



# How SPAWAR's Information Technology & Information Assurance Technical Authority Support Navy Cybersecurity Objectives

DON IT Conference // AFCEA West 2015

Presented by:

**RDML John Ailes**

Chief Engineer

SPAWAR 5.0



# Presentation Overview

---

- ➡ ▼ Overview of SPAWAR 5.0
  - ▼ Today's Cyber Environment
  - ▼ Information Technology (IT) & Information Assurance (IA) Technical Authority



# SPAWAR's Role

- ▼ Provide advanced communications and information capabilities to Navy, joint and coalition forces
  
- ▼ More than 9,700 employees deployed globally and near the fleet
  - Military – 591
  - Civilian – 9,170





# Aligning to the CNO's Navigation Plan

## CNO's Navigation Plan 2015 - 2019

A Navigation Plan draws from *Sailing Directions* to describe in greater detail how a ship will use its resources to safely and effectively sail to a new destination. Similarly, CNO's Navigation Plan describes how Navy's budget submission for Fiscal Year (FY) 2015-2019 pursues the vision of CNO's Sailing Directions. It highlights investments in support of DoD missions outlined in our defense strategic guidance (DSG), *Sustaining U.S. Leadership: Priorities for 21st Century Defense*, and *2014 Quadrennial Defense Review (QDR)*, viewed through the lens of my *three tenets*: Warfighting First, Operate Forward, and Be Ready. This Navigation Plan defines the course and speed we will follow to organize, train, and equip our Navy over the next several years.

This fiscal climate compelled the Navy to make tough choices across a wide range of competing priorities. We focused first on building appropriate capability, then delivering it at a capacity we could afford. Our Navy will do its part to "put our fiscal house in order," but we will do so in a responsible way, balancing current readiness with the need to build a highly capable future fleet. Despite likely sequestration in FY 2016, our priority is to operate forward where it matters, when it matters, and be ready to address a wide range of threats and contingencies.

Six programmatic priorities guided our budget submission as we planned for the future: (1) maintain a credible, modern, and survivable sea-based strategic deterrent, (2) sustain forward presence, distributed globally in places that count, (3) preserve the means to win decisively in one multi-phase contingency operation and deny the objectives of another aggressor in a second region, (4) focus on critical afloat and ashore readiness to ensure our Navy is adequately funded and ready, (5) enhance the Navy's asymmetric capabilities in the physical domains as well as in cyberspace and the electromagnetic spectrum, and (6) sustain a relevant industrial base, particularly in shipbuilding. I will take a "fix" on where we stand with these priorities later this year in a "Position Report."

Everything we do must be grounded in this responsibility. Our Navy must be able to achieve access in any domain—where we need it, when we need it—and possess the capability mix of kinetic and non-kinetic weapons to prevail today and be ready to win tomorrow. To maintain our warfighting edge, our FY 2015-2019 budget submission will:

- ◆ Sustain a credible, survivable, and modern sea-based strategic deterrent, including today's force of 14 OHIO-class SSBNs, the

**WARFIGHTING FIRST**

**Warfighting First**  
**Operate Forward**  
**Be Ready**

## Sailing Directions

▼ Included in the six programmatic priorities:

- Critical afloat and ashore readiness
- Capabilities in the physical domains, cyberspace and the electromagnetic spectrum



# SPAWAR 5.0 – What We Do



- ▼ Provide engineering discipline across the acquisition lifecycle
- ▼ Create specifications and standards for Information Technology and Cybersecurity
- ▼ Provide agile and cost-effective engineering rigor with the Fleet in mind
- ▼ Bring a holistic perspective to ensure well-integrated, interoperable and resilient systems across the Navy
- ▼ Secure the network



# Presentation Overview

---

- ▼ Overview of SPAWAR 5.0

-  ▼ Today's Cyber Environment

- ▼ Information Technology (IT) & Information Assurance (IA) Technical Authority



# Current Cyber Environment

Since I took command as SPAWAR's Chief Engineer (Aug 2014), there have been numerous incidents that highlight the severity of the cyber threat:

