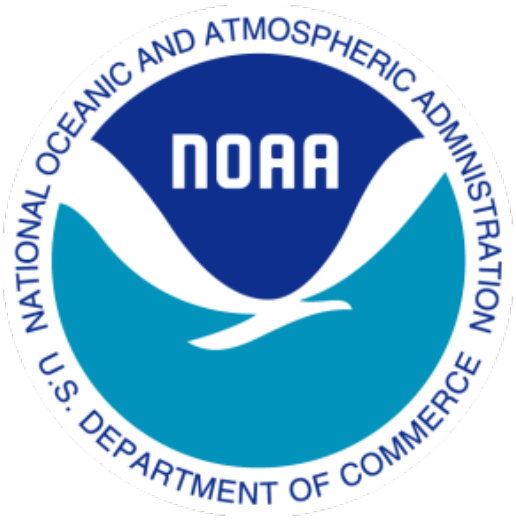
Strategic Plan
Network Optimization & Transport Services
2013-2018



Office of the Chief Information Officer
National Oceanic and Atmospheric Administration
United States Department of Commerce

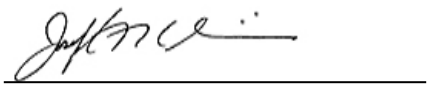
Version 2.0

The NOAA Executive Panel commissioned this Strategic Plan for Network and Transport Services on November 29, 2012. The NOAA CIO Council enacted version 2.0 of the plan on June 11, 2013.

Joseph.F. Klimavicz

NOAA Chief Information Officer

Director, High Performance Computing & Communications



June 14, 2013

Table of Contents

Overview 4

Goal 1: Deliver Enterprise Transport Services 6

- **Action 1: Manage NOAA's Network at the Enterprise Level** 6
- **Action 2: Provide Network Services through the IT Service Portfolio** 6
- **Action 3: Integrate Enterprise-wide Network Operations Centers** 6
- **Action 4: Align Network Acquisitions to Enterprise Standards** 6

Goal 2: Enhance NOAA's Network Security 7

- **Action 1: Route Networks Through TICAPs** 7
- **Action 2: Improve Security Controls** 7
- **Action 3: Build a Trusted NOAA Intranet** 7
- **Action 4: Utilize SOC to Monitor Enterprise Services** 7

Goal 3: Scale Network Capabilities 8

- **Action 1: Strategically Acquire Networking Capabilities** 8
- **Action 2: Improve Network Performance** 8
- **Action 3: Build Network Engineering Core Competencies** 8
- **Action 4: Deploy NOAA Enterprise Services for Federal Agency Accessibility** 8

Goal 4: Optimize Network Services 9

- **Action 1: Identify Opportunities** 9
- **Action 2: Enhance Service Delivery** 9
- **Action 3: Continuously Modernize Enterprise Standards** 9

References 10

Overview

In fulfilling its critical mission of science, service, and stewardship, the National Oceanic and Atmospheric Administration (NOAA) generates tremendous value for the Nation – and the world – by advancing our understanding of, and ability to respond to, changes in the Earth's environment, by improving society's ability to make scientifically informed decisions, and by conserving and managing ocean and coastal resources.[i] NOAA's mission touches the lives of every American and we are proud of our role in protecting life and property and conserving and protecting natural resources.[ii]

NOAA's mission and operations span all 50 states and international sites, and so rely on having a secure, resilient network infrastructure. Our current networks have grown organically in response to the needs of the Agency. Increased frequency and volumes of observational data gathering, tighter coupling of computational activities, decreased timeframes for product delivery and emergency response, and the exponential growth of environmental data – each of these dynamics place more demanding requirements and operational dependencies on NOAA's networks.

This document presents a plan to improve NOAA's network acquisition, management and security processes. In order to achieve the overall objectives four goals have been identified: Deliver Enterprise Transport Services, Enhance NOAA's Network Security, Scale Network Capabilities, and Optimize Network Services.

Each of these goals will deliver specific benefits to NOAA, and taken as a whole, will represent the transformation of our networks into an enterprise-managed, secure, agile, and reliable resource. The following sections provide details, including the specific actions designed to ensure achievement of the goals, as well as discrete metrics that will be used to measure our progress. Our strategic approach is not intended as a single set of initiatives, but as a recurring series of activities that build, in successive iteration, on the improvements made in the previous cycle.

