



Navy Cybersecurity: *Moving to Implementation*



Presented to:

National Defense Industrial
Association (NDIA)

Presented by:

Mr. Brian Marsh
Assistant Chief Engineer
(Certification & Mission Assurance)
Space and Naval Warfare Systems
Command (SPAWAR)



Distribution Statement A. Approved for Public Release.
Distribution is unlimited (10 April 2017).

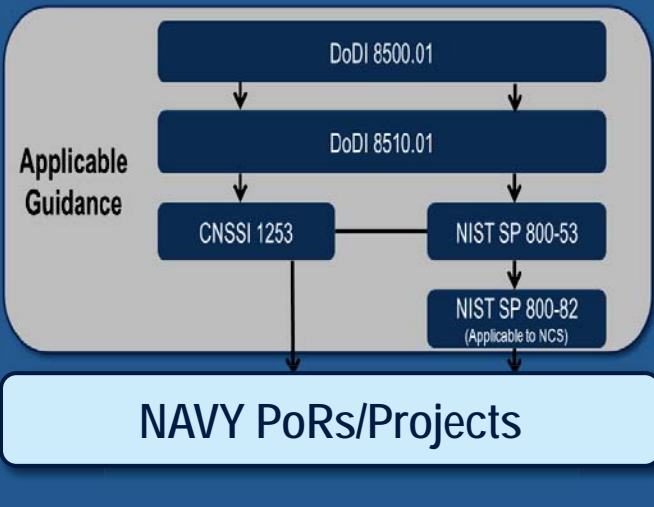


Holistic Implementation Strategy

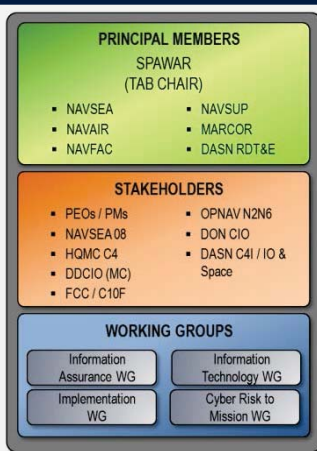
Designing for Cyber

Cyber Requirements:

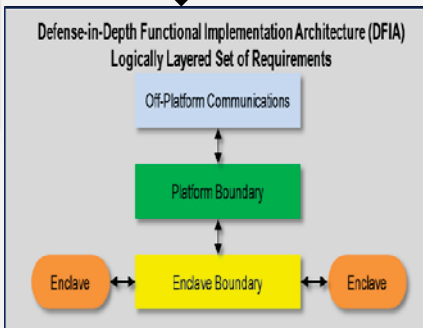
- Higher level DoD guidance
- National Institute of Standards & Technology (NIST)



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



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

FY15	FY16	FY17
Defense-in-Depth Functional Implementation Architecture (DFIA)		
DFIA Afloat	DFIA Aviation	DFIA Space
	DFIA Ashore	DFIA Enterprise
<i>DFIA provides the domain-specific basis for applying the below Technical Standards</i>		
Host Level Protection V2.3*	Operating System	Web Security***
Network Firewall	Cyber Risk Assessment**	Info Sharing - Cross Domain Solution***
IDS / IPS	Trusted Systems and Networks	Email Security***
Continuous Monitoring	CYBERSAFE Grading Criteria	Software Assurance***
Security Information Event Management	CYBERSAFE Grade Requirements	Remote Access***
Vulnerability Scanning	Cyber Situational Awareness	Patch Management***
Boundary Protection	IT Asset Management	BIOS Protection***
	Account Management	Authentication & Authorization / IAM***
	CYBERSAFE Certification Criteria	Event / Incident Management***
	CYBERSAFE Audit Criteria	Information Management - Data Tagging
	Cyber Configuration Management	Public Key Enabling
		Virtualization Security
		Assured Cloud Computing
		Unified Capability
		Maintenance / Support / Calibration Equip
		Wireless Communications
		Wireless Enclave Access Control
		Data Encryption - DT_Link
		Data Encryption - DAR
		Key Management / Exchange
		DNS Security

Legend

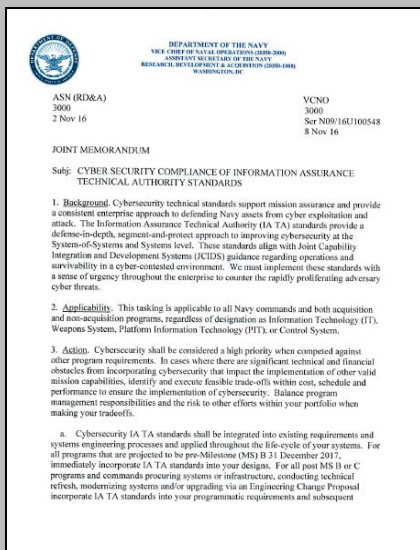
- Informal Review
- Formal Review
- Out for Signature
- Completed



Cybersecurity Requirements

A Key Consideration in All Acquisition Activities

Cybersecurity Compliance of Information Assurance Technical Authority Standards



Signed 8 Nov 2016
VCNO
ASN RDA

▼ Clear direction from Navy Leadership

- *"We must implement these standards with a sense of urgency throughout the enterprise to counter the rapidly proliferating adversary cyber threats."*

▼ Elevated priority of cybersecurity requirements → "a high priority when competed against other program requirements"

- *"...where there are significant technical and financial obstacles from incorporating cybersecurity that impact the implementation of other valid mission capabilities, identify and execute feasible trade-offs within cost, schedule and performance to ensure the implementation of cybersecurity."*

▼ Quarterly progress measurement and reporting reviews via the Cybersecurity EXCOM (VCNO and ASN RDA)



Implementation in the C4I Domain

Defense-in-Depth Functional Implementation Architecture Network Transformation (DFIANT) within C4I

- ▼ DFIANT C4I defines the DFIA-compliant implementation of the cybersecurity standards within the C4I domain
 - Influence CANES Objective Baseline 2 and all applications that connect to CANES
 - Enables the physical separation of critical functions and a virtualized environment that provides greater cyber resiliency
 - SPAWAR working with Naval Information Forces (NAVIFOR) and its newly created Information Warfare Development Center to develop CONOPs and TTPs for DFIANT



Implementation in the Navy Enterprise Domain

Defense-in-Depth Functional Implementation Architecture Network Transformation (DFIANT) for Navy Enterprise

- ▼ DFIANT Enterprise defines the DFIA-compliant implementation of the cybersecurity standards within the Navy's Enterprise domain
 - Defines network technology refresh approach that complies with DFIA
 - Provides a supportable approach to incorporate commercial cloud capabilities
 - Integrates voice, video, and data services
 - Supports Navy planning for the NGEN re-compete

SPAWAR

®