## ▼ Sony Hack

- Stole data (employees' personal information, e-mails, ~100TB of data/content)
- Implanted malware to erase data from servers

## ▼ Anthem Data Breach

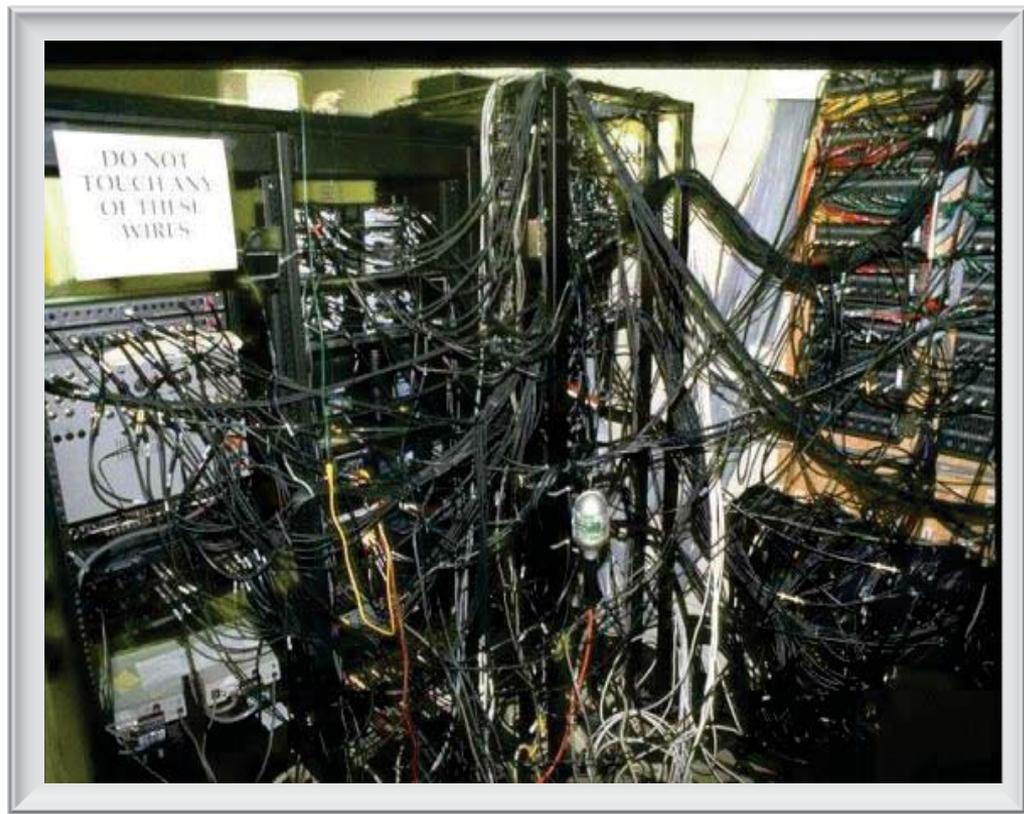
- Infiltrated database to gain access to customers' names, birthdays, Social Security numbers, addresses and employment data (could affect as many as 80M customers)

## ▼ German Steel Mill

- Massive physical damage by manipulating and disrupting control systems
- Access through business network via spear-phishing to inject malware; worked their way into production networks

# A System of Systems Engineering Challenge: Mitigating the Vulnerabilities & Risks

Where We Were



- ▼ A series of stovepipes wired together & not organized or aligned for effective interoperability
  - Little-to-no focus on System-of-Systems or Enterprise-level engineering
  - Integration & Interoperability an afterthought
  
- ▼ Resulting in an IT infrastructure that is:
  - Too large
  - Too old & too hard to upgrade
  - Too varied & expensive
  - Too hard to manage & operate
  - *Too hard to defend*