Figure 1: NOAA's Network Optimization Framework

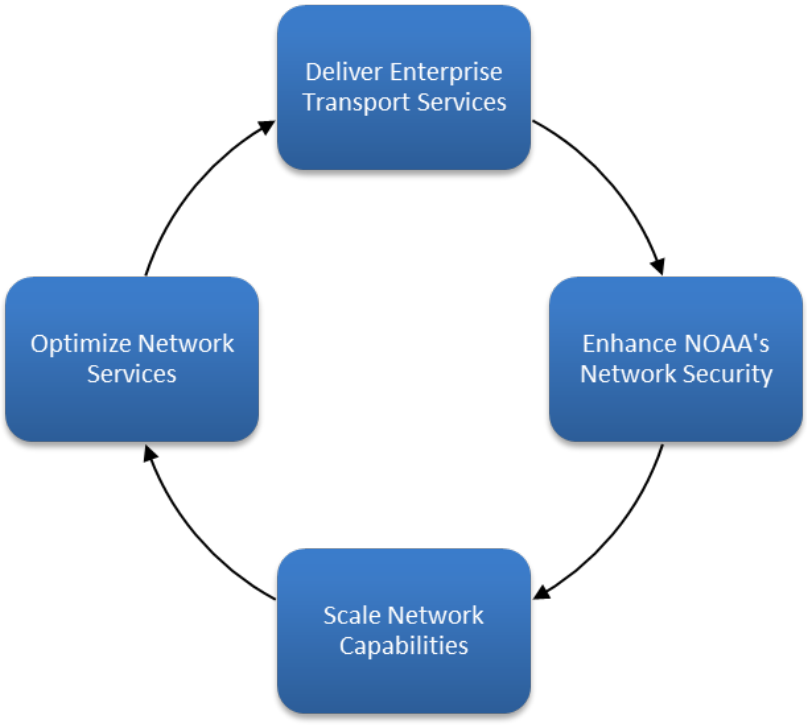


Table 1: NOAA's Enterprise Network Optimization Strategic Goals, Actions, and Metrics

Strategic Goal	*Implementation Actions*	*Metrics (Timeframes)*

Deliver Enterprise Transport Services	- Manage NOAA's network at the enterprise level
	- Provide network services through the IT Service Portfolio
	- Integrate enterprise-wide NOCs
	- Align Network Acquisitions to Enterprise Standards
		- Integrate external NOCs (FY13-14)
		  - Common Configuration Management
		  - Common tools
		- Build NOAA NOC (FY14-17)
		- Institute enterprise-level funding (FY16)
		- Service Portfolio Management (FY13-18)
		- Complete Enterprise Network Services Standards (FY13-18)
		- Implement controls to ensure standards conformance (FY 14-18)
		- Establish Enterprise Network Services Acquisition Vehicles (FY13-14)

Enhance NOAA's Network Security	- Route networks through TICAPs
	- Improve security controls
	- Build a trusted NOAA Intranet
	- Utilize SOC to monitor enterprise services
		- Routing through established TICAPS
		  - 50% by end of FY13
		  - Compliant by end of FY14
		- Common NOC security controls:
		  - Security processes (FY13)
		  - Common tools at network edge (FY14-15)
		  - Common tools for enterprise (FY13-18)
		- Standard templates for ISA&SLA (FY14-18)
		- Establish Base Trusted Intranet (FY16)
		- Establish Multi-zone Trusted Intranet (FY17)
		- SOC monitoring border routers (FY14)
		- SOC monitoring internal core routers (FY15)

Scale Network Capabilities	- Strategically Acquire Networking Capabilities - Improve network performance - Build network engineering core competencies - Deploy NOAA Enterprise Services for Federal Agency Accessibility	- Utilize Strategic Acquisition Vehicles (FY13-18) - Integrate WAN backbones (FY14-18) - Improve networking policy, security, and design engineering core competencies (FY13-18) - Exchange ideas with other Agencies (FY13-18) - Publish Inter-Agency Service Level Agreement for the Enterprise Network Service (FY15)
Optimize Network Services	- Identify opportunities - Enhance service delivery - Continuously modernize enterprise standard	- Modernize network components of the Enterprise Architecture (FY14) - Identify opportunities to reduce cost, improve services or security, or improve performance (FY13-18) - Monitor and integrate industry trends into planning and standards (FY13-18)

Goal 1: Deliver Enterprise Transport Services

Action 1: Manage NOAA's Network at the Enterprise Level

By having an accurate and comprehensive understanding of its environment, agency IT leadership will develop realistic operational network goals, implement plans that adhere to operational and security constraints, and will be able to make informed trade-offs among technical, financial, operational, and security considerations. Managing transport services as an enterprise will allow for quicker response to cyber threats, better monitoring, and improved provisioning of services, while providing improved capabilities and cost-efficiencies.

