Cybersecurity Panel

20170404

Moderator: RADM Nancy Norton

Assured C2 – Battlespace Awareness – Integrated Fires
# Integrated Navy Cybersecurity Plan

<table>
<thead>
<tr>
<th>End Goal</th>
<th>Action</th>
<th>Core Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Account for what needs to be protected</td>
<td>• Establish, Maintain Baseline</td>
</tr>
</tbody>
</table>
| Protect | Harden the platform | • Develop, Implement Technical Standards  
|          |        | • Implement CYBERSAFE  
|          |        | • Reduce Attack Surface |
| Detect   | Identify anomalous activity | • Implement Situational Awareness |
| React    | Fight through | • Develop Response Processes  
|          |        | • Segment Network |
| Restore  | Restore normal conditions | • Develop Recovery Processes, Solutions |

| Foundational | Grow workforce | • Conduct Exercises, Training |

**Orchestrating and unifying toward common objectives**

**Assured C2 – Battlespace Awareness – Integrated Fires**
C4I-Space Domain

Mr. Brian Marsh, SPAWAR
Navy is using a holistic systems engineering process to enhance cybersecurity readiness
- RMF is a part of that integrated process
- Using Navy's Technical Authority construct

Cross-Navy SYSCOM team effort to define Navy’s implementation of security controls
- Maximize operational effectiveness
- Minimize Total Ownership Cost

Focus: minimize risk to successfully accomplish missions

RMF is integrated into Navy’s Systems Engineering process
Cyber Requirements:
• Higher level DoD guidance
• National Institute of Standards & Technology (NIST)

Information Technology (IT) / Information Assurance (IA) Technical Authority Board (TAB) provides guidance tailored for Navy-specific implementation.

Navy Cybersecurity Architecture with Afloat, Ashore and Aviation instantiations

Cyber Specifications and Standards guide POR/Project efforts toward common implementation of Security Controls.

These specifications, standards and architecture will be implemented across combat/weapon system, naval control system, business and C4I programs in all of the Navy Systems Commands.
Risk Management Framework
Process Overview

Operations Management

Step 6
MONITOR
Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update Security Plan, SAR, and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

Cybersecurity Engineering

Step 1
CATEGORIZE
System

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2
SELECT
Security Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve Security Plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3
IMPLEMENT
Security Controls

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in Security Plan

Step 4
ASSESS
Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5
AUTHORIZE
System

- Prepare the POA&M
- Submit Security Authorization Package (Security Plan, SAR, and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decisions

Authorizing Official (AO) / Functional Security Controls Assessor (SCA)

Risk Management Framework intended to provide greater insight into cyber risk

Unclassified
Assured C2 – Battlespace Awareness – Integrated Fires
Ashore Domain

Mr. Rob Baker, NAVFAC
**Navy Ashore Domain Cybersecurity Plan**

<table>
<thead>
<tr>
<th>End Goal</th>
<th>Action</th>
<th>Core Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Account for what needs to be protected</td>
<td>• Industrial Control Systems &amp; Utilities</td>
</tr>
<tr>
<td>Protect</td>
<td>Harden the platform</td>
<td>• Implement Technical Standards</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Apply Cybersecurity Unified Facilities Criteria</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Defense in Depth Enclaves</td>
</tr>
<tr>
<td>Detect</td>
<td>Identify anomalous activity</td>
<td>• Enhanced Continuous Monitoring</td>
</tr>
<tr>
<td>React</td>
<td>Fight through</td>
<td>• Incident Response and Resiliency</td>
</tr>
<tr>
<td>Restore</td>
<td>Restore normal conditions</td>
<td>• Implement CM and TTPs</td>
</tr>
<tr>
<td>Foundational</td>
<td>Grow a trained/certified workforce</td>
<td></td>
</tr>
</tbody>
</table>

Hiring for specialized positions (industrial control systems and cybersecurity) is increasingly challenging due to competitive environment for these high demand skillsets and long turnaround following OPM processes.
Navy Ashore Domain Strategy Picture

Layers of Cybersecurity

DoD Information Network

Enterprise Level

Gateway Device

Outer Boundary

(Isolated Zone)

Control Point (CP)

Platform Network Enclave

Internal Threats

Inner Boundary

CP

Access Control Systems

CP

ELMR

CP

NERMS IDS/Alarms

CP

Advanced Metering

CP

Building Control Systems

CP

Utility Control Systems

Control/Platform/Info. Systems

Base/Facility Level

Region Level

Unclassified

Assured C2 – Battlespace Awareness – Integrated Fires
Afloat Domain

Mr. Scott St. Pierre, NAVSEA
## NAVSEA Cybersecurity Strategy
**Afloat and Ashore**

<table>
<thead>
<tr>
<th>End Goal</th>
<th>Action</th>
<th>Core NAVSEA Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Account for what needs to be protected</td>
<td>• Establish, maintain system/network baselines</td>
</tr>
<tr>
<td>Protect</td>
<td>Harden the platform</td>
<td>• Establish and secure enclaves</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Implement integrated, complementary cybersecurity solutions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Reduce attack surface</td>
</tr>
<tr>
<td>Detect</td>
<td>Identify anomalous activity</td>
<td>• Implement situational awareness</td>
</tr>
<tr>
<td>React</td>
<td>Fight through</td>
<td>• Cyber Planning and Response Center</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Develop response processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Maneuver the network</td>
</tr>
<tr>
<td>Restore</td>
<td>Restore normal conditions</td>
<td>• Develop recovery processes</td>
</tr>
<tr>
<td>Foundational</td>
<td>Train personnel</td>
<td>• Conduct exercises, training</td>
</tr>
</tbody>
</table>

### Holistic approach: Working across a broad front

**Assured C2 – Battlespace Awareness – Integrated Fires**
Cyber Resilience Strategy

Defense-in-Depth Protection Levels

Level 0
- DISN (Ship-to-Ship Comms)
- NOC
- Pier side Comms

Level 1
- External Comms

Level 2
- C2ISR / IO Control Point
- C4I Control Point

Level 3
- Combat Control Point
- Navigation Control Point
- HM&E Control Point
- Aviation Control Point

Level 4
- L16 Control Point
- CEC Control Point
- Radar / EW Control Point

GAINES
- SCI
- UNCLASS
- SEC REL
- GENSER

External Interfaces

Cyber Situation Awareness

Control Points

Critical Functions
- Enclave Boundary Protection
- Incident Isolation
- Recovery Operations
- Agile Technology Insertion

Leverage common engineering across multiple ship classes

Assured C2 – Battlespace Awareness – Integrated Fires
Aloft Domain

Mr. Bill Williford, MARCORSYSCOM
Cybersecurity Requirements

- What do our aircraft really need?
  - Keep the bad out
    - Defense-in-depth
      - No single measure is good enough
    - Know when and where there are problems
  - Keep what we have working
    - Day to day reliability
    - Operate through an attack
      - “Play hurt”
    - Post event restoration
- Keep the Fleet operating

- Protect
- Detect
- React
- Restore
NAVAIR CYBERSAFE Process

1: Categorize System
2: Select Security Controls
3: Implement Security Controls / Harden System/
4: Assess Security Controls
5: Authorize System (ATO)
6: Monitor Security Controls

Results

Authorization

CSPD Approval
Objective Risk Criteria

CYBERSAFE Certification

Assessment of cyber risk to safety and mission effectiveness

CYBERSAFE certifications at platform level in alignment with Airworthiness

Unclassified