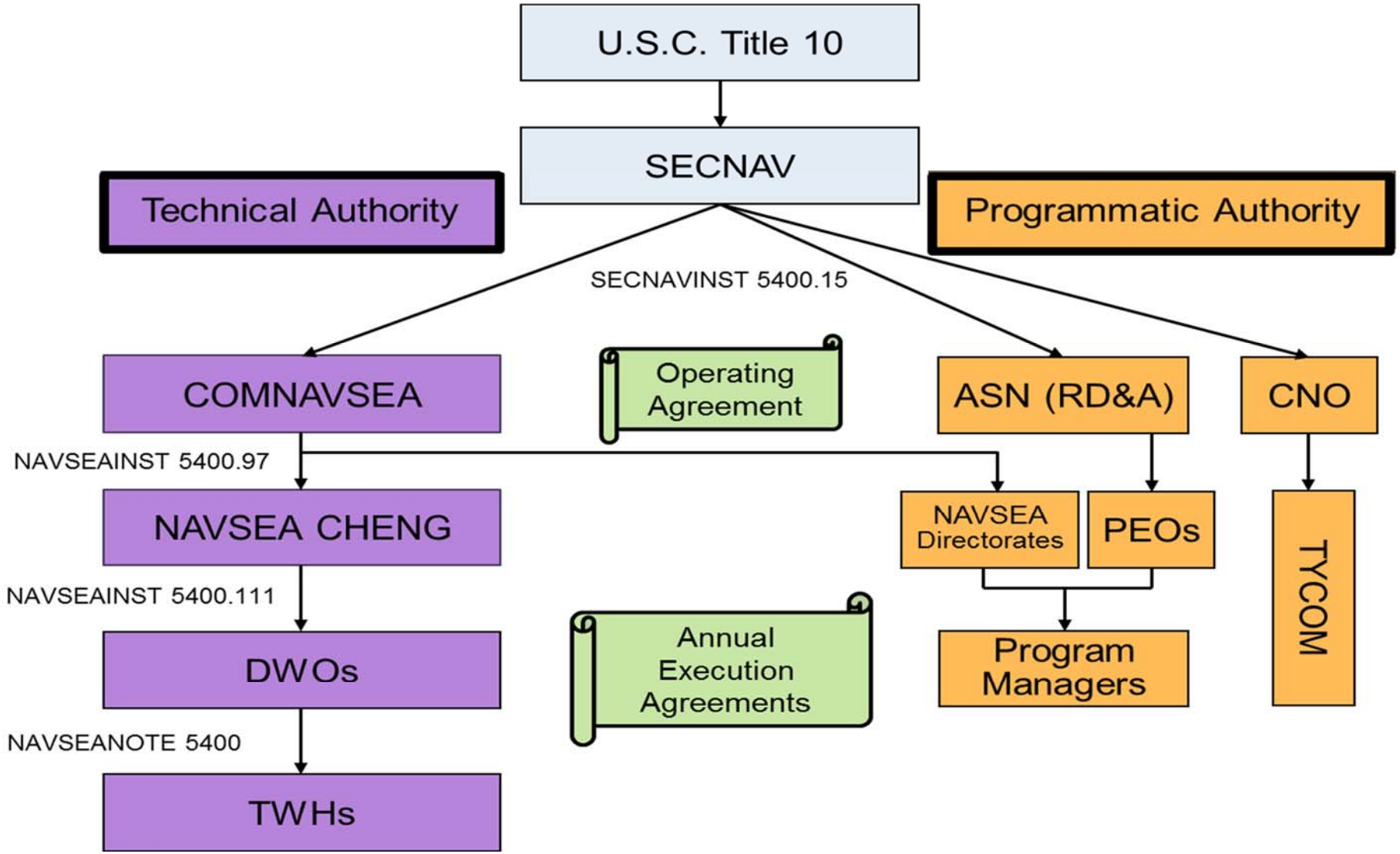
NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVSEA 05

