

Unclassified

# Navy Cybersecurity Division (N2N6F4)



## Navy Cyber Resilience

20160218

Mr. Troy Johnson

*Assured C2 – Battlespace Awareness – Integrated Fires*



# Agenda

- ❑ Impetus for Task Force Cyber Awakening (TFCA)
- ❑ Transition from TFCA to Navy Cybersecurity Division
- ❑ Foundational work
- ❑ Cyber resilience strategy
- ❑ Conclusions

***From cybersecurity to cyber resilience***



# Cyber Awakening Story

- ❑ Disconnected response through stove-piped assessments & initiatives across the enterprise:
  - Operation ROLLING TIDE (ORT)
  - N81 Cyber Defense Studies
  - Cyber Platform Risk Assessment
  
- ❑ Unified response through Task Force Cyber Awakening:
  - NOT 'N2/N6-centric' – “cyber platform” spans the entire Navy
  - Use existing mechanisms where possible
  - Cybersecurity must be a resourcing and organizing principle
  - Accountability and rigor are key
  - POM-17 Cyber Resiliency BAM inclusive of full DOTMLPF

***Cybersecurity is as important as the next missile or platform***

*Assured C2 – Battlespace Awareness – Integrated Fires*



# Transition from TFCA to Navy Cybersecurity

**DCNO Information Dominance**  
**VADM Ted Branch**  
**Director Naval Intelligence**  
*Deputy: Ms. Lynn Wright (DISES)*  
**DON Deputy Chief Information Officer (Navy)**  
*Deputy: Ms. Janice Haith (SES)*  
**\* Director of Cyber**  
*\* Deputy: RADM (sel) Nancy Norton*

**Cyber EXCOM**  
 Co-Chairs: VCNO & ASN (RD&A)

**RMF Authorizing Official Council**  
 Chair: DDCIO (N)

**Advisory Board**  
 Co-Chairs: DASN C4I / Director of Cyber

**Cybersecurity Req. Steering Committee**  
 Chair: DCNO N2N6

**Deputy Director,  
 Navy Cybersecurity  
 (N2N6F)** ★★

**Navy Cybersecurity Division  
 (N2N6F4)** 🍷

**IT/IA Technical Authority Board (TAB)**

**Navy Cybersecurity Deputies**

**Strategy & Compliance  
 (N2N6F41)** 🦅

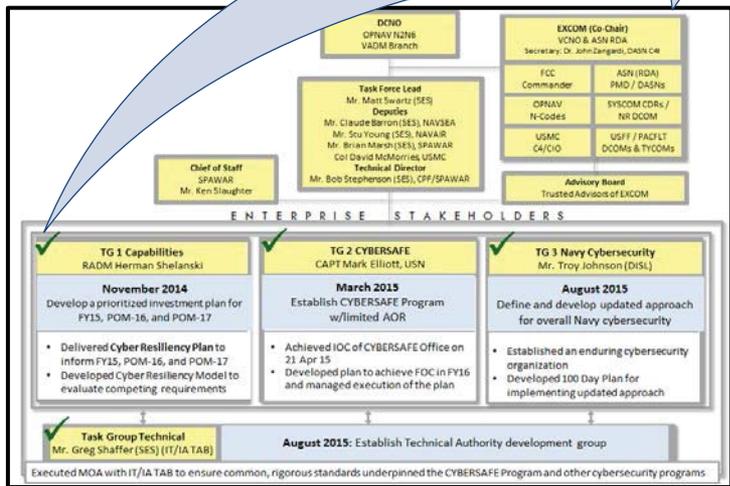
**Requirements & Resource Oversight  
 (N2N6F42)**

**Cybersecurity Safety (CYBERSAFE)  
 (N2N6F43)** 🦅

- ❑ Retained TFCA governance structure, added 2 other governing bodies
- ❑ Augmented TFCA tasks with other functions and tasks
- ❑ Orchestrating Navy-wide cybersecurity efforts
- ❑ Not just conventional IT

