PMW-205
Naval Enterprise Networks (NEN)

Closing Brief and Summary Remarks

CAPT Michael Abreu
Program Manager
Naval Enterprise Networks (PMW-205)
17 November 2015

DISTRIBUTION STATEMENT A. Approved for public release.
Naval Enterprise Networks

CHARTER
- Provide enterprise IT infrastructure and services to Navy and USMC personnel
  - Navy Marine Corps Intranet (NMCI) via NGEN contract
  - Base Level Information Infrastructure (BLII) for OCONUS Network (ONE-Net)
  - Support to USMC via NGEN

PORTFOLIO
- NGEN -- 34 services, 700,000+ users, +2,500 sites for NMCI management and ops
- OCONUS Enterprise Network (ONE-Net) -- 14 major sites, 30,000+ users
- Global Piers Connectivity -- 18 CONUS and 8 OCONUS sites

PRIORITIES
- Support the operations and defense of the network
- Transition ONE-Net fully into the NEN Operating Model
- Optimize the people, processes, tools and technology to effectively deliver the Navy’s networks in partnership with mission partners and fleet users
- Enhance existing capability while planning the future network architecture

Full Life Cycle Responsibility for CONUS and OCONUS network services

DISTRIBUTION STATEMENT A. Approved for public release.
Program organization intended to allow effective management of all areas of network service provision to meet a global Navy need

* TRMP = Technology Refresh and Modernization Program

DISTRIBUTION STATEMENT A. Approved for public release.
The Evolution of NMCI
NMCI matured over a 15 year journey with an end goal of providing the DON with secure, efficient, and affordable IT capabilities to DON users.

History of NMCI

Security

Regional capabilities for government C2 of networks.

Local network security standards.

CO/CO – transition to enterprise network security.

NGEN: Secure, Integrated, Agile

Increased focus on enterprise cyber security.

GO/CO - achieved full government C2 and increased network situational awareness.

NGEN Competition

Improving network security through multiple efforts and aligning to JIE/JRSS.

Optimizing the business model to balance speed, security, capability, cost-effectiveness, and availability at scale and meet fleet requirements.

Delivered enterprise services to include EUHW, Cell phones, pagers, Enterprise Applications, hosting, etc.

Improved enterprise services: Tablets, Blackberry, WIFI, operating systems, Tiered Storage, virtualization, and refreshed PCs.

Evolved enterprise services such as HVD, Win 7, Office 2010, DoD Visitor, Enterprise GAL.

Enabled competition & transition flexibility by purchasing IF/IP.

Future transition flexibility increased with service model structure.

Modernizing: MPLS and QoS, JRSS, storage upgrades, cloud planning, BYOD planning, iPhones, Androids, UC, 10G network.

Hundreds of networks and contracts of various lengths.
A Global Navy Network

**NNE END STATE VISION**

**NMCI**
- CONUS Network
  - 300,000+ seats
- GO/CO Model
- Contractor - HP

**ONE-Net**
- OCONUS Network
  - 30,000+ seats
- GO/CO & GRC/CO Model
- Contractor - CSC

**NNE**
- Enterprise Network
  - 427,000+ seats
- GO/CO Model
- Contractor - Multiple

Efficiencies of an Integrated Enterprise Network

**People:** Standardized roles and responsibilities within an aligned organizational structure

**Governance:** Unified governance approach with enterprise-wide governance bodies

**Process:** Standardized process framework with clearly defined government touch points and aligned SOPs

**Service:** Integrated service providers with enterprise service portfolios, uniform user experience

**Tools & Technology:** Integrated and documented tools and technology communicating across enterprise

**Performance Management:** Unified measurement of performance with standardized metrics focused on CSI

End State

Current State

DISTRIBUTION STATEMENT A. Approved for public release.
“Our military will remain ready to deter and defeat threats to the homeland, including against missile, cyber, and terrorist attacks, while mitigating the effects of potential attacks and natural disasters.”

“We live in a time of growing cyber threats to U.S. interests. State and non-state actors threaten disruptive and destructive attacks against the United States and conduct cyber-enabled theft of intellectual property to undercut the United States’ technological and military advantage.

“Cyberspace will be operationalized with capabilities that span the electromagnetic spectrum – providing superior awareness and control when and where we need it.”

“Through the intelligent use of cyberspace, Navy warfighters will bring unique capabilities to the fight in order to achieve superior operational outcomes at the time and place of our choosing.”

DISTRIBUTION STATEMENT A. Approved for public release.
The Challenge

Deliver critical capabilities... ...to hundreds of thousands of end users... ...globally across multiple networks... ...involving many stakeholders... ...while complying with dynamic requirements...

...in a budget-constrained environment on a network that is continuously under attack.

DISTRIBUTION STATEMENT A. Approved for public release.
• The Navy’s NIPR and SIPR networks are critical to enabling Information Dominance and conducting our everyday mission

• The future of information technology must be forecasted as well as possible to help outline the most effective way to deliver new capability

• That added capability must be balanced with the need for security, cost effectiveness, high availability, scalability, and speed (both of the network and of new technology).

Thank you for your participation, your feedback, and your help in continuing to meet the Navy’s network needs across the globe
QUESTIONS?