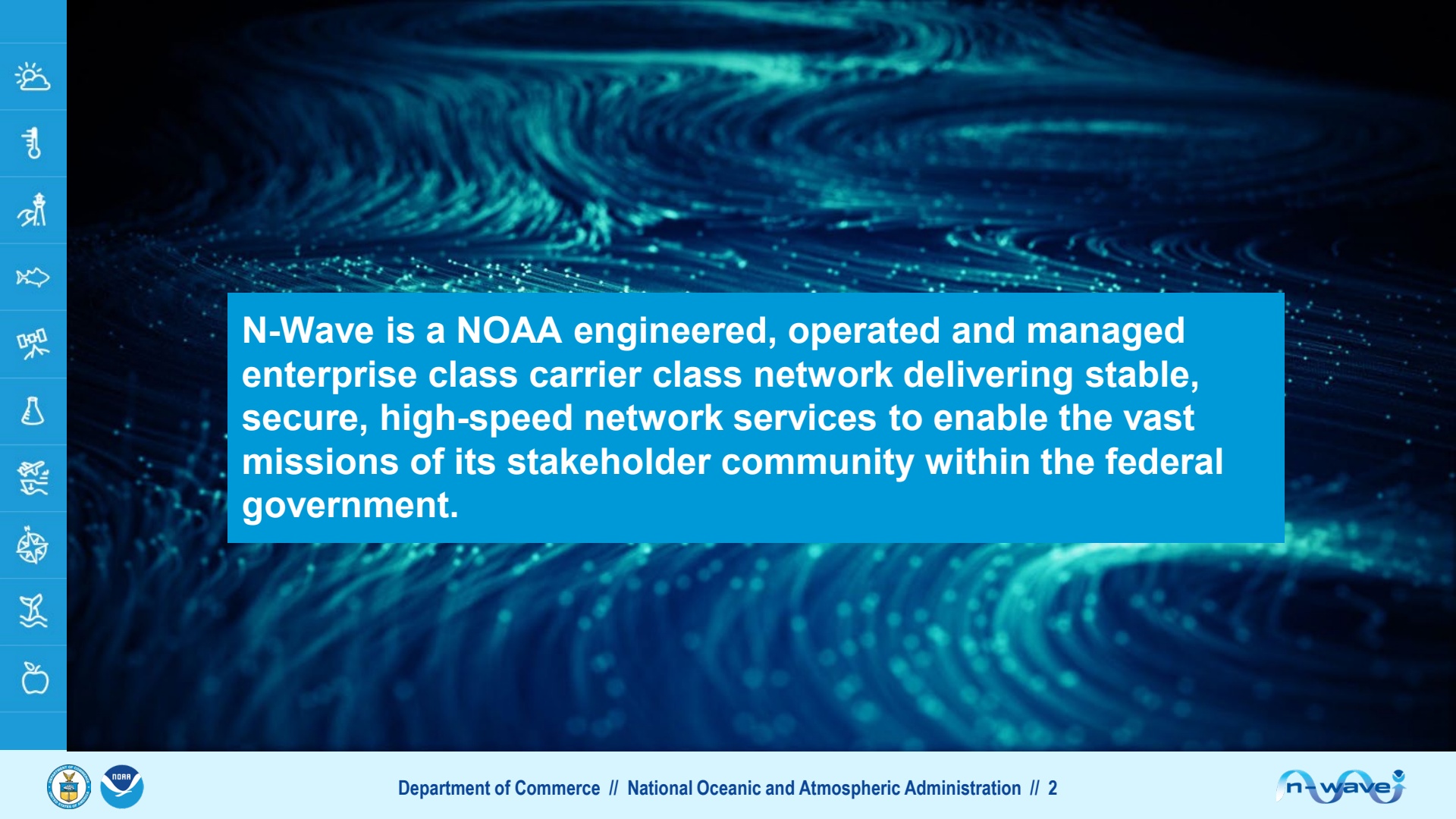


Mission, Mandates and Partnerships



Adam Nemethy, N-Wave Deputy Director, OCIO/NOAA
October 3, 2023





N-Wave is a NOAA engineered, operated and managed enterprise class carrier class network delivering stable, secure, high-speed network services to enable the vast missions of its stakeholder community within the federal government.