**Moving beyond TFCA resourcing, organizing focus**

*Assured C2 – Battlespace Awareness – Integrated Fires*





# Adding Structure to Navy Cybersecurity

## Architecture Framework

- ✓ Initial consensus on Architecture Framework
- ✓ Synchronizes cybersecurity architectural strategies, standards and plans

## Strategy

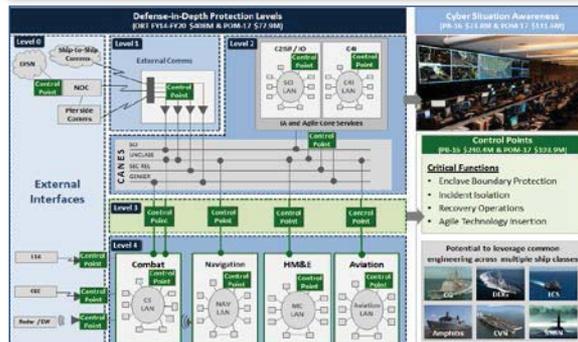
- ✓ Outlined cybersecurity strategy w/ focus on top-level strategic goals
- ✓ Develop operational concepts, cyber resiliency, workforce, organize for optimal effectiveness

## Risk Posture

- ✓ Developing dashboard with FCC, IFOR, SYSCOMs
- ✓ Organized by views – Operating Forces, Echelon II
- ✓ Developing measures for Navy Cyber Resilience

## Requirements

- ✓ Developed collection of draft Key Systems Attributes (KSA) and other systems attributes
- ✓ Developing OPNAV Instruction (w/ KSAs) – will be part of SECNAV Acquisition Manual



## Communications

- ✓ Navy cybersecurity communications campaign in coordination with stakeholders
- ✓ Released NAVADMIN, articles on navy.mil and Navy's Facebook page, videos, infographics

## Standards

- ✓ IT/IA Technical Authority Board (TAB) has 20 of 48 standards signed, or being reviewed
- ✓ 2 CYBERSAFE standards signed
- ✓ 4 of 16 FY16 standards being reviewed

## CYBERSAFE

- ✓ Developed CYBERSAFE Certification Guidance & Test Plan
- ✓ IT/IA TAB developed CYBERSAFE Selection Criteria & Requirements
- ✓ SYSCOMs developed Strategic Roadmap for their programs

## Training

- ✓ Working Group to synchronize training
- ✓ NETC – User
- ✓ Working Group – Leader
- ✓ SYSCOMs – Enhanced User

**Collaboratively executing across orchestrated lines of effort**

*Assured C2 – Battlespace Awareness – Integrated Fires*



# Development of Cyber Resilience Strategy

- ❑ **TFCA Hypothesis:** To achieve robust cybersecurity, we need to:
  - Make cybersecurity a resourcing and organizing principle
  - Address all known deficiencies immediately
- ❑ **Expected Outcome:** A Navy that has the right command and control, accountability and an affordable set of cybersecurity solutions
- ❑ **TFCA/N2N6F4 Assessment**
  - Confirmed that C2 and accountability are key
  - Discovered that:
    - The cost of adding resources for every individual solution is unaffordable
    - Impregnable defense is very costly and complex
    - We should focus on mission prioritization, recovery and fighting through
    - Industry experts agree
- ❑ **Adjustment:** Developed cyber resilience strategy that focuses on cyber resilience for mission assurance

***Cyber resilience is continued operations in a contested cyber environment***



# Cyber Resilience Approach

## NSA's Top 10 IA Mitigation Strategies

Mitigation Strategies	Mitigation Goal Areas			
	Device Integrity	Damage Containment	Defense of Accounts	Secure & Available Transport
Application Whitelisting	■			
Control Administrative Privileges		■	■	
Limit Workstation-to-Workstation Communication		■		■
Use Anti-Virus File Reputation Services	■			
Enable Anti-Exploitation Features	■			
Implement Host Intrusion Prevention System (HIPS) rules	■			
Set a Secure Baseline Configuration	■			
Use Web Domain Name System (DNS) Reputation	■			■
Take Advantage of Software Improvements	■			
Segregate Networks and Functions		■		■

## Industry Recommendations (Controls against Cyber Espionage)

**RECOMMENDED CONTROLS**

Isolating the root cause of an espionage-related breach is a bit of a snipe hunt. Sure, victims make mistakes (prior and otherwise) that are exploited in the process, but the real root issue is a determined, skillful, patient, and well-resourced adversary who will keep poking until he finds (or makes) a hole. With that in mind, let's take a closer look at the holes and other thin spots these adversaries often take advantage of.