Cyber Security Industry Day

October 30, 2015
RDML Bryant Fuller

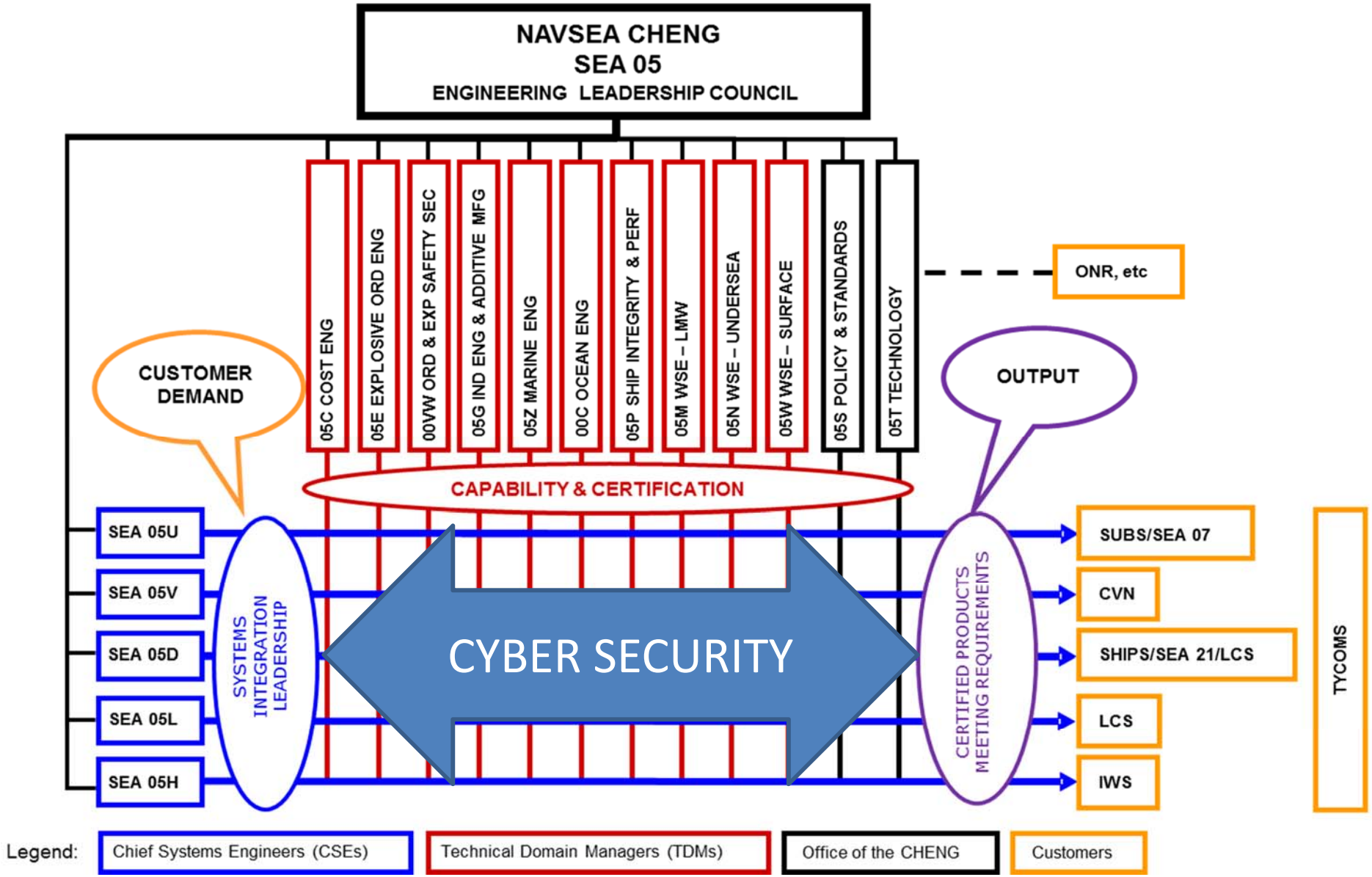
Technical Authority