**We Need a Disciplined Engineering Approach**

# Holistic Enterprise Approach to Cybersecurity

## Cybersecurity Today

*Attackers see a single network with seams*

- ▼ Compilation of systems segregated by enclave
    - C4I, HM&E, Combat, Aviation
  - ▼ Each program implements security controls
  - ▼ ATO covered by ODAA
- 
- ▼ Inefficient, duplicative efforts are not cost effective
- 
- ▼ Introduces seams & vulnerabilities...and larger attack vector
  - ▼ Overly complex design
    - Difficult for sailors to operate and maintain multitude of devices that provide similar functions
    - Perpetuates interoperability issues

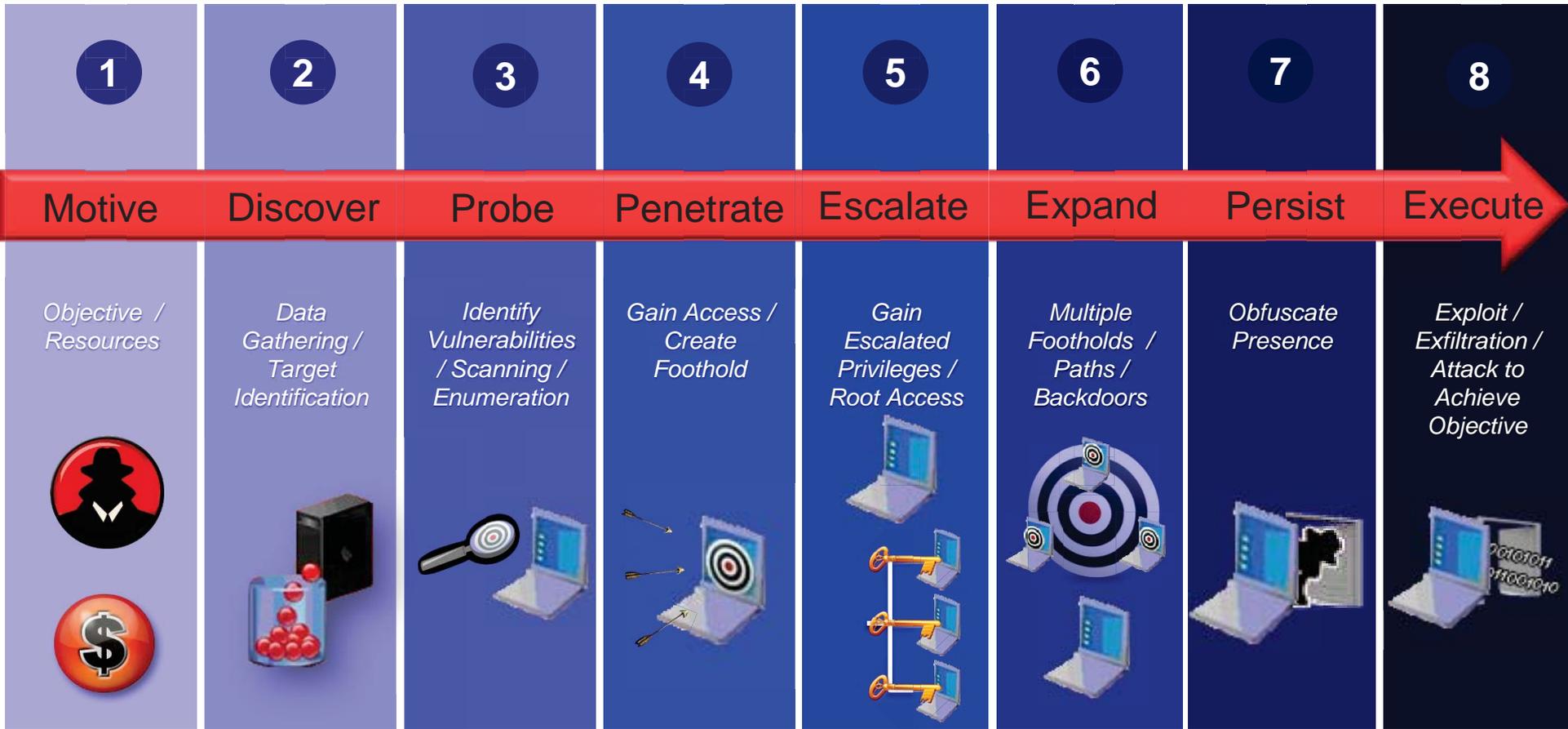


## Vision: A Single Navy Plan for Cyber

- ▼ Holistic enterprise cybersecurity architecture
    - Provides a layered, Defense-in-Depth approach that enables inheritance
  - ▼ Mandatory implementation of standardized security controls
  - ▼ Certified systems meet security requirements
- 
- ▼ Streamlined investment
- 
- ▼ Fewer seams and smaller attack vector
  - ▼ Easier for sailors to operate and manage
  - ▼ Greater interoperability

