Naval Enterprise Networks
Naval Enterprise Networks 101
NMCI and BLII

Andrew Tash
Chief Engineer, PMW 205
17 November 2015

DISTRIBUTION STATEMENT A. Approved for Public Release.
Agenda

- Network Environment and Challenge
- Global Ashore End State
- NMCI and BLII Current Architectures
- Cybersecurity Challenges and Improvements
- Capability Evolution
- Summary
Naval Enterprise Networks (NEN)

- PMW 205 Acquisition Portfolio
  - **NMCI** (network) via **NGEN** (contract)
    - 34 services, +700,000 users, +2,500 sites
  - **BLII** (network) via **ONE-Net** (contract) – IT services, 33,000 users, 14 major sites
  - **Global Piers** – 18 CONUS / 8 OCONUS sites
- Must continue to mature the business model and drive program and network stability

| Full Life Cycle Responsibilities | IT Service Strategy → Design → Transition → Support of Operations → Continuous Service Improvement |

DISTRIBUTION STATEMENT A. Approved for Public Release.
We Deliver Capabilities

Goal

Cost Effective, Innovative, Scalable, Secure, Agile Solutions

DISTRIBUTION STATEMENT A. Approved for Public Release.
We Embrace the Challenge

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

Cyber Security
Network
Enterprise
End User

...in a budget-constrained environment on networks that are continuously under attack.

DISTRIBUTION STATEMENT A. Approved for Public Release.
Global Ashore End State

NNE END STATE VISION

NMCI
CONUS Network
400,000+ seats
GO/CO Model
Contractor – HP

ONE-Net
OCONUS Network
27,000+ seats
GO/CO & GO/GO Models
Contractor - CSC

FCC/NWNC/NCDOC
NCTAMS

NAPLES TNOSC
7,700+ seats
EU UNDCs

BAHRAIN TNOSC
4,700+ seats
ME UNDCs

YOKOSUKA TNOSC
7,700+ seats
JL UNDCs

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

Critical Success Factor

Cost Effective, Innovative, Scalable, Secure, Agile –
global alignment of C2 and service delivery

DISTRIBUTION STATEMENT A. Approved for Public Release.
NMCI Current Architecture

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B1</td>
<td>Boundary 1</td>
</tr>
<tr>
<td>DSTB</td>
<td>Deployable Site Transport Boundary</td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operations Center</td>
</tr>
<tr>
<td>RAS</td>
<td>Remote Access Service</td>
</tr>
<tr>
<td>TB</td>
<td>Transport Boundary</td>
</tr>
<tr>
<td>VSS</td>
<td>Very Small Site</td>
</tr>
</tbody>
</table>

DISTRIBUTION STATEMENT A. Approved for Public Release.
NMCI Current Architecture
Hosting Solutions & Legacy Networks

DISTRIBUTION STATEMENT A. Approved for Public Release.
Cybersecurity Challenges

Enterprise only as secure as its weakest link

#1 Enterprise Boundary Protection

#2 All improvements not available to enterprise

#3 JIE: JRSS / IPN IA requirements
Continuous Cybersecurity Improvements

• Executing over 30 cybersecurity projects and planning out-year requirements

• Focus
  – Server & end user client hardening
  – Accelerated incident response
  – Network administration
  – Boundary & DMZ upgrades
  – Reduce attack surface and limit lateral movement

Critical Success Factor | Must ensure security enhancements at system level are able to be leveraged by the enterprise
Near-term

Strategic
- Innovation Cell
- Cloud
- JRSS
- Navy Network Consolidation
- Data Center Consolidation
- NGEN Recompete
- ONE-Net Transition

Capability Evolution

Goal
Faster Follower of Industry

DISTRIBUTION STATEMENT A. Approved for Public Release.
DoD cloud services guidance is evolving
- Better direction for commercial cloud providers, system/application owners
- Review and approval processes – BCAs, Tech assessments, procurement requests
- Sensitive Data via Cloud Access Point(s) (CAP)
- Security Requirements Guide (SRG) for Computer Network Defense (CND)

Full cloud computing depends on providing security as required and a sound business case

Cloud service requirement in NGEN re-compete

Critical Success Factor

Government and industry engagement
Capability Evolution: Unified Capabilities

Operational View When Connected to DISN

Operational View When Disconnected from DISN

Only signaling & non-intrabase media is routed to CDC

DISTRIBUTION STATEMENT A. Approved for Public Release.
Capability Evolution: Mobility Service Model

Goal: Cost-effective, secure, standardized, sustainable access to shared data across the NMCI enterprise to enhance Navy productivity.
Summary

• Network and Delivery of Services Today
  – Technology refresh of network infrastructure ongoing
  – Expanding mobile device capability
  – Well over 100 improvement projects in various stages of work

• Network and Delivery of Services Tomorrow
  – Consolidation Initiatives in place (NNC & DCC)
  – Significant Cybersecurity focus
  – BLII alignment with NMCI
  – Looking to industry for ideas to improve IT services
  – NGEN contract re-compete
  – Pursuing JIE initiatives

Forward Thinking  Future informed by the past, not constrained by it