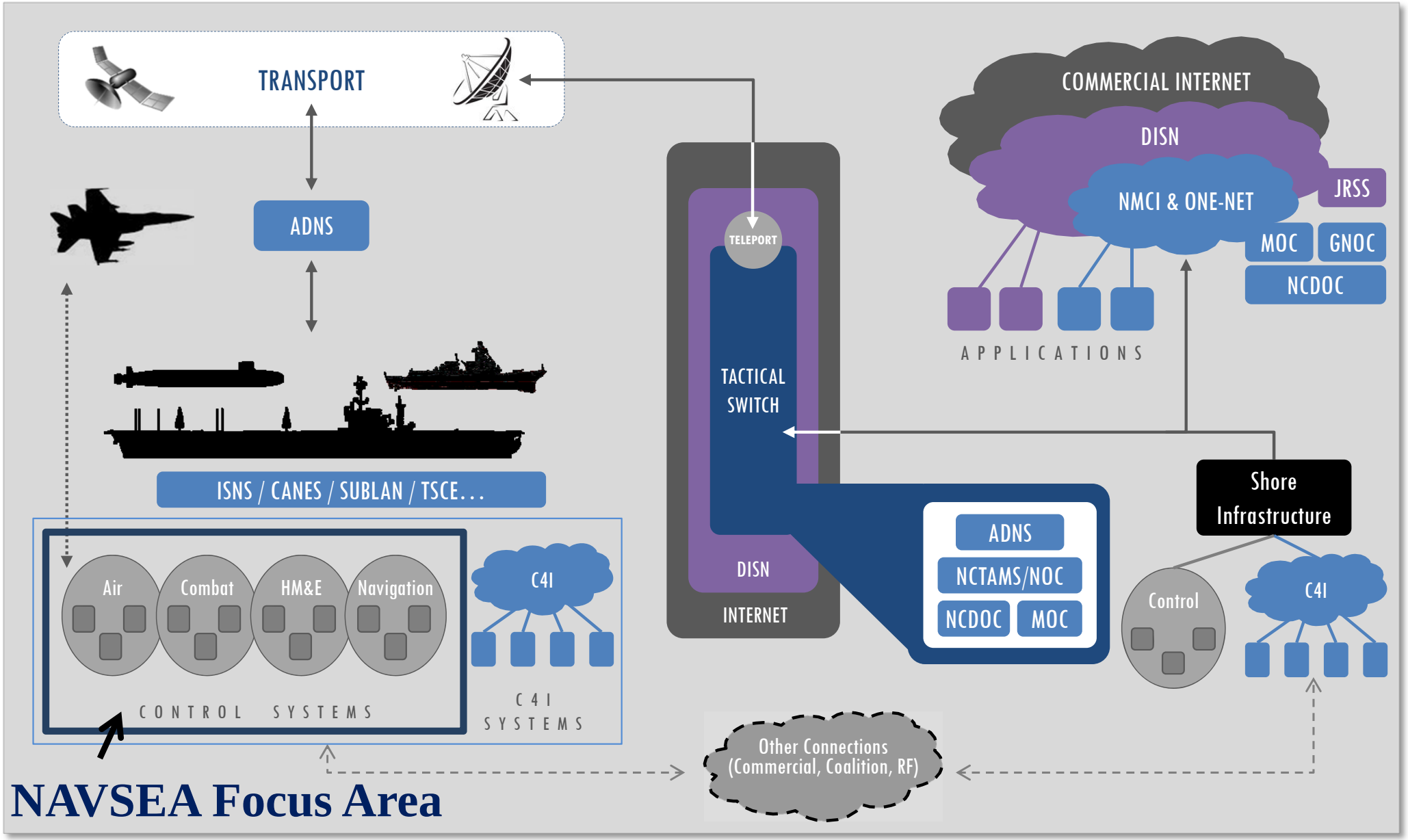
Inherently governmental chains of command
Independent and collaborative to enable the warfighter