**Upfront Systems Engineering Informs Investments in Cybersecurity Solutions Across the Navy Enterprise**

# Anatomy of Attack



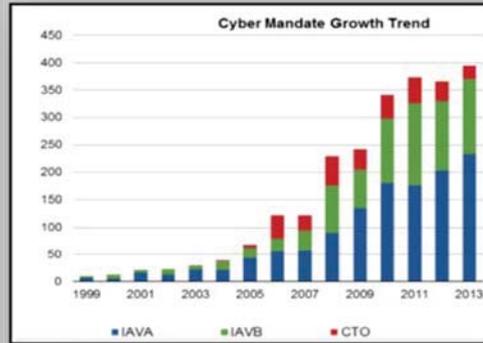
# Growing Operational Risk

$$\text{Risk} = f(\text{Threat, Vulnerability, Consequence})$$

## Dynamic & Growing



## Exploitation Space



## Impact to Mission



Create Bounded Cyber Statement of Risk



# Presentation Overview

---

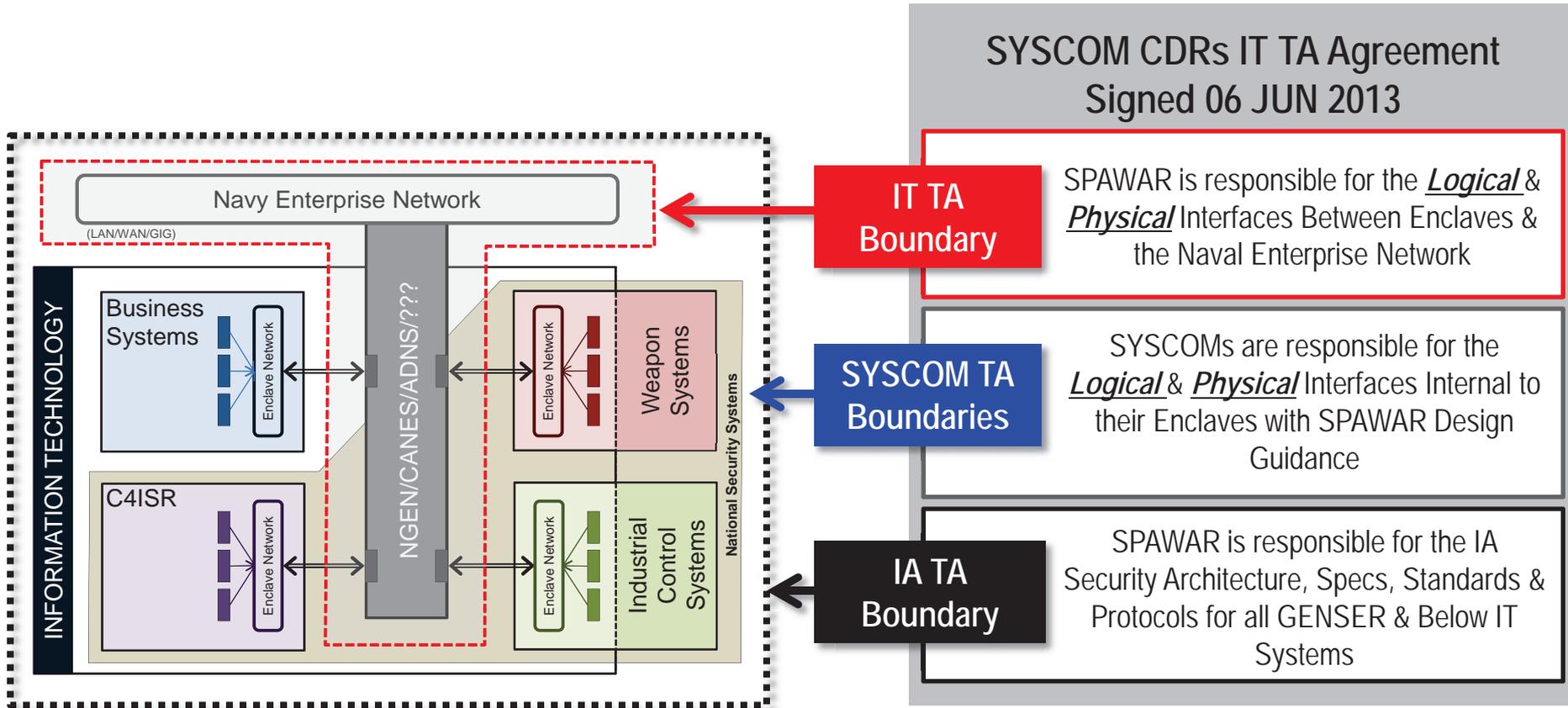
- ▼ Overview of SPAWAR 5.0

- ▼ Today's Cyber Environment

-  ▼ Information Technology (IT) & Information Assurance (IA) Technical Authority