Key Drivers

- NOAA-operated and managed national infrastructure, ensuring capacity, security and data delivery assurance
- Solid partnerships within the Science, Research and Education community
- Trusted Internet Connection (TIC) services (X-Wave)
- Scalable cloud solutions
- Robust catalog of enterprise managed services
- Advanced network operations
- High value asset, authorized high FISMA system, full network service provider

Bandwidth

Data Delivery Assurance

Security

Cost

N-Wave Origins

Origins

Growth

Future

2009 – Under ARRA, \$170 million directed to climate modeling, \$10 million of which to fund HPC facilities interconnections

2010 – N-Wave backbone deployed, meeting ARRA goals and setting cost-effective foundation for NOAA-wide use

2011 – R&D customer connectivity established for HPC facilities at Boulder, Oak Ridge, Fairmont, Princeton

2011-14 – N-Wave expanded to serve NOAA HPC; National Environmental Satellite, Data, and Information Service (NESDIS); National Ocean Service (NOS); National Weather Service (NWS); Oceanic and Atmospheric Research (OAR)



N-Wave Growth and Expansion

Origins

Growth

Future

2015 – N-Wave moved under the Office of the CIO to execute NOAA’s strategic plan for network transport and optimization; transitioned from research to enterprise network

2017 – N-Wave Network Operations Center (NOC) and NOAA NOC in Silver Spring, Maryland, consolidated to form a single N-Wave NOC

2018 – N-Wave became network provider for Trusted Internet Connections across all of NOAA; all NOAA external traffic now routed through N-Wave

N-Wave Growth and Expansion

Origins

Growth

Future

2015-19 – N-Wave expanded its service catalog to deliver Enterprise Wireless, Remote Access VPN, Managed LAN, Cloud Transport

2019 – N-Wave backbone upgraded to 100 Gbps, DC Metro ring upgraded to 800 Gbps

2019-20 – Connections from McLean and Chicago to NOAA Environmental Security Computing Center (NESCC) in Fairmont upgraded to 100 Gbps

2020 – Department of Commerce Headquarters connects to N-Wave, representing the largest single site on the network and opening possibilities for future department-wide network optimizations

2022 - N-Wave backbone upgraded to 400 Gbps

N-Wave Growth and Expansion

Origins

Growth

Future

Present – 2023

Continue to grow the N-Wave service portfolio

Extend services to support NOAA line offices

Extend services to other DOC bureaus and federal agencies

Refine and optimize internal processes and workflows

Innovate the network to meet customer needs (e.g., network virtualization, separate optical paths for research traffic)



Enterprise Transport



- National Fiber Optic Backbone
- Multi-Protocol Label Switching
- Optical Transport
- TICAP
- Cloud Transport
- 24x7 Network Operations & Security