NOAA's Information Services Strategic Plan, 2013-2018[iii] describes the enterprise information services delivery model NOAA OCIO is moving towards. This model has been designed to achieve a number of benefits, including: cost avoidance; increased efficiencies; economies of scale; improved processes; enhanced enterprise-wide security and networking standards; and improved network services. In order to realize these benefits, the Agency must utilize a common set of services, infrastructure, and funding model.

Focus will initially be on external and non-local network connections. As the network service portfolio matures, enterprise standards for management at the local area network level will be developed and implemented.

Action 2: Provide Network Services through the IT Service Portfolio

To reduce duplicative effort, ensure adherence to policy and standards, and provide greater customer service and support, network services need to be offered through the IT Service Portfolio. As a shared enterprise service itself, the IT Service Portfolio is provided through a standardized infrastructure (consisting of processes and technologies). The result is a familiar, reliable method and set of tools for users across NOAA to identify, select, and configure services they need.

Action 3: Integrate Enterprise-wide Network Operations Centers

Network Operations Centers (NOCs) are responsible for the oversight, provisioning, monitoring, tuning, reporting, and responding to events on the network. In addition, the NOC will provide a single point of contact for connectivity issues. The NOC will be constituted of a primary and backup center. By the end of FY14, NOAA will establish and implement a common Configuration Management (CM) system, acquisition methodology, service catalog, and shared engineering for the network's border services. By the end of FY17, the Integrated NOC will be responsible for all NOAA networks that are "inter-FISMA system" (or between accreditation boundaries).

Action 4: Align Network Acquisitions to Enterprise Standards

IT acquisitions need to enable the adoption of enterprise stands. In order to effectively support the operation and evolution of enterprise network services, NOAA's Enterprise Architecture artifacts will accurately reflect the agency's current infrastructure, standards, and technologies, as well as the planned advancement of each. Standards will be documented in the Enterprise Architecture and enforced, a) operationally, through the Configuration Management process and b) strategically, through the system design and acquisition process, IT Investment Authority, and Authorization and Accreditation cyber security processes.

Goal 2: Enhance NOAA's Network Security

Action 1: Route Networks Through TICAPs

NOAA has initially established four Trusted Internet Connection Access Providers (TICAPs)[iv]. In compliance with OMB mandates, NOAA intends to route its external network connections through a TICAP location by the end of FY14. In order to meet our operational requirements for high network availability, NOAA will implement a solution to allow systems to route through multiple TICAPs.

Action 2: Improve Security Controls

The NOC will provide oversight for the routers on the external border of NOAA's network. Common cyber security controls will be utilized throughout the network infrastructure. NOAA's backbone Wide Area Network (WAN) will maintain controls appropriate for "moderate impact" systems (as categorized by NOAA, following the NIST FIPS 199[v] standard). Business policies, processes, and practices (e.g. centralized logging with the SOC, common authentication methods) will be defined and implemented to ensure that cyber attacks are avoided to the extent feasible. When cyber attacks do occur, the N-CIRT will be engaged to quickly perceive, understand, and contain the situation.

As standard templates for Interconnection Security Agreements (ISA), Interface Control Documents (ICD), and Service Level Agreement (SLA) are created, they will be shared to reduce effort and ensure that expectations are appropriately documented.

Action 3: Build a Trusted NOAA Intranet

Within the intranet, behind the TICAPS, the NOC will provision trusted networks for geographically distributed systems and for sharing information between systems. A multi-level "trust model" will be designed and implemented, allowing systems and data stores to be designed and implemented with standards for identifying, sharing, merging, analyzing, disseminating, and storing information assets.

Action 4: Utilize SOC to Monitor Enterprise Services

NOAA's Security Operations Center (SOC) will deploy its monitoring infrastructure to ensure the cyber-security of the enterprise network and services. The SOC will prescribe counter-measures for ongoing threats. All inter-system border connections will have centralized logging, custom reporting, and active monitoring. NOAA's Homeland Security Program Office will be appropriately updated when there are major events or outages.