First, we'll start with a few blocking and tackling fundamentals that you really ought to be doing regardless of whether or not you're worried about espionage. If you don't do these, all those super-advanced cyberstastic API cryptonite solutions may well completely defend against phishing, such as not relying solely on spam detection and blocklists, but also doing header analysis, pattern matching based on past detected samples, and sandbox analysis of attachments or links included.

For more mature organizations, check out the growing collection of Data Execution Prevention (DEP) and Endpoint Threat Detection and Response (ETDR) solutions. We don't promote specific products in this report, but you'll find some good options in this space by starting your search with some of our they aren't intelligence, but they're certainly useful within intelligence and monitoring operations.

Monitor and filter outbound traffic for suspicious connections and potential exfiltration of data to remote hosts. In order to recognize "abnormal," you'll need to establish a good baseline of what "normal" looks like. Those indicators you collected/bought will come in handy here.

Monitor your DNS connection, among the single best sources of data within your organization. Compare these to your threat intelligence, and mine this data often.

Two-factor authentication will help contain the widespread and unchallenged re-use of user accounts.

We mentioned network segmentation in the basics, but since doing it well is challenging, we'll mention it here again. Don't make a straight shot from patient zero to a full-fledged plague.

Watch for user behavior anomalies stemming from compromised accounts.

**POINT-OF-SALE INTRUSIONS**

**WEBAPP ATTACKS**

**NEED-AND PRIVILEGE/ABUSE**

**PHYSICAL THEFT AND LOSS**

**MISCELLANEOUS BRIBERY**

**OSINT/WARE**

**PAYMENT CARD SKIMMING**

**CYBER-ESPIONAGE**

**DOS ATTACKS**

**EVERYTHING ELSE**

**42** **VERSION/ENTERPRISE SOLUTIONS**

**Break the delivery-exploitation-installation chain**

**Patch ALL THE THINGS!**

**Use and update anti-virus (AV)**

**Train users**

**Segment your network**

**Keep good logs**

**Spot C2 and data exfiltration**

**Stop lateral movement inside the network**

## Cyber Resilience Approach

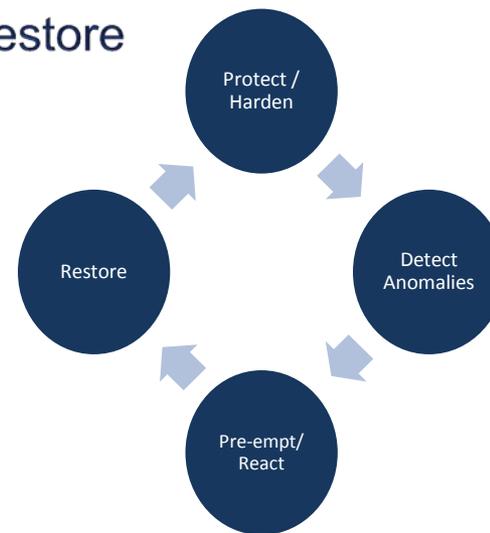
- Control Points:** Control Points will allow us to effectively isolate portions of our networks and prevent adversaries who gain a foothold from moving laterally. Also improve boundary defenses for individual portions of the network and serve as insertion points in the network for emerging technology solutions.
- Cyber Situational Awareness (SA):** Allow us to visualize the activity in the "cyber-field", promote timely assessment of normal vs. abnormal activity, and mitigate possible threats. Cyber SA provides us with the tools to detect and respond to higher level threat actors.
- Designing (vice retroactively Patching-in) Resilience within Systems and Networks:** Generating common sets of standards and protocols to improve our cyber posture by driving down variance, and also designing-in resilience in future system designs.
- Cyber Hygiene:** Use of focused Tactics, Techniques and Procedures (TTPs) and workforce training.
- Cyber Ready Workforce:** Improving manning levels, personnel training and Fleet readiness via readiness reviews, Fleet cyber security efforts, Cybersecurity Workforce continuing education, unit patch/scan compliance and adherence to computer tasking orders (CTO).