Enterprise Services



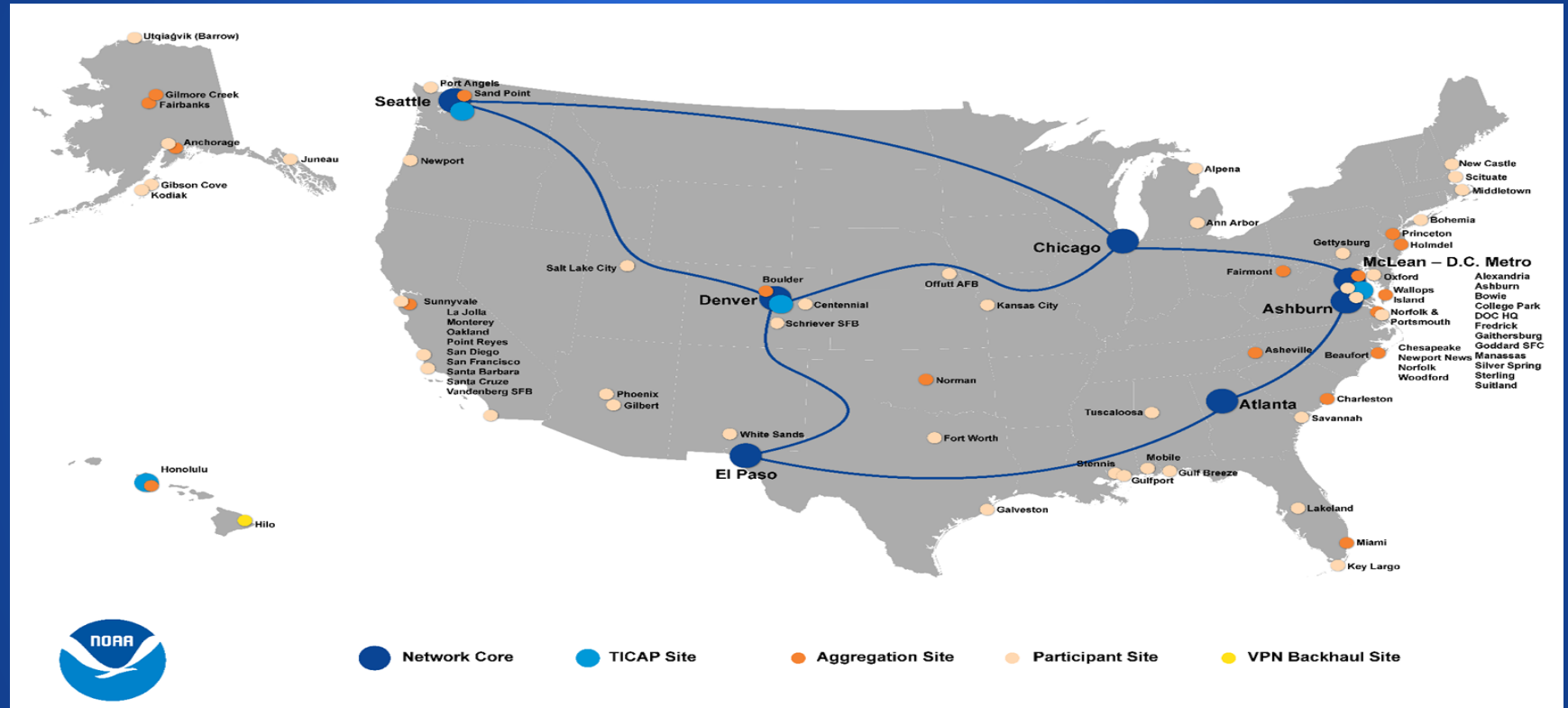
- Enterprise Wireless
- Enterprise Remote Access VPN (ERAV)
- Managed Local Area Networks (LAN)
- Cable Plant Management
- 24x7 Network Operations (per SLA)
- Managed Firewall

