SENEDIA Defense Innovation Days

Innovation from the Cybersecurity Perspective

VADM Nancy A. Norton
Director, DISA
Commander, JFHQ-DODIN
Two Organizations - Synchronized Mission Focus

MISSION
Builds, Operates, Secures
DISA Component of Global Enterprise
Combat Support Agency

MISSION
Command and Control
Synchronizes Protection
Enables Power Projection Across DODIN

DOD CIO Direct Report

Director DISA / CDR JFHQ

OPCON

USCC

TRUST IN DISA: MISSION FIRST, PEOPLE ALWAYS!
# Strategic Goals

<table>
<thead>
<tr>
<th>Operate and Defend</th>
<th>Adopt, Buy, and Create Solutions</th>
<th>Enable People &amp; Reform the Agency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Modernize the Infrastructure</td>
<td>2. Optimize for the Enterprise</td>
<td>3. Enable People</td>
</tr>
<tr>
<td>2. Enhance Operations</td>
<td>2. Strengthen Cybersecurity</td>
<td>3. Reform the Agency</td>
</tr>
<tr>
<td>2.3 Drive Innovation</td>
<td>2. Drive Innovation</td>
<td></td>
</tr>
</tbody>
</table>

## Strategic Objectives

1. Modernize the Infrastructure
   - Network Enhancements
   - Legacy Elimination
   - Internet Protocol v6
   - Fourth Estate Network/Data Center Consolidation
   - Spectrum Modernization
   - Joint Information Environment
   - Survivable Infrastructure
   - SATCOM Modernization
   - Software Defined Enterprise

2. Enhance Operations
   - Network Operations
   - Defensive Cyber Operations – Internal Defensive Measures
   - Mission/Quality Assurance & Critical Infrastructure
   - Defense Industrial Base
   - Exercises and Training
   - Contingency Plans
   - Ecosystem
   - Active-Active
   - Airborne Intelligence Surveillance & Reconnaissance
   - Special Access Programs
   - Assessments
   - National Leadership Command

3. Optimize for the Enterprise
   - milCloud 2.0
   - Unified Capabilities
   - C2 Portfolio
   - Mobility Offering
   - IT Tools Reform and Consolidation

4. Strengthen Cybersecurity
   - Cybersecurity Service Provider
   - Artificial Intelligence
   - Machine Learning
   - Identity Credential Access Management/Affirmed Identity
   - Endpoint Security
   - Comply-to-Connect

5. Drive Innovation
   - Development, Security, Operations/Agile Software Development
   - Acquisition Strategies
   - Partnerships Across DoD
   - Mobile/Desktop Convergence
   - Agile Software Development
   - Universal Transport

## Strategic Capabilities

### 1.1 Modernize the Infrastructure

- Network Enhancements
- Legacy Elimination
- Internet Protocol v6
- Fourth Estate Network/Data Center Consolidation
- Spectrum Modernization
- Joint Information Environment
- Survivable Infrastructure
- SATCOM Modernization
- Software Defined Enterprise

### 2.1 Optimize for the Enterprise

- milCloud 2.0
- Unified Capabilities
- C2 Portfolio
- Mobility Offering
- IT Tools Reform and Consolidation

### 2.2 Strengthen Cybersecurity

- Cybersecurity Service Provider
- Artificial Intelligence
- Machine Learning
- Identity Credential Access Management/Affirmed Identity
- Endpoint Security
- Comply-to-Connect

### 2.3 Drive Innovation

- Development, Security, Operations/Agile Software Development
- Acquisition Strategies
- Partnerships Across DoD
- Mobile/Desktop Convergence
- Agile Software Development
- Universal Transport

### 3.1 Enable People

- Trust and Accountability
- Culture and Reputation
- Recruiting
- Hiring
- Training
- Retention
- Cyber Workforce
- Acquisition Workforce
- Equal Opportunity
- Total Force Fitness Framework

### 3.2 Reform the Agency

- DOD IT Reform
- Internal Business Systems and Processes
- Audit Readiness
- Financial Systems
- Testing
- Customer Service
- Provisioning Timelines
- Joint Enterprise License Agreements

## Guiding Principles

- Improve Customer Service - Collaborate to Innovate - Measure What Matters – Take Prudent Risks
DOD Information Network - Defined

- Service, Combatant Command & Special Networks
- Industrial Control Systems
- Coalition & Multi-National Networks
- Tactical Communications Systems
- Leased Telecom Services
- Mobile Devices
- Educational Institutions
- CAC
- Communications Satellites
- Cloud Services
- Agencies & Field Activities Networks
- Programs of Record/Platform IT

Department of Defense Information Network
Global Communications and Enterprise Services

Facilitating Joint Interoperability

Robust, diverse, resilient, and protected communications and computing environment enabling warfighting operations
DODIN – Layered Defense

- 300TB data inbound / day
- 798M cybersecurity events / day
- 38M incoming emails / day
- 80% inbound email malicious, blocked

INTERNET and CLOUD ENVIRONMENT
Dozens of Internet, Strategic Gateways & Cloud Access Points

EMAIL / TELEWORK / MOBILITY
- 15K unclassified, classified, special purpose networks
- 4M DOD computers
- 3.2M users
- 180K mobility devices

TACTICAL EDGE
- Camp/Post/Base/Station
- Organization & Enclave Networks

BIG DATA PLATFORMS
JOINT REGIONAL SECURITY STACK
BREAK & INSPECT

Cross Domain & Coalition Environments

Combatant Command/Services/Agencies & Field Activities

COALITION
Cyber Defense Framework

Countermeasures
- Firewalls,
  Intrusion Detection Ports/Protocols
- White Lists,
  Access Control Lists,
- JRSS, Firewalls,
  Intrusion Detection, Sensors, Proxies
- Firewalls,
  Proxies
- HBSS,
  Data at Rest

Attack Surface
- Perimeter Access
- Internet Access Points
- NIPRNet
- One DoD Backbone
- CC/S/A Networks
- ~30 WANs
- Local Networks
- ~15,000 LANs
- Devices/Info
- ~4M Devices

Threats

~15,000 LANs
~4M Devices
Driving Innovation in Cybersecurity

Adopt, Buy, Create