# Technical Authority for Navy Information Technology (IT) & Information Assurance (IA)

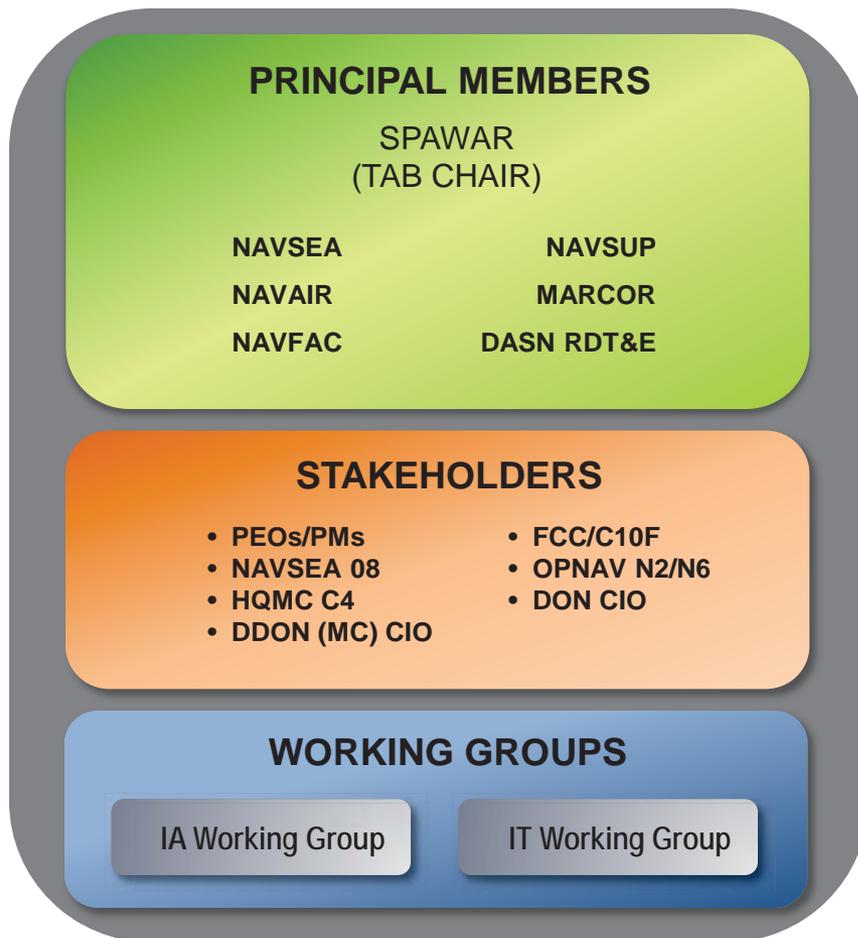


Enterprise Approach to Ensure Our Systems Are Secure & Interoperable



# IT/IA TA Technical Authority Board (TAB)

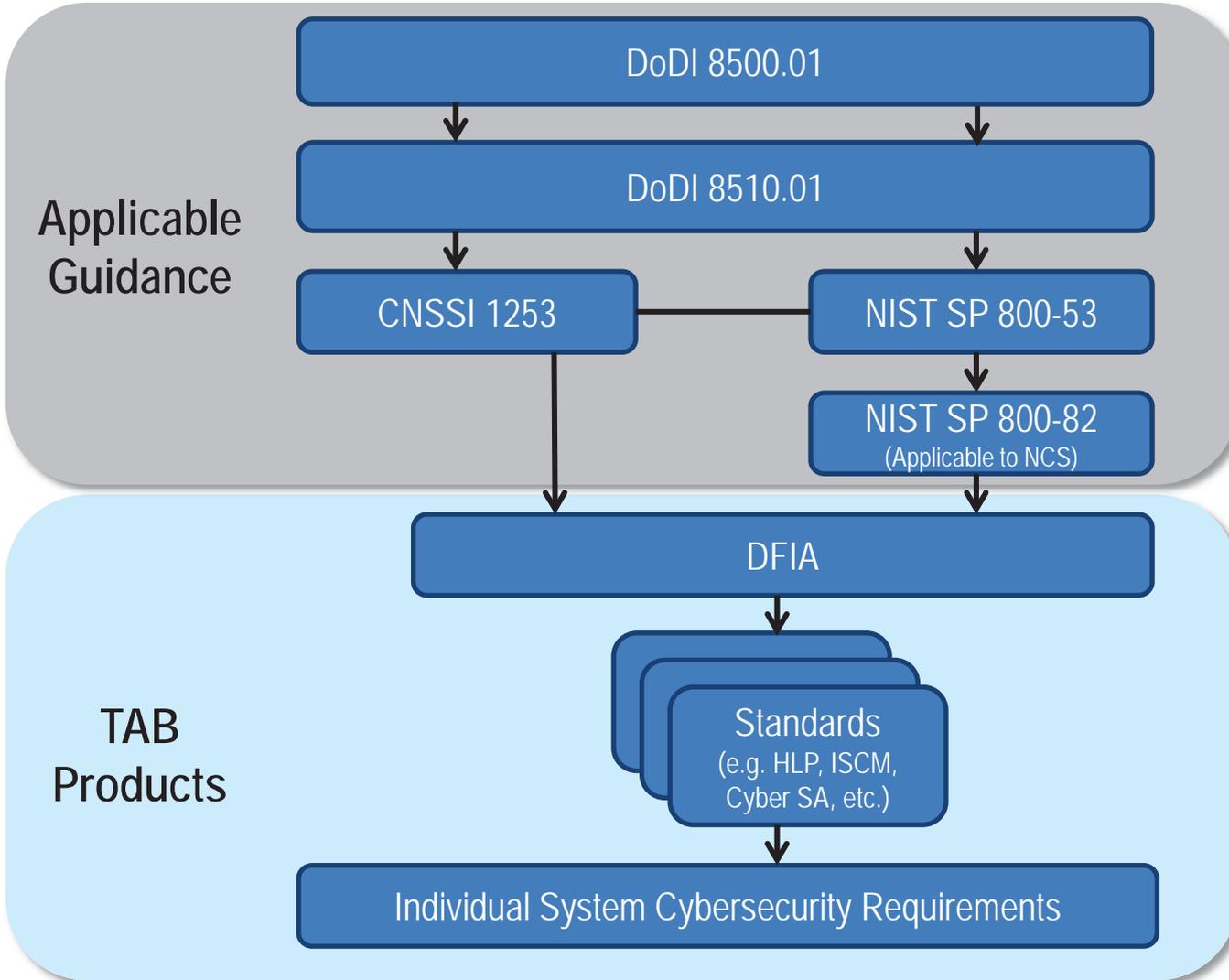
- ▼ Cross-SYSCOM governance board for reviewing, adjudicating & endorsing IT & IA TA products for use throughout the Naval Network Enterprise
- ▼ Charter signed by SYSCOM CHENGs
- ▼ Stakeholders provide key policy & operational perspectives
- ▼ Working Groups collaborate & refine SPAWAR-initiated IT & IA TA products