**Leveraged stakeholder, community, industry recommendations to develop approach**



# Cyber Resilience for Mission Assurance

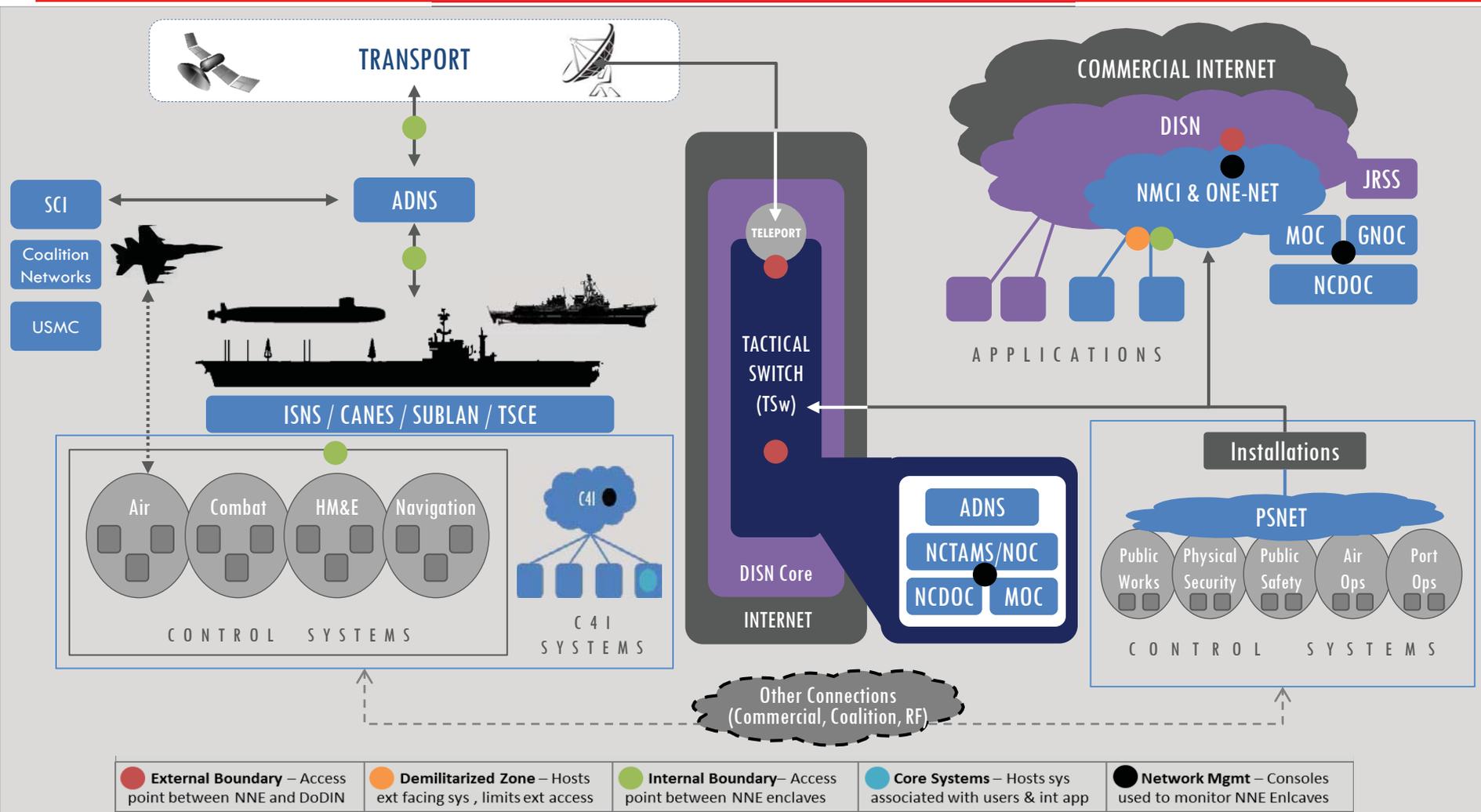
- ❑ Cybersecurity has traditionally focused on the protection of systems and networks.
- ❑ To be cyber resilient – to “fight through” – we must do more than just protect our systems, networks and platforms.
- ❑ Cyber Resilience = Protect + Detect + React + Restore
  - Protect – strengthen assets against threats to prevent most adversary actions
  - Detect – identify and assess adversary actions
  - React – fight through with pre-emptive or reactive measures
  - Restore – restore assets to normal condition and operations