Value Add

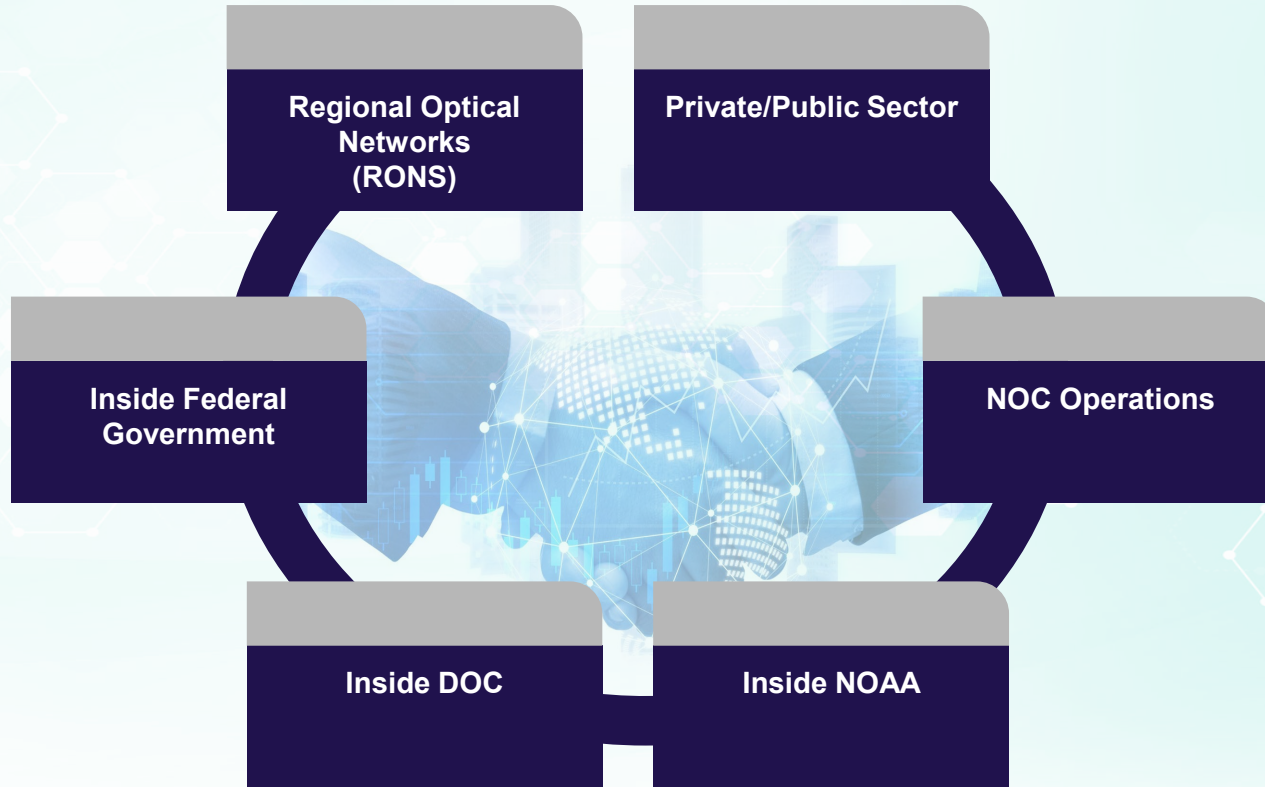


- Engineering Assessments
- Architecture, Design and Consulting
- Technology Exchanges and Stakeholder Engagement
- Monitoring, Measurement and Visualization
- 24x7 Advanced Network Operations & Security

N-Wave Backbone



Partnerships



Advanced Network Operations

Provided in partnership with
GlobalNOC at Indiana University

- 24x7 support
- Tier I, II and III engineering
- Advanced monitoring, measurement and analysis
- Primary, secondary and tertiary ops sites



Photo credit: GlobalNOC at Indiana University

Regional Networks

Regional optical networks or RONS, are consortium based communities made up of Universities, non-profit corporations, and government agencies that cooperate in an aggregated infrastructure of services in order to share advanced high speed Wide Area Networking (WAN) services, access to the Commodity Internet, and access to the Internet2.

All work toward common goals of supporting and enabling the research and education pursuits of their member institutions

REGIONAL RESEARCH & EDUCATION NETWORKS IN THE UNITED STATES



QUILT MEMBERS & AFFILIATES



Q-v3-8-5-22



Internet2

Internet2 is a community providing a secure high-speed network, cloud solutions, research support, and services tailored for research and education. TheirI2 community includes higher education, research institutions, government entities, corporations and cultural organizations.