**TAB is the Cross-SYSCOM Governing Body for Enforcing IT/IA TA Discipline**



# Requirements Flow



## Requirements References:

- [DoDI 8500.01](#): Cybersecurity
- [DoDI 8510.01](#): Risk Management Framework for DoD IT
- [CNSSI 1253](#): Community on National Security Systems (CNSSI) 1253, "Security Categorization & Control Selection for National Security Systems"
- [NIST SP 800-53](#): National Institute of Standards & Technology (NIST) Special Publication (SP) 800-53, "Security & Privacy Controls for Federal Information Systems & Organizations"
- [NIST SP 800-82](#): National Institute of Standards & Technology (NIST) Special Publication (SP) 800-53, "Guide to Industrial Control Systems Security"

**DFIA** – Defense-in-Depth Functional Implementation Architecture  
**HLP** – Host Level Protection  
**ISCM** – Information Systems Continuous Monitoring

\* Flowchart is representative of the DFIA vision to satisfy the required Cybersecurity controls



# Collaboration Across SYSCOMs is Working

## *Some Initial Progress*



### ▼ TAB Endorsed Products to Date:

- Four (4) IA Standards:
  - Host Level Protection, Firewall, Intrusion Detection & Prevention, Defense-in-Depth Functional Implementation Architecture (DFIA) Afloat Overview
- Seven (7) Interface Control Documents (ICDs):
  - Navy Cash to CANES; CDLS to DCGS-N; CDLS to CV-TSC (Remote Interface); CDLS to CV-TSC (MH-60R); BFFT to TVS; BFFT to CANES; BFFT to NAVSSI

### ▼ Still much to be done!

- Nine (9) TAB-Prioritized IA Standards
  - DFIA Ashore, DFIA Airborne, Security Information & Event Management (SIEM); Cyber Situational Awareness; Vulnerability Scanning; Boundary Protection; Asset Management; Supply Chain Risk Management (SCRM)
- 43 remaining ICDs (many of which are in various stages of development/coordination)

### ▼ Quickly move focus to the end state—determine our cybersecurity readiness across the Navy and define our plan to protect, detect and respond to cyber threats



# SPAWAR 5.0: Technical Alignment with Joint Information Environment (JIE)

## JIE

- ❑ Enterprise Data Centers
- ❑ Single Security Architecture
- ❑ Enterprise Services
- ❑ Network Normalization
- ❑ Unified Capabilities
- ❑ Identity and Access Management
- ❑ Enterprise Operations Centers

## Navy Enterprise

- ❑ Navy Enterprise Data Centers (NEDCs)
- ❑ Defense in Depth Functional Implementation Architecture (DFIA)
- ❑ Navy Enterprise Services –PaaS via ACS V3
- ❑ Naval Enterprise Networks (NEN) via NGEN
- ❑ Integrated Voice & Video Over Internet Protocol
- ❑ Identity and Access Management – PKI, CLO, ABAC, RBAC
- ❑ NCDOC – Component support

# Summary



- ▼ Threats continually evolve and so must our policies, tools, products and processes
  - No domain is immune to these threats
- ▼ Technology growth and its impact challenge both government and commercial cybersecurity enterprises
- ▼ Successful IT and IA TA increases our interoperability and security posture
- ▼ Cybersecurity is a team sport