***Cyber resilience is continued operations in a contested cyber environment***



# Navy Cyber Platform



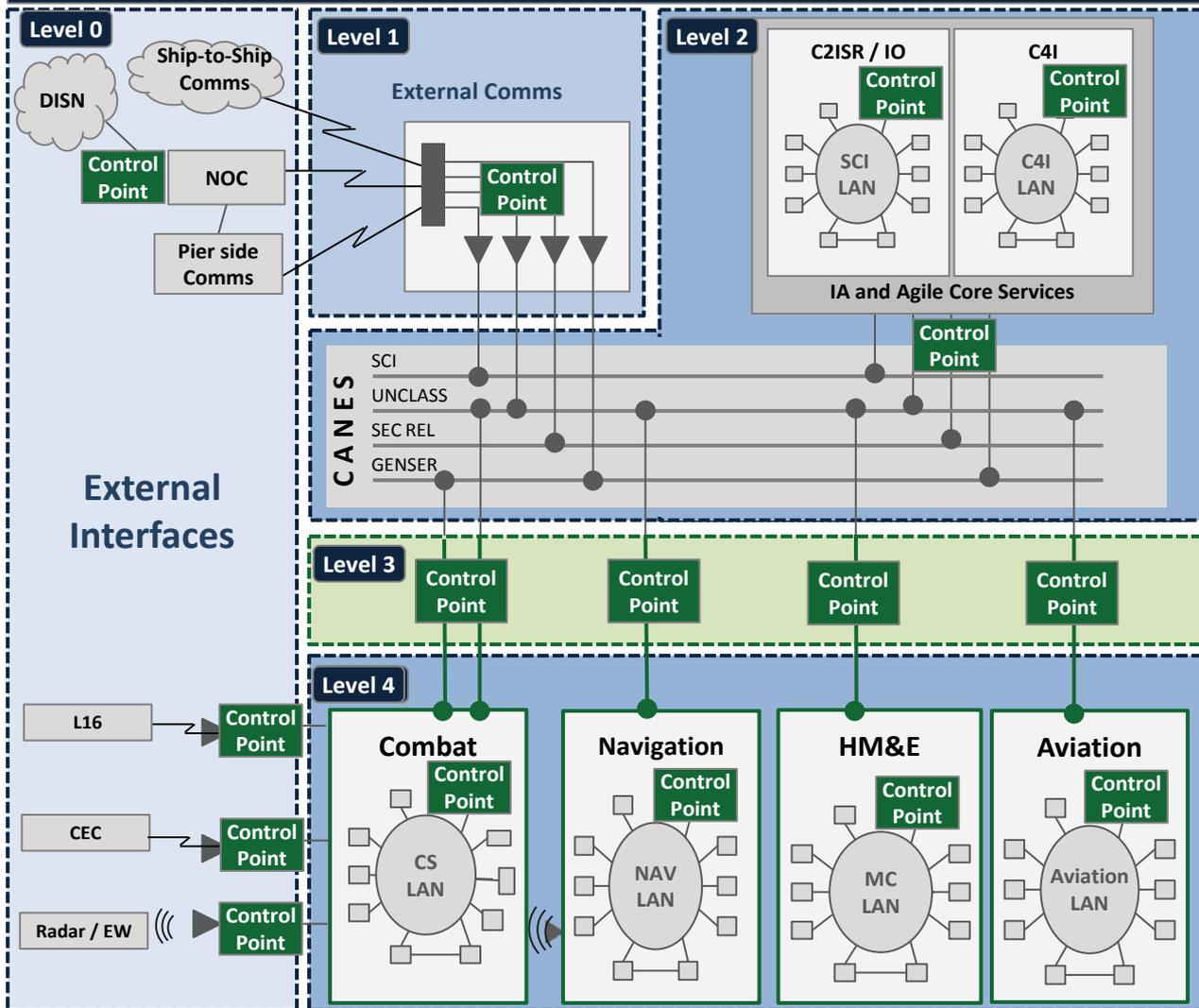
**Cyber resilience efforts need to extend across the enterprise**