Responsibility

TDMs and CSEs within NAVSEA



Cyber Platform



Control Systems

Diesel Engines & Power Transmission Systems

Combat Systems

Machinery Controls

Auxiliary Machinery & Fluid Systems

Electric Power Systems

Damage Control & Firefighting

Condition Assessment Systems & Video Systems

Life Support Systems, Climate Control and Compressed Air Systems

Maneuvering, Hydraulics, Hull Outfitting & Habitability

Navy Control Systems vs Information Systems

Category	Information System	Control System
Performance Requirements	• Non-real-time • High delay and jitter may be acceptable • Processing can be non-deterministic	• Real-time • System behavior and response time needs to be consistent (i.e., deterministic) and is time-critical • High delay and/or jitter is not acceptable
Availability Requirements	• Responses such as rebooting are acceptable • Availability deficiencies can often be tolerated, depending on the system's operational requirements	• Many Navy Control systems require high availability • Availability requirements may necessitate redundant systems • Outages must be planned and scheduled days/weeks in advance • High availability requires exhaustive pre-deployment testing
Communications	• Standard communications protocols used • Primarily wired networks with some localized wireless capabilities • Typical IT networking practices	• Both proprietary and standard communication protocols used • Ship control systems networks are complex and require the expertise of both network and control engineers
Change Management	• Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated.	• Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. Navy control system outages must be planned and scheduled days/weeks/months in advance.
Managed Support	• Allow for diversified support styles	• Service support is usually via a single vendor
Component Lifetime	• Lifetime on the order of 3-5 years	• Lifetime on the order of 15-20 years

Specifications and Standards

Functional Requirements Document is derived from:

- NIST SP800-53
- NIST SP800-82
- Technical Authority Board Standards
- Military Specific Standards

Standards below and FRD will be rolled into a Technical Publication for implementation as a one stop shop.

Specifications and Standards	Signed	Virtual TAB	Jan TAB
Host Level Protection	X		
Network Firewall	X		
Network Intrusion Detection System	X		
DFIA Afloat	X		
Information Systems Continuous Monitoring	X		
Security Information Event Management	X		
Vulnerability Scanning	X		
Boundary Protections	X		
CYBERSAFE Grade Criteria		X	
CYBERSAFE Grade Requirements		X	
DFIA Aviation		X	
OS Standard		X	
Cyber Risk Assessment			X
Tabletop Mission Cyber Risk Assessment			X
Supply Chain Risk Management (Trusted Networks & Systems)			X
DFIA Ashore			X