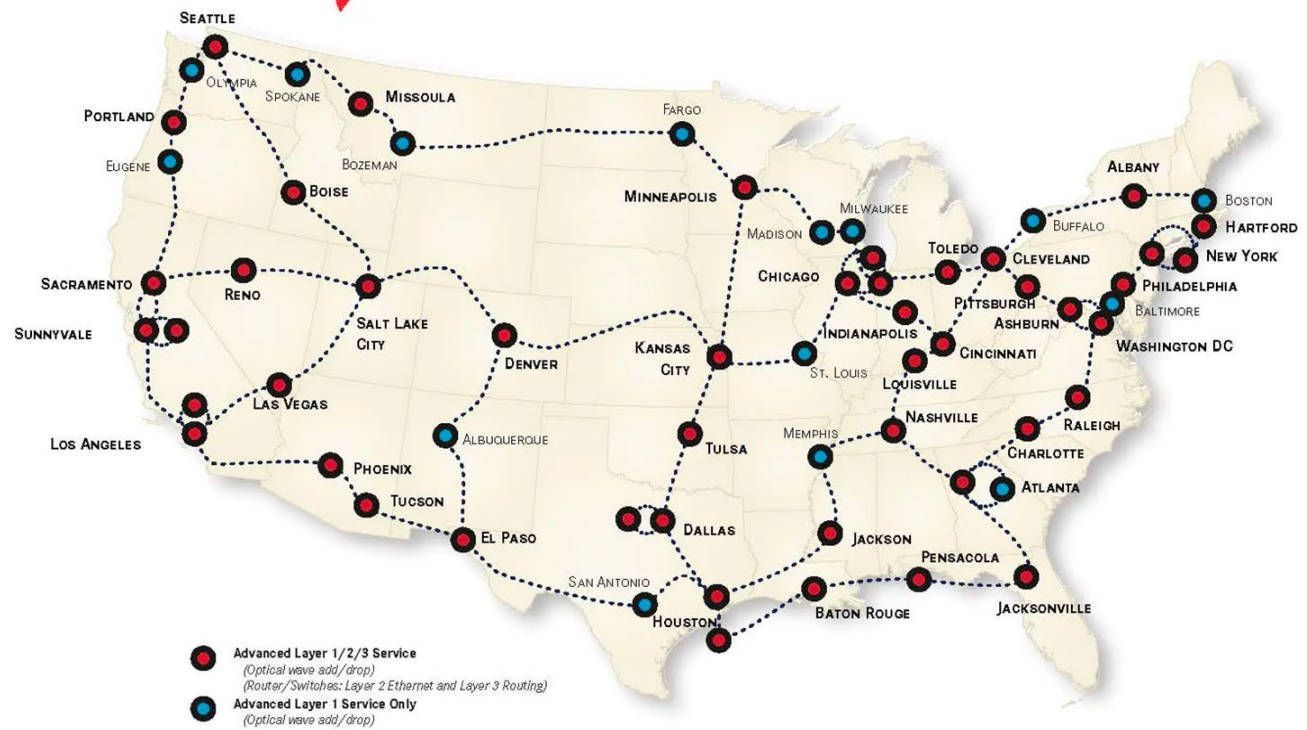
Internet2, formally titled the University Corporation for Advanced Internet Development (UCAID), is a not-for-profit organization governed by a Board of Trustees who represent theirtheir diverse membership.

Internet2 and its community of research and education partners have worked together to solve technology challenges and develop solutions to advance research.



INTERNET2 NETWORK INFRASTRUCTURE TOPOLOGY

OCTOBER 2020



- Advanced Layer 1/2/3 Service**
(Optical wave add/drop)
(Router/Switches: Layer 2 Ethernet and Layer 3 Routing)
- Advanced Layer 1 Service Only**
(Optical wave add/drop)



Other Traditional and Non-Traditional Partners

- **City Fiber Owners**
- **Power Companies**
- **State Department of Transportation**
- **Terrestrial Commercial Providers**
- **Satellite Commercial Providers**



Partnerships

★ Get Involved

- Spread the word
- Combine efforts
 - Information sharing
 - Communities of practice
- Build strong relationships
- Solve requirements and problems together

★ Learn from Others in Government and Beyond

★ Meet with Vendors

- ## ★ Projects and Improvements
- Take Time** – focus on short and long-term needs

Engagement & Outreach Portfolio

Meetings

Alaska Region Technology
Interchange Consortium
(ARTIC) Meetings
(Monthly)