*Assured C2 – Battlespace Awareness – Integrated Fires*



# Cyber Resilience Strategy

## Defense-in-Depth Protection Levels



## 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*



# Conclusions

- ❑ Moving beyond protection to operationalize (detect, react, restore)
- ❑ Cyber resilience is guiding investments, actions
- ❑ Navy-wide risk will be measured using the cyber resilience framework

***Cyber resilience is the Navy's strategy for winning in the contested cyber environment***

Unclassified//FOUO

# Backup



*Assured C2 – Battlespace Awareness – Integrated Fires*



# Acronyms

- ❑ **ADNS:** Automated Digital Networking System
- ❑ **BAM:** Baseline Assessment Memorandum
- ❑ **C2:** Command and Control
- ❑ **C4I:** Command, Control, Computer, Communications and Intelligence
- ❑ **CANES:** Consolidated Afloat Networks and Enterprise Services
- ❑ **CRSC:** Cybersecurity Requirements Steering Committee
- ❑ **CSWF:** Cybersecurity Workforce
- ❑ **DFIA:** Defense-in-Depth Functional Implementation Architecture
- ❑ **DISN:** Defense Information System Network
- ❑ **DOTMLPF:** Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities
- ❑ **EXCOM:** Executive Committee
- ❑ **FOC:** Full Operational Capability
- ❑ **G/ATOR:** Ground/Air Task Oriented Radar
- ❑ **GNOC:** Global Network Operations Center
- ❑ **HBSS:** Host Based Security System
- ❑ **HM&E:** Hull, Mechanical, and Electrical
- ❑ **ICS:** Industrial Control Systems
- ❑ **IOC:** Initial Operational Capability
- ❑ **ISEA:** In-Service Engineering Agent
- ❑ **ISNS:** Integrated Shipboard Network System
- ❑ **IT/IA TAB:** Information Technology / Information Assurance Technical Authority Board
- ❑ **JRSS:** Joint Regional Security Stack
- ❑ **KSA:** Key Systems Attribute
- ❑ **MOC:** Maritime Operations Center
- ❑ **NOC:** Network Operations Center
- ❑ **NCD:** Navy Cybersecurity Division
- ❑ **NCDOC:** Navy Cyber Defense Operations Command
- ❑ **NCTAMS:** Naval Computer and Telecommunications Area Master Station
- ❑ **NGEN:** Next Generation Enterprise Network
- ❑ **NMCI:** Navy and Marine Corps Intranet
- ❑ **NOC:** Network Operations Center
- ❑ **ONE-NET:** OCONUS Navy Enterprise Network
- ❑ **ORT:** Operation Rolling Tide
- ❑ **POR:** Program of Record
- ❑ **PSNET:** Public Safety Network
- ❑ **S&T:** Science and Technology
- ❑ **SSDS:** Ship Self-Defense System
- ❑ **TFCA:** Task Force Cyber Awakening
- ❑ **TNOSC:** Theater Network Operations and Security Center
- ❑ **TSCE:** Total Ship Computing Environment
- ❑ **TSw:** Tactical Switching
- ❑ **VRAM:** Vulnerability Remediation Asset Manager