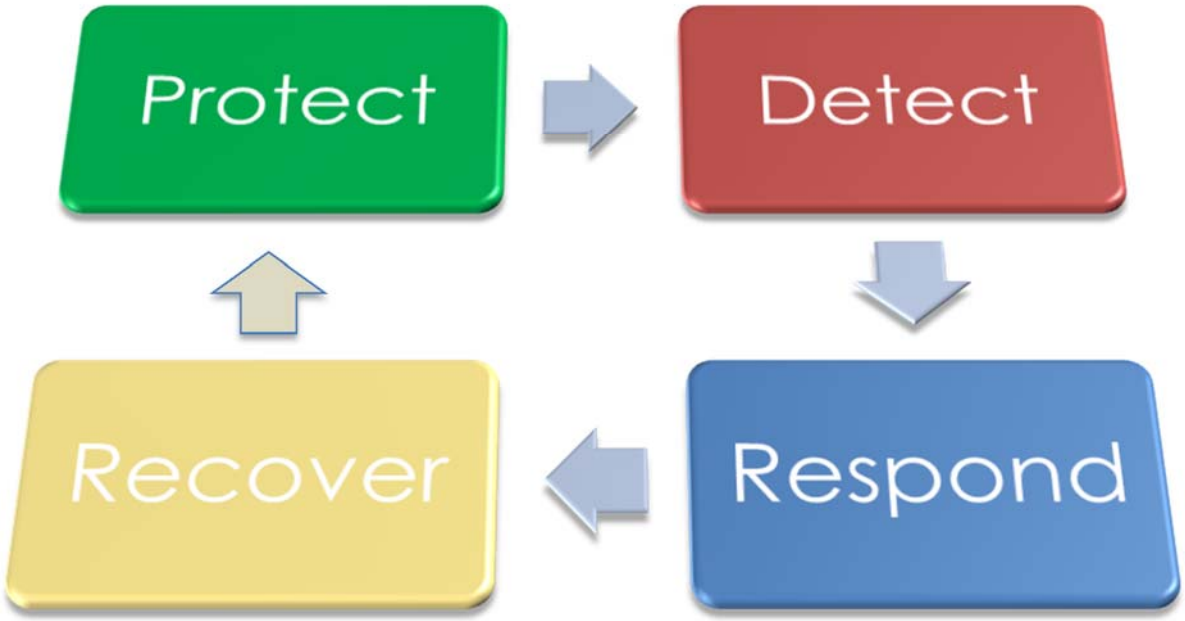
Future Cyber Security Standards

FY14	FY15	FY16	FY17
Host Level Protection	Security Information Event Management (SIEM)	Cyber Situation Awareness	Information Tagging - Data Tagging
Network Firewall	Vulnerability Scanning	Asset Management	Public Key Enabling
Network Intrusion Detection System (IDS) / Intrusion Protection System (IPS)	Boundary Protection	Information Sharing-Cross Domain Solution	Wireless Communications
DFIA Afloat	DFIA Aviation	CYBERSAFE Certification Requirements	Wireless Enclave Access Control
Continuous Monitoring	Operating System	CYBERSAFE Audit Criteria	Data Encryption - DIT, Link
Host Level Protection v2	Cyber Risk Assessment	Account Management	Data Encryption - DAR
	CYBERSAFE Grade Criteria	Cyber Configuration Management	Key Management / Exchange
	CYBERSAFE Grade Requirements	Software Assurance	DNS Security
	Trusted Systems and Networks	Event Management-Incident Management, Contingency Planning, Disaster Recovery, and Incident Response	Cyber Best Practices
	DFIA Ashore	Authentication and Authorization / IdAM	Virtualization Security
	DFIA and Standards POR Implementation Guidance and Glossary (includes Controls / Standards mapping)	Web Security	Assured Cloud Computing
		Email Security	Unified Capability - VoIP, Telecom
		BIOS Protection / TPM / Embedded Firmware	Maintenance / Support / Calibration Equipment
		Remote Access	
		Patch Management	
		Cyber Best Practices	

Completed
Swapped

Near Term Interests

1) Network graphing and display products
2) Intrusion detection products
3) User authentication or physical security products for control systems
4) Defensive software and hardware



Moving Forward

- Migrating out of the Windows environment
- Complete Functional Requirements Document and associated Tech Pub
- Establish notional architecture based on FRD/Tech Pub
- Develop Cyber Security SCDs
- Implement Cybersecurity Training for all
- Develop USS Secure Land Based Test Capability (Complete Virtual Ship)
- Implement Cyber Security SCDs

Cyber Security Points of Contact

Principal for Cyber Security for Control Systems (202) 781-1874	Cyber Security Program Manager (202) 781-3623	Information Assurance Technical Warrant Holder (360) 315-3426
Director of Marine Engineering (202) 781-5195	Chief Systems Engineer for Aircraft Carriers (202) 781-2150	Director Integrated Warfare Systems Engineering (202) 781-3740