DOC/NOAA IPv6 Transition
Coordination Team Meetings
(Monthly)

Joint Engineering & Technical
Interchange (JETI)
Technical Crosstalk Meetings
(Monthly)

Events

Stakeholders & Science
Engagement Summit
(Annual)

JETI Annual Meeting
(Annual)

JETI Path Workshops
(Ad hoc)

Outreach

N-Wave Newsletter
(Semi-Annual)

Dashboards/Visualization
Resources

N-Wave Website

Robert Sears also serves as the Chair of the Federal IPv6 Task Force, Co-Chair of the Cloud & Infrastructure Community of Practice (C&I CoP) and Government Chair for the ACT-IAC Networks and Telecommunications Community of Interest.

Mandates

- **IPv6 and Zero Trust**

- Discussed in next slides

- **Be Positive**

- Get others motivated, be a voice of change

- **Progress Over Perfection**

- Easy to talk about the 20% that can't comply and use that as a crutch to not do anything. Focus on the easy wins and gain momentum.

- **Plan**

- Plans that are achievable, with milestones that build confidence and drive

- **...Just Get Started**

- **Committees**

- Get involved to share and learn information from peers.

Mandates - *M-22-09 OMB mandate*

- **M-22-09 OMB Mandate**

Subject: “*Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*”

Requires agencies to achieve specific zero trust security goals by the end of Fiscal Year (FY) 2024. These goals are organized using the zero trust maturity model developed by CISA.

www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

Mandates - *M-22-09 OMB mandate*

- 1. Identity:** Agency staff use enterprise-managed identities to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks.
- 2. Devices:** The Federal Government has a complete inventory of every device it operates and authorizes for Government use, and can prevent, detect, and respond to incidents on those devices.
- 3. Networks:** Agencies encrypt all DNS requests and HTTP traffic within their environment, and begin executing a plan to break down their perimeters into isolated environments.
- 4. Applications and Workloads:** Agencies treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome external vulnerability reports.
- 5. Data:** Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies are taking advantage of cloud security services to monitor access to their sensitive data, and have implemented enterprise-wide logging and information sharing.

Mandates - *M-21-07 OMB Mandate*

- **M-21-07 OMB Mandate**

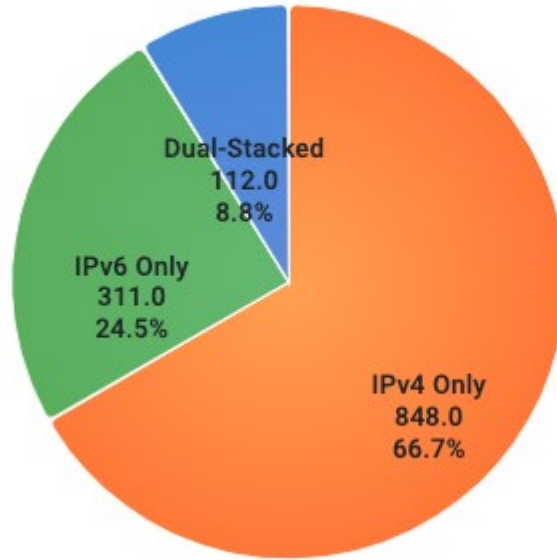
Subject: *“Completing the Transition to Internet Protocol Version 6 (IPv6)”*

- At least 20% of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2023;
- At least 50% of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2024;
- At least 80% of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2025; and
- Identify and justify Federal information systems that cannot be converted to use IPv6 and provide a schedule for replacing or retiring these systems;

www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf

Awareness: N-Wave IPv6 Implementation

All Network Overview



	Value	Percent
IPv4 Only	848.0	66.7%
IPv6 Only	311.0	24.5%
Dual-Stacked	112.0	8.8%

QUESTIONS?

Adam Nemethy, N-Wave Deputy Director

Email: adam.nemethy@noaa.gov

Phone: (252) 777-2398

Credits: Images © / Adobe Stock