Goal 3: Scale Network Capabilities

Action 1: Strategically Acquire Networking Capabilities

NOAA will realize the benefits of economies of scale and cost-reduction by employing strategic sourcing initiatives for acquiring network circuits, equipment, and services. Acquisitions will have oversight to ensure observance of enterprise initiatives, security, and procurement objectives. Maintenance and training opportunities will also be combined to reduce cost. NOAA will continue to take advantage of the cost effective capabilities of the N-Wave Science Network and the pre-negotiated bundled services of Federal telecommunication services (e.g. GSA Networx) to provision high-performance networks.

To ensure competition during the acquisition process and our quick adoption of new technology, NOAA will embrace open standards within its enterprise network. Standards will be defined for a core set of services, and they will be enforced as requirements during the acquisition process.

NOAA is comprised of many small field offices, some medium size offices, and a few large campuses. In addition, NOAA has staff located in partner locations. Solutions will need to be designed and acquired with the flexibility to address the diversity of requirements in a cost-efficient and effective way.

Action 2: Improve Network Performance

Network infrastructure will be consolidated, when appropriate, and new capabilities will be deployed. Monitoring will be incorporated to check usage and identify constraints. Concurrently, NOAA will improve our network performance by deploying advanced, but proven, technologies, configurations, and operating approaches. Also, standardization of network management tools and performance analyzers to continuously "tune" the network, adjust configurations and deploy resources to achieve required performance, consistent with cost and security constraints. The network backbone will be designed, constructed, and deployed to accelerate the adoption of new services, keep up with our explosive rate of data growth, and to aid in the data movement related to NOAA's big data challenge.

NOAA will leverage National Education and Research Networks (NRENs) for both its internal and external network traffic. They will be utilized, when appropriate, to keep up with the data growth, and to route through TICAPs, for international and other external network traffic including satellite, modeling, and radar.

Action 3: Build Network Engineering Core Competencies

Network performance and security is limited by the capability of the engineering staff. Building on the skills of the NOAA Network Committee (NNC), NOAA will foster and ongoing technical dialog to maintain an awareness of industry trends and emerging technologies. This will actively support the OCIO's workforce positioning strategy, which includes ongoing training and development of industry best practices across the networking community.

Action 4: Deploy NOAA Enterprise Services for Federal Agency Accessibility

Enterprise network services will be designed and implemented with the flexibility to be utilized by other Federal Agencies. This will allow other Government Agencies to leverage the improved services and cost advantages derived by NOAA.

Goal 4: Optimize Network Services

Action 1: Identify Opportunities

NOAA will regularly explore cost reducing, performance improving, or security enhancing opportunities. The NNC will be responsible for researching and prioritizing these opportunities, and they will be evaluated against mission requirements, enterprise standards and their ability to support special requirements like NOAA's Primary Mission Essential Functions (PMEF). NOAA-wide programs and teams (e.g., NOAA's Web Operations Committee, IT Security Committee) will collaborate on identifying, analyzing, prioritizing, and implementing network improvements.

Action 2: Enhance Service Delivery

Selected opportunities will be deployed at the enterprise level and documented in the Enterprise Service Catalog. Services will adhere to the Enterprise Architecture and will be authorized through the Configuration Management process. Solution providers will provide monitoring or reporting to either the Security Operations Center or Network Operations Center, as appropriate. Services and infrastructure will be continuously measured, reviewed and evaluated to identify opportunities to restructure or increase efficiencies.

Action 3: Continuously Modernize Enterprise Standards

NOAA will employ open standards wherever possible. Based upon Agency needs and ongoing market research, the Enterprise Architecture will reflect NOAA's current network standards. The NNC will regularly review NOAA's standards and ensure that they are communicated throughout the Line Offices, that they are integrated into operations and planning, and that they are continuously validated and updated.

References

[i] National Oceanic and Atmospheric Administration, *NOAA's Next Generation Strategic Plan, December 2010*, http://www.ppi.noaa.gov/wp-content/uploads/NOAA_NGSP.pdf, page v.

[ii] National Oceanic and Atmospheric Administration, *About NOAA*, http://www.noaa.gov/about-noaa.html

[iii] "Information Services Strategic Plan, 2013-2018", April 2013

[iv] Homeland Security, *Trusted Internet Connections*, http://www.dhs.gov/trusted-internet-connections

[v] FIPS 199-Standards for Security Categorization of Federal Information and Information Systems, February 2004, Computer Security Division, Information Technology Laboratory, National Institute for Standards and Technology, csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf