Cybersecurity Awareness

3.4.3

SEAPOWER THROUGH ENGINEERING

TOPIC LEARNING OBJECTIVES

Upon successful completion of this topic, the student will be able to:

1. Recognize the importance of cybersecurity in the DoD, including its history and evolution.
2. Recognize the increasing sophistication of the threat to DoD cybersecurity.
3. Explain the consequences of not protecting DoD systems from cyber attacks.
4. Recognize key players and policy in cybersecurity including the intelligence community.
5. Recognize the critical processes that make and maintain secure systems, to include Risk Management Framework (RMF).
6. Explain how cybersecurity is integrated into every aspect of the acquisition program life-cycle, including both sides of the Systems Engineering "V" and the program protection plan.
7. Recognize that everyone, including EDOs, have a role in cybersecurity.

STUDENT PREPARATION

Student Support Material

1. 1. DAU Cybersecurity Video https://media.dau.edu/media/1_azceykk4

Primary References

1. DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle

Additional References

1. DAU ISA 1011 Information Systems Acquisition
2. DAU ISA 220 Risk Management Framework (RMF) for the Practitioner
3. DAU CLE 074

Overview

- The Basics
  - What is cybersecurity
  - Importance of cybersecurity (real world examples of threat environment)
- DoD’s (and the Navy’s) Approach
  - Cyber-related organizations
  - Cybersecurity Risk Management Framework and the Acquisition Process
  - Defense-in-Depth Functional Implementation Architecture (DFIA)
- Cybersecurity is everyone’s role
  - Cyber hygiene
  - Role of EDOs

What is Cybersecurity? (DoDI 8500.01)

- Prevention of damage to, protection of, and restoration of computers, electronic communication systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its:
  - Confidentiality
    - Is my data safe against disclosure to unauthorized entities?
  - Integrity
    - Is my data safe against modification and destruction?
  - Availability
    - Can I access my data/network resources as required and in a timely manner?
  - Non-Repudiation
    - Ensures that no parties can deny that it sent or received a message via encryption and/or digital signatures or approved some information
  - Authentication
    - The process of verifying whether someone is, in fact, who it is declared to be

What is Cybersecurity? (DoDI 8500.01)

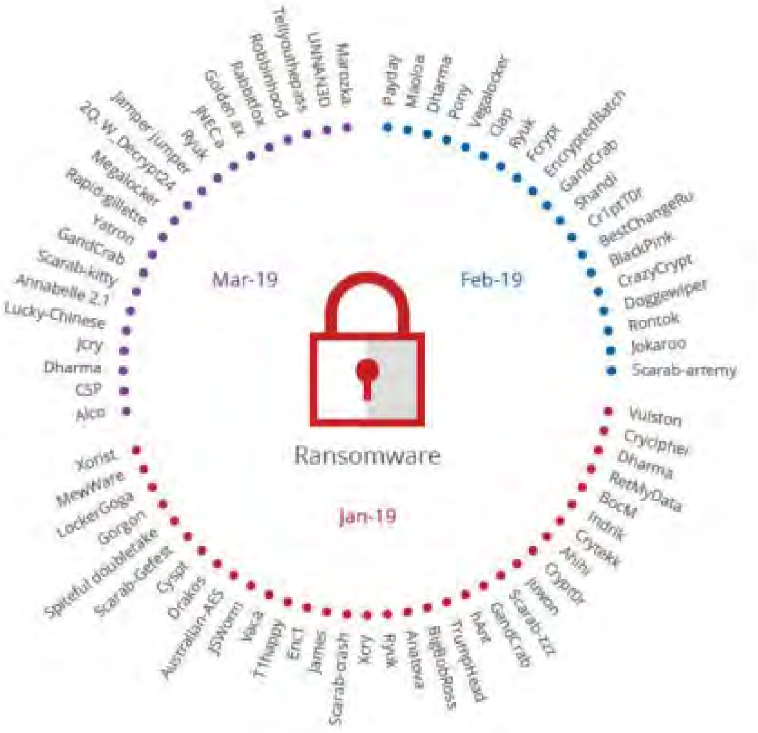
- A loss of confidentiality is the unauthorized disclosure of information
  - Theft of Personal Identifiable Information (PII) - Social Security Number (SSN), etc.
  - Classified information exfiltration from Secret Internet Protocol Router Network (SIPRNet)

- A loss of integrity is the unauthorized modification or destruction of information
  - Unauthorized modification of Global Positioning System (GPS) navigation information
  - Unauthorized destruction of PII on a Defense Business System (DBS)

- A loss of availability is the disruption of access to or use of information or an information system
  - Denial of Service (DoS) attack on Nuclear Command, Control and Communications (NC3) network
  - DoS attack on logistics parts ordering system
  - DoS attack on unmanned system command and control (C2) link

Driving Emphasis for Cybersecurity

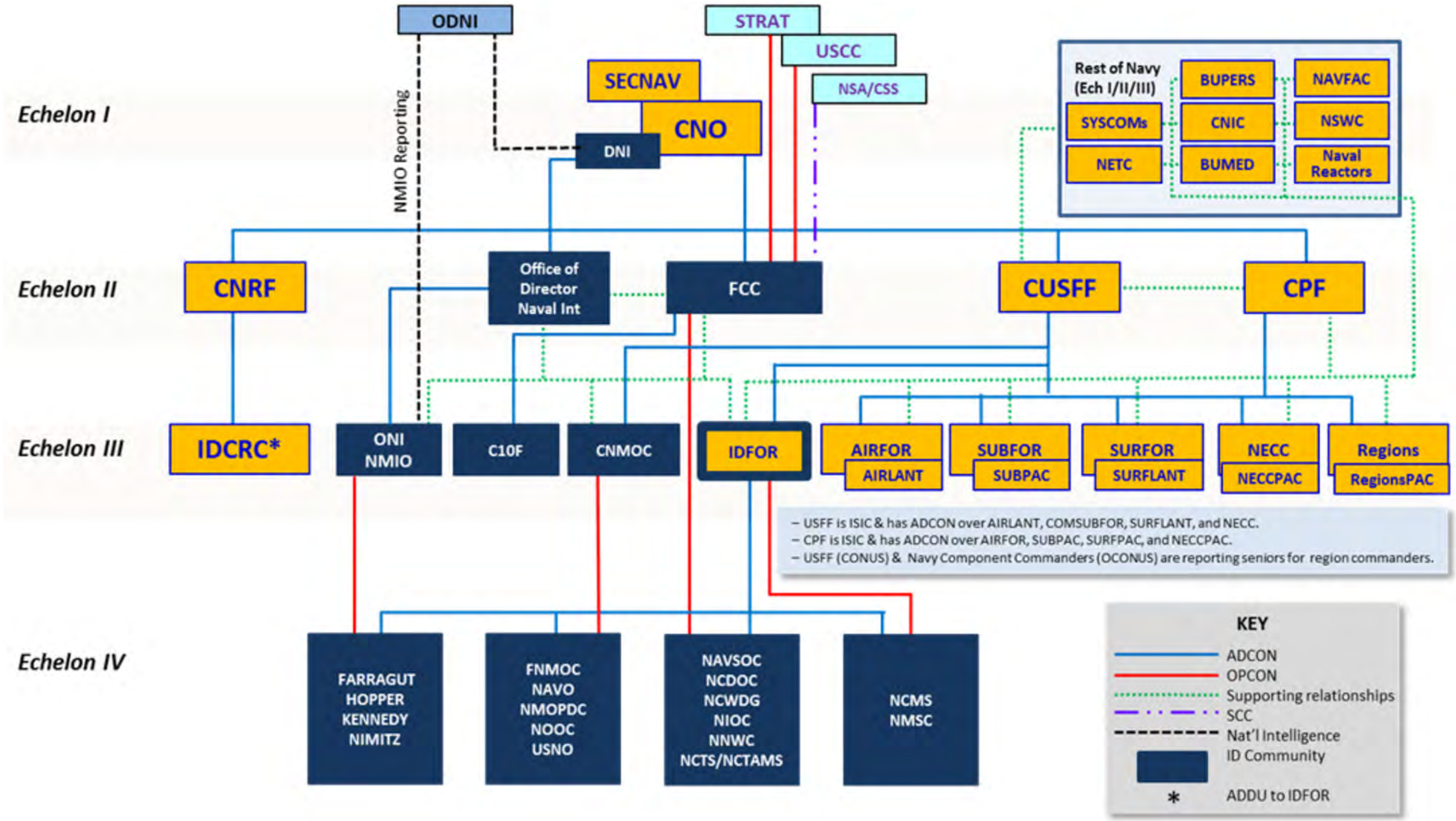
- **1998** – SOLAR SUNRISE Network intrusion on DoD networks
- **2006** – State Department networks hacked by unknown foreign intruders
- **2008** – Agent.btz: USB intrusion on DoD computers
- **2008** – Supply chain attack on credit card readers made in China
- **2009** – Conficker worm infects military databases and grounds French naval aircraft
- **2013** – Operation ROLLING TIDE in response to adversary intrusion on Navy networks
- **2015** – Office of Personnel Management (OPM) data breach
- **2017** – Equifax data breach
- **2018-2020** - Ransomware attacks on U.S. cities & hospitals



Overview

- The Basics
  - What is cybersecurity
  - Importance of cybersecurity (real world examples of threat environment)
- DoD’s (and the Navy’s) Approach
  - Cyber-related organizations
  - Cybersecurity Risk Management Framework and the Acquisition Process
  - Defense-in-Depth Functional Implementation Architecture (DFIA)
- Cybersecurity is everyone’s role
  - Cyber hygiene
  - Role of EDOs

Cyber C2 Organization



Echelon I

Echelon II

Echelon III

Echelon IV

ODNI

NMIO Reporting

STRAT

USCC

NSA/CSS

SECNAV

CNO

DNI

Rest of Navy (Ech I/II/III)

BUPERS

NAVFAC

SYSCOMs

CNIC

NSWC

NETC

BUMED

Naval Reactors

CNRF

Office of Director Naval Int

FCC

CUSFF

CPF

IDCRC*

ONI NMIO

C10F

CNMOC

IDFOR

AIRFOR

AIRLANT

SUBFOR

SUBPAC

SURFOR

SURFLANT

NECC

NECCPAC

Regions

RegionsPAC

- USFF is ISIC & has ADCON over AIRLANT, COMSUBFOR, SURFLANT, and NECC.
- CPF is ISIC & has ADCON over AIRFOR, SUBPAC, SURFPAC, and NECCPAC.
- USFF (CONUS) & Navy Component Commanders (OCONUS) are reporting seniors for region commanders.

FARRAGUT
HOPPER
KENNEDY
NIMITZ

FNMOC
NAVO
NMOPDC
NOOC
USNO

NAVSOC
NCDOC
NCWDG
NIOC
NNWC
NCTS/NCTAMS

NCMS
NMSC

KEY

━━━	ADCON
━━━	OPCON
┈┈┈	Supporting relationships
━ · ━ ·	SCC
- - - -	Nat'l Intelligence
■	ID Community
*	ADDU to IDFOR

Cyber-related Organizations

- DoN Chief Information Officer (CIO)
  - Policy and guidance
    - Evaluating and improving security of IT systems
    - Network architectures and interoperability
- US Cyber Command (USCYBERCOM)
  - Combatant Commander responsible for global cyber operations
  - Sets policy for entire DoD enterprise
- Fleet Cyber Command/U.S. 10th Fleet
  - Responsible for operations, maintenance, and defense of Navy networks (OPCON)
  - Navy Component Commander to USCYBERCOM
    - Sets cyber policy for the Navy, at the direction of USCYBERCOM
- Navy Cyber Defense Operations Command (NCDOC)
  - Cyber Security Service Providers (CSSP)
  - Actively defends Navy networks and performs incident response and forensics
  - Threat focused

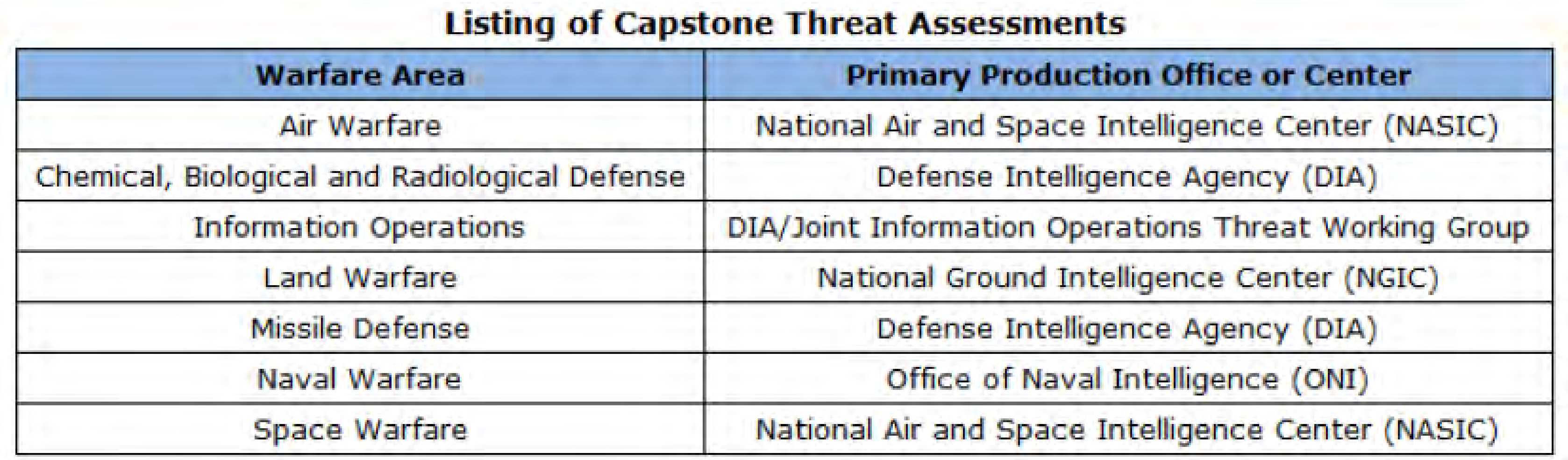
Cyber-related Organizations

- Naval Network Warfare Command (NAVNETWARCOM)
  - Tactical level command and control of Navy networks
  - Directs, operates, maintains, and secures Navy communications and network systems
  - Focus on security
- Naval Information Forces Command (NAVIFOR)
  - ***Cyber Type Commander (TYCOM)***
  - Organizes, mans, trains, and equips cybersecurity workforce
    - Cybersecurity Division Officer billet added to some ships
    - Training/assist visits for cybersecurity readiness inspections
- Naval Information Warfare Systems Command (NAVWAR)
  - ***Navy Cybersecurity Technical Authority (CS TA)***
  - Establish, monitor, and approve technical standards, tools, and processes
  - Responsible for cybersecurity architecture, specs, standards, and protocols
  - Warrant cybersecurity technical warrant holders within SYSCOMs
- Other Systems Commands
  - Design secure systems in alignment with CS TA standards

4

Intelligence Community

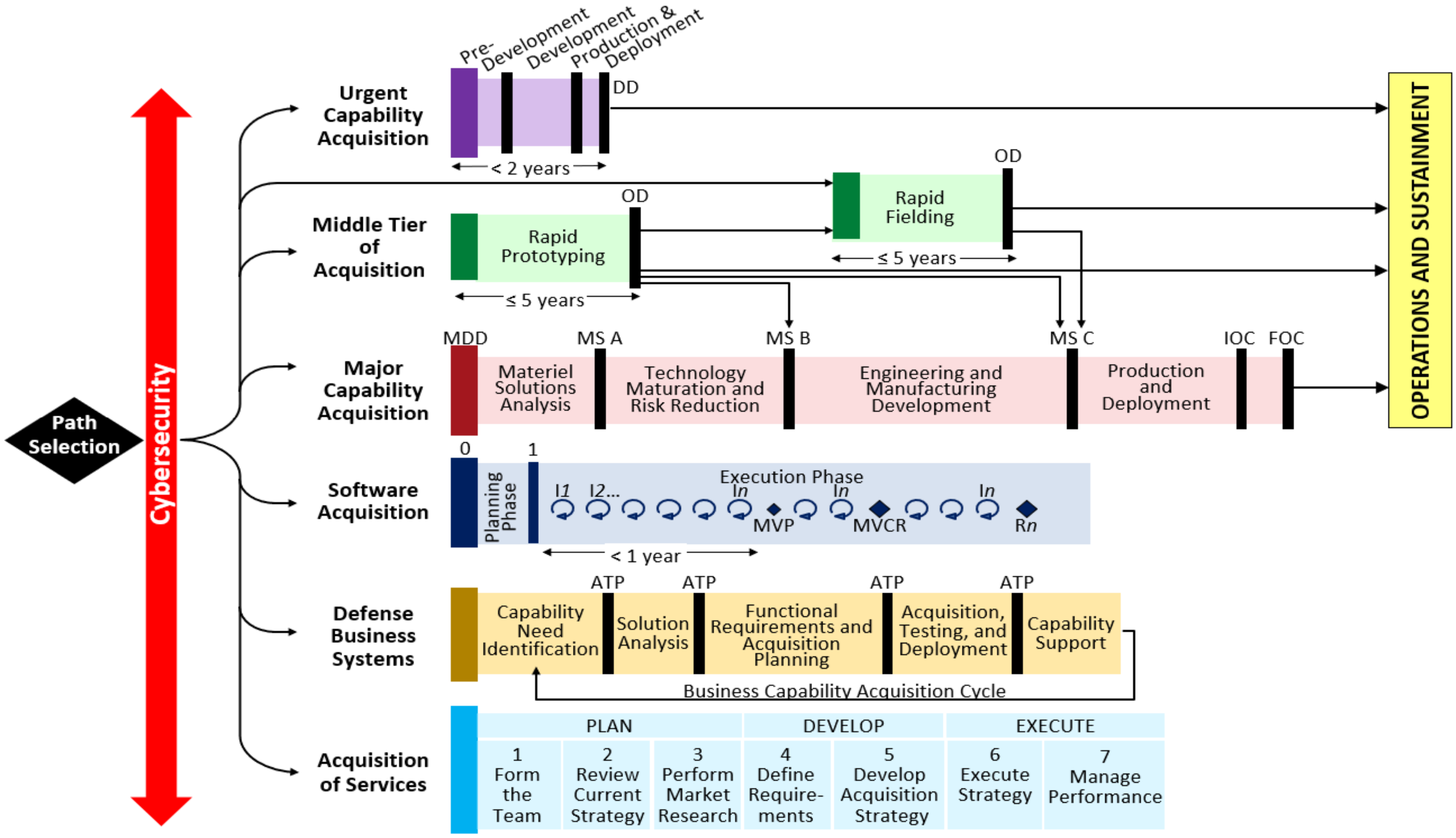
- PMs must use cyber threat information produced by the Intelligence Community (IC) in the development of their cyber security strategy assessment of risks
- Intelligence Community products that support acquisition programs include:
  - Validated Online Life-cycle Threat (VOLT) reports
    - The primary threat document supporting a specific defense program
    - Includes all threat modules relevant to the supported program
  - Capstone Threat Assessments (CTA): Forecast threat capabilities for specific warfare areas
  - Technology targeting risk assessments



Listing of Capstone Threat Assessments

Warfare Area	Primary Production Office or Center
Air Warfare	National Air and Space Intelligence Center (NASIC)
Chemical, Biological and Radiological Defense	Defense Intelligence Agency (DIA)
Information Operations	DIA/Joint Information Operations Threat Working Group
Land Warfare	National Ground Intelligence Center (NGIC)
Missile Defense	Defense Intelligence Agency (DIA)
Naval Warfare	Office of Naval Intelligence (ONI)
Space Warfare	National Air and Space Intelligence Center (NASIC)

Cybersecurity and Adaptive Acquisition Framework



Path Selection

Cybersecurity

Urgent Capability Acquisition

Pre-Development | Development | Production & Deployment | DD

< 2 years

Middle Tier of Acquisition

Rapid Prototyping | OD

≤ 5 years

Rapid Fielding | OD

≤ 5 years

Major Capability Acquisition

MDD | Materiel Solutions Analysis | MS A | Technology Maturation and Risk Reduction | MS B | Engineering and Manufacturing Development | MS C | Production and Deployment | IOC | FOC

Software Acquisition

0 | Planning Phase | 1 | Execution Phase

I1 | I2... | In | MVP | In | MVCR | In | Rn

< 1 year

Defense Business Systems

Capability Need Identification | ATP | Solution Analysis | ATP | Functional Requirements and Acquisition Planning | ATP | Acquisition, Testing, and Deployment | ATP | Capability Support

Business Capability Acquisition Cycle

Acquisition of Services

PLAN			DEVELOP		EXECUTE	
1 Form the Team	2 Review Current Strategy	3 Perform Market Research	4 Define Require-ments	5 Develop Acquisition Strategy	6 Execute Strategy	7 Manage Performance

OPERATIONS AND SUSTAINMENT

Cybersecurity Strategy crosses all pathways within the Adaptive Acquisition Framework

Cybersecurity in the Acquisition Process

- The PM is responsible for meeting cybersecurity requirements throughout the life-cycle of the program
- A program's cybersecurity strategy annex must be documented within the Program Protection Plan (PPP)
  - The cybersecurity annex will document how the system will operate in a cyber-contested environment as well as the consequences of a cybersecurity breach and related concerns
- The Cybersecurity Risk Management Framework (RMF) is required for all acquisitions containing Information Technology

Cybersecurity Strategy is part of the Program Protection Plan and is a statutory requirement starting at M/S A and updated at each milestone

Risk Management Framework

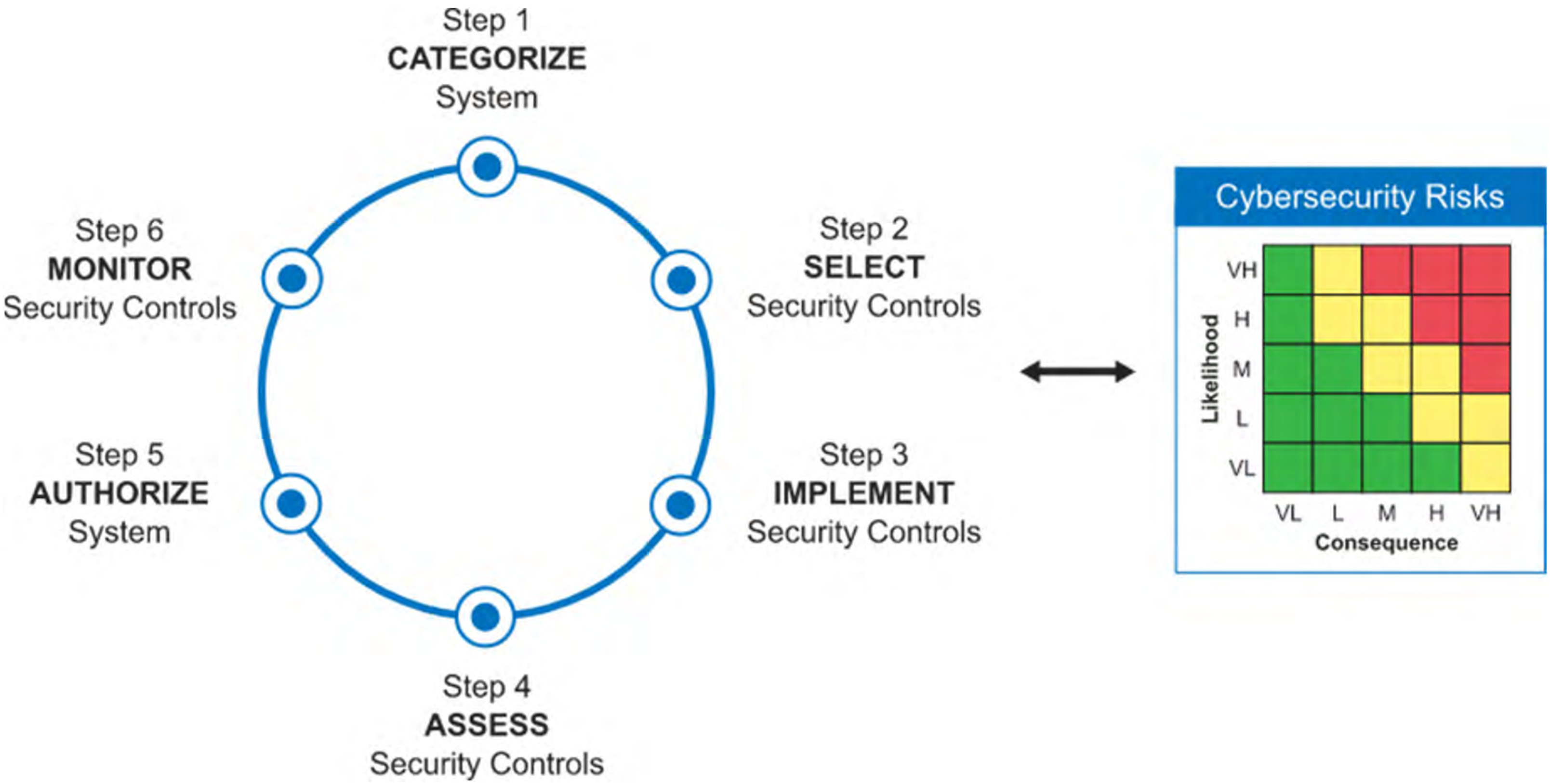
- What is RMF?
  - A process that integrates security and risk management activities into the acquisition life-cycle
  - A 6-step process that emphasizes continuous monitoring and timely correction of deficiencies
  - Applicable to all Information System (IS) and Platform Information Technology (PIT) systems as well as DoD partnered systems
- Goals of RMF
  - Perform risk assessment throughout the acquisition life-cycle
  - ***Cybersecurity "baked in" vs "bolted on"***
  - Improve information security
  - Improve understanding of risks to Navy systems and missions

RMF is executed throughout the acquisition life-cycle

Importance of Assessing Risk

- RMF requires cybersecurity risk assessments and management
  - Risk assessments help decision-makers determine:
    - To what degree can threat actors impact Navy systems and missions via cyber-attack?
    - Where can mitigations most effectively and efficiently be employed?
    - Which risks should the Navy prioritize, accept, or actively mitigate?
- Risk assessments allow information system owners to identify high-level risks
- Information System Owners may tailor security controls, but the risk associated with not implementing a control must be assessed and recorded

Risk Management Framework



Step 1
CATEGORIZE
System

Step 2
SELECT
Security Controls

Step 3
IMPLEMENT
Security Controls

Step 4
ASSESS
Security Controls

Step 5
AUTHORIZE
System

Step 6
MONITOR
Security Controls

Cybersecurity Risks

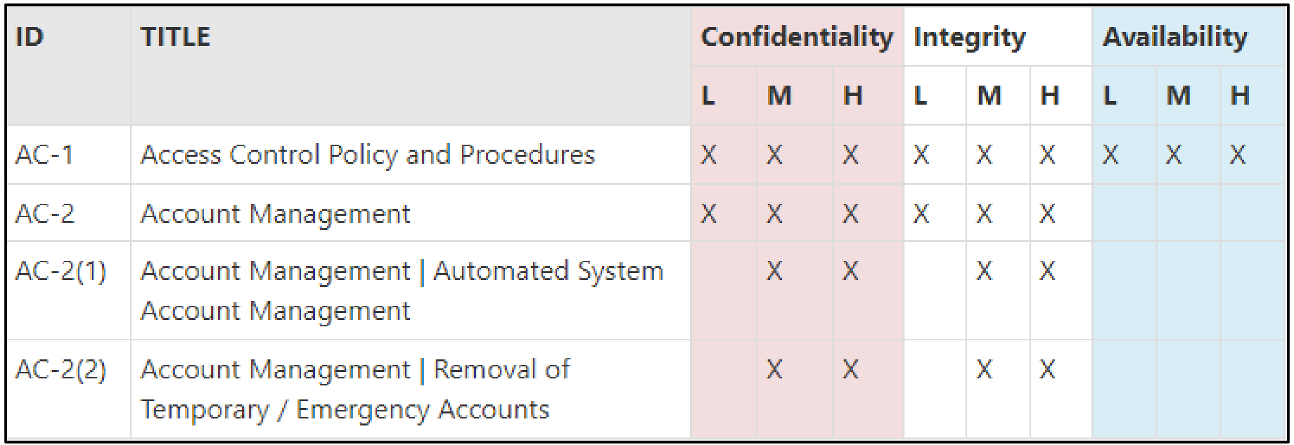
Likelihood					
VH	🟩	🟨	🟥	🟥	🟥
H	🟩	🟨	🟨	🟥	🟥
M	🟩	🟩	🟨	🟨	🟥
L	🟩	🟩	🟩	🟨	🟨
VL	🟩	🟩	🟩	🟩	🟨
	VL	L	M	H	VH
	Consequence				

Step 1: Categorize the System

- Categorize the system and the information processed, stored, and transmitted by that system based on a potential impact
  - Identify all types of information:
    - e.g., privacy, medical, proprietary, financial, investigative, contractor-sensitive, security management
    - Can be defined by an organization or, in some instances, by a public law, executive order, directive, policy, or regulation
  - Select Security Objective: Confidentiality, Integrity, Availability
  - Determine Level of impact (X): Low, moderate, or high
  - Security Category = (Confidentiality, X), (Integrity, X), (Availability, X)
    - Example: Security Control Health Information= (Confidentiality, High), (Integrity, High), (Availability, Low)
  - Document the categorization within the program protection plan
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2: Select Security Controls

- Select security controls based on categorization of the system
  - To meet security requirements as defined by DoD baseline configuration standards
  - To ensure the integrity, confidentiality, and availability of the information and information system in accordance with the organization's protection strategy
  - Security controls are selected according to CNSSI 1253 for all DoD systems, including National Security Systems (NSS)
  - Can tailor and supplement security controls to address the risk associated with the specific system
- Develop system-level continuous monitoring strategy
- Review and approve the Security Plan and continuous monitoring strategy



ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X
AC-2	Account Management	X	X	X	X	X	X			
AC-2(1)	Account Management | Automated System Account Management		X	X		X	X			
AC-2(2)	Account Management | Removal of Temporary / Emergency Accounts		X	X		X	X			

Step 3: Implement Security
Step 4: Assess Security Control

- Implement security controls
  - Implement control solutions consistent with DoD Component Cybersecurity architectures
    - Translate security controls into systems specification
    - Integrate specifications into the system design
  - Document security control implementation in the Security Plan

- Assess security controls
  - Develop and approve Security Assessment Plan
  - Assess security controls
    - Were the system controls properly implemented?
  - Security Control Assessor (SCA) prepares Security Assessment Report (SAR)
    - SCA makes recommendation for cybersecurity risk acceptance or denial
  - Conduct initial remediation actions

Step 5: Authorize System

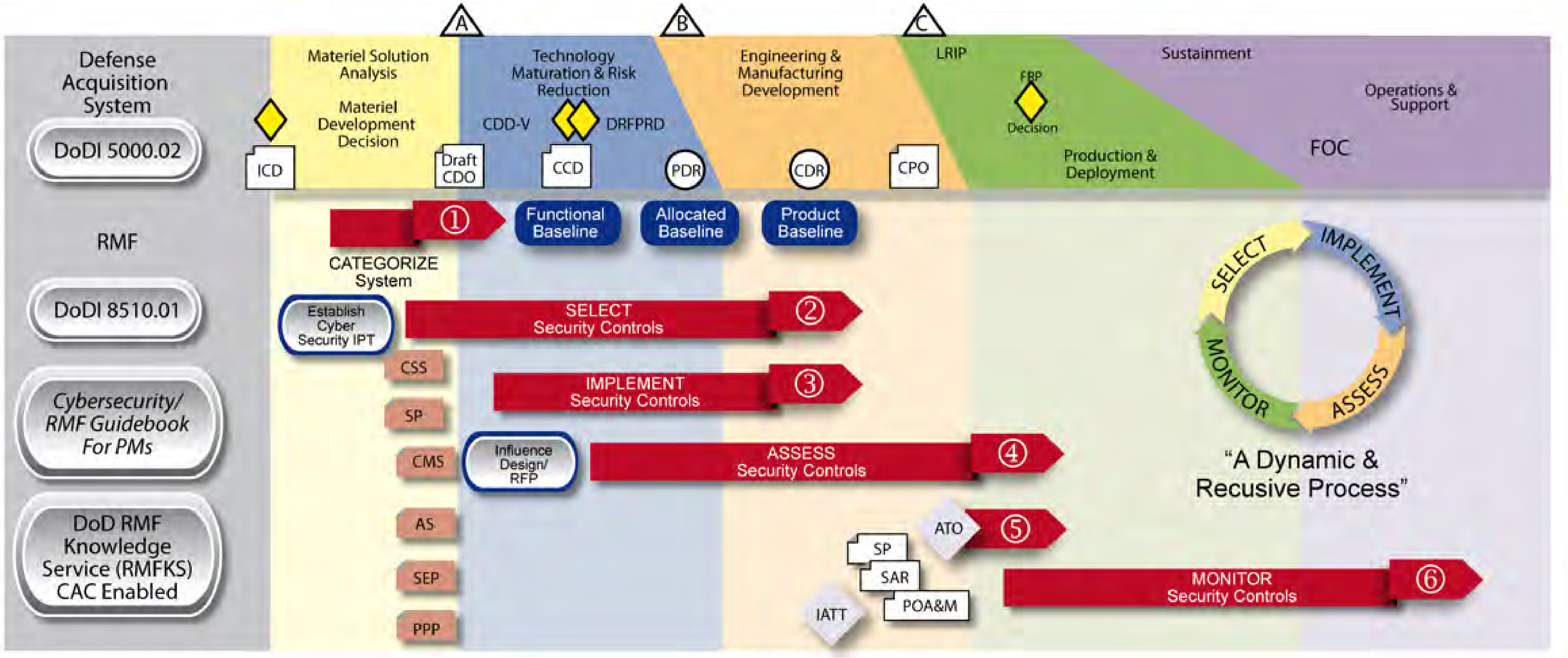
- Authorize system
  - Prepare Plan of Action and Milestones (POA&M) based on vulnerabilities identified in Step 4
    - POA&M reflects organizational priorities for addressing any remaining weaknesses and deficiencies in an information system and its environment of operation
  - Submit Security Authorization Package to Authorizing Official (AO). The Authorization Package contains:
    - Security Plan
    - Security Assessment Report
    - POA&M
  - AO conducts final Risk Determination and Risk Assessment
  - AO makes authorization decision
    - A DoD authorization decision is expressed as an Authorization to Operate (ATO), an Interim Authorization to Test (IATT), or a Denial of Authorization to Operate (DATO)

5

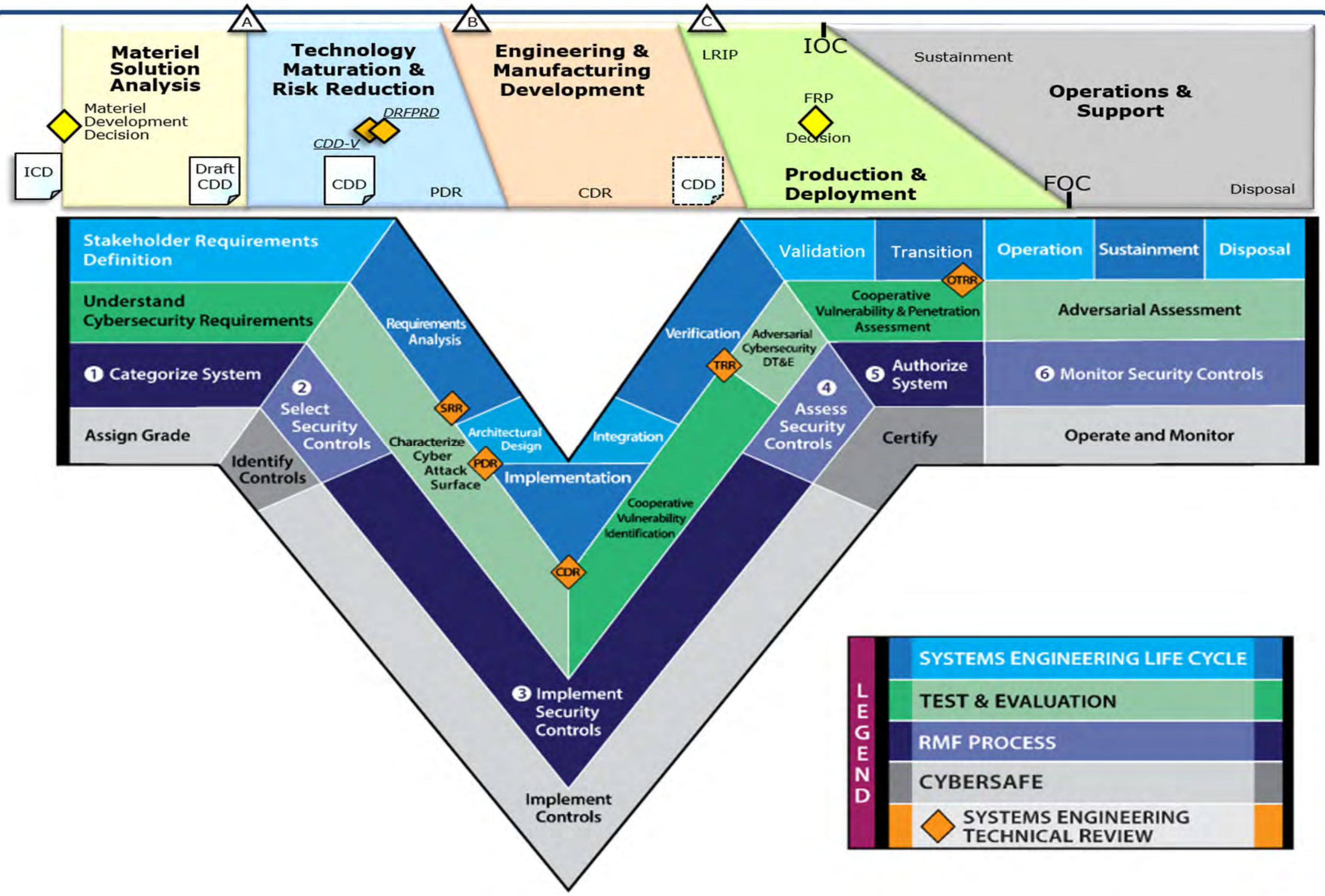
Step 6: Monitor Security Controls

- 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

RMF across Acquisition Lifecycle


Defense Acquisition System
DoDI 5000.02
RMF
DoDI 8510.01
Cybersecurity/ RMF Guidebook For PMs
DoD RMF Knowledge Service (RMFKS) CAC Enabled
A
B
C
Materiel Solution Analysis
Materiel Development Decision
Technology Maturation & Risk Reduction
CDD-V
DRFPRD
Engineering & Manufacturing Development
LRIP
FRP Decision
Sustainment
Operations & Support
Production & Deployment
FOC
ICD
Draft CDO
CCD
PDR
CDR
CPO
①
CATEGORIZE System
Functional Baseline
Allocated Baseline
Product Baseline
Establish Cyber Security IPT
SELECT Security Controls
②
CSS
IMPLEMENT Security Controls
③
SP
CMS
Influence Design/ RFP
ASSESS Security Controls
④
AS
ATO
⑤
SP
SAR
POA&M
SEP
IATT
PPP
MONITOR Security Controls
⑥
SELECT
IMPLEMENT
ASSESS
MONITOR
"A Dynamic & Recusive Process"

RMF Across the Life-cycle


A
B
C
Materiel Solution Analysis
Materiel Development Decision
ICD
Draft CDD
Technology Maturation & Risk Reduction
DRFPRD
CDD-V
CDD
PDR
Engineering & Manufacturing Development
CDR
CDD
LRIP
IOC
FRP
Decision
Production & Deployment
Sustainment
Operations & Support
FOC
Disposal
Stakeholder Requirements Definition
Understand Cybersecurity Requirements
1 Categorize System
Assign Grade
2 Select Security Controls
Identify Controls
Requirements Analysis
SRR
Characterize Cyber Attack Surface
Architectural Design
PDR
Implementation
CDR
3 Implement Security Controls
Implement Controls
Integration
Cooperative Vulnerability Identification
Verification
TRR
Adversarial Cybersecurity DT&E
4 Assess Security Controls
Validation
Transition
OTRR
Cooperative Vulnerability & Penetration Assessment
5 Authorize System
Certify
Operation
Sustainment
Disposal
Adversarial Assessment
6 Monitor Security Controls
Operate and Monitor
LEGEND
SYSTEMS ENGINEERING LIFE CYCLE
TEST & EVALUATION
RMF PROCESS
CYBERSAFE
SYSTEMS ENGINEERING TECHNICAL REVIEW

Overview

- The Basics
  - What is cybersecurity
  - Importance of cybersecurity (real world examples of threat environment)
- DoD’s (and the Navy’s) Approach
  - Cyber-related organizations
  - Cybersecurity Risk Management Framework and the Acquisition Process
  - Defense-in-Depth Functional Implementation Architecture (DFIA)
- Cybersecurity is everyone’s role
  - Cyber hygiene
  - Role of EDOs

Cyber Hygiene

- Install and maintain firewalls
  - Review firewall logs for signs of intrusion
- Perform routine scans of network systems, looking for malware or other unauthorized software
- Perform routine scans of systems looking for known vulnerabilities
  - Take timely actions to eliminate or mitigate those vulnerabilities
- Whitelisting
  - Software that will only allow authorized programs to run
  - Prevents programs that are downloaded inadvertently or maliciously from running
- Ensuring all network hardware uses a common and approved baseline image
  - Don't make changes that contradict a system's configuration management policy and procedures

EDO’s Role in Cybersecurity

- Program Managers are responsible for the Cybersecurity of their programs, systems, and information
  - Cybersecurity must be part of every stage in the program life-cycle
- EDOs must be knowledgeable leaders
  - Cybersecurity is a critical aspect of any domain an EDO is asked to lead
  - Be accountable and hold others accountable
  - Make cybersecurity part of the programmatic, engineering, and acquisition processes
  - Involve cybersecurity professionals
- Cybersecurity knowledge and leadership is now an essential part of the EDO skillset, no matter where an EDO is assigned
- We need to know how to keep programs focused on cybersecurity and weave it into every aspect of program planning, execution, and maintenance
- Understanding of cyber tools and processes is necessary for acquiring and maintaining secure systems

Responsibility for Cybersecurity extends to all members of the acquisition workforce

7

Summary

- Which organization is the Type Commander for cyber?

- Which organization is the Navy's component commander to U.S. Cyber Command

- What process does DoD use to "bake in" cybersecurity in acquisition programs

Navy Cyber Safety (CYBERSAFE) Program

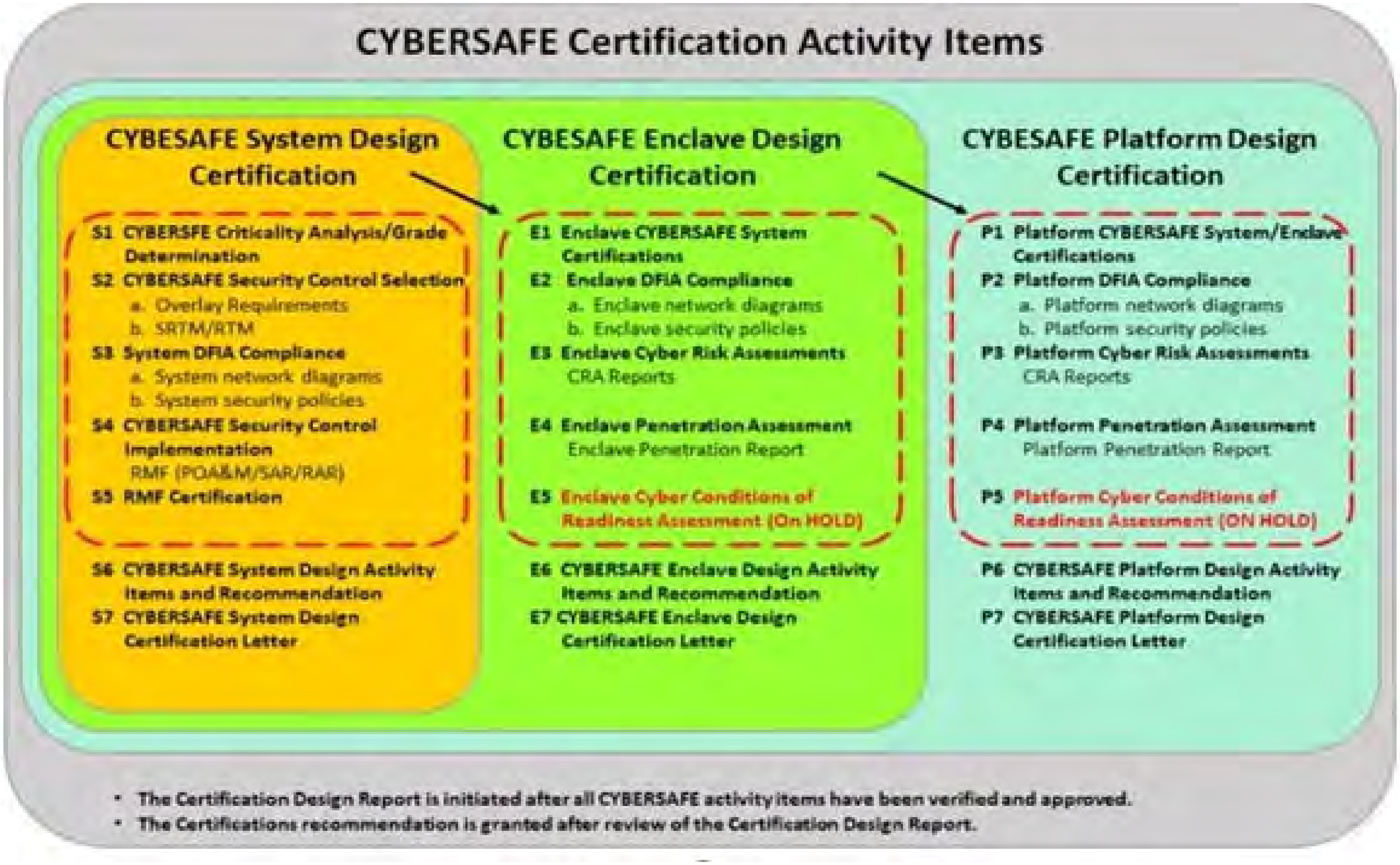
- What is CYBERSAFE?
  - Harden mission-critical systems and components which will provide ***maximum reasonable assurance of survivability and resiliency*** for critical warfighting missions
    - CYBERSAFE requirements focus on ensuring resiliency of a system's security controls in a contested environment

- What does CYBERSAFE do?
  - ***Assesses risk to the mission*** (system of systems), and applies an elevated set of security controls that apply to only a selected subset of systems and components

- Three CYBERSAFE Certifications
  - System Design Certification
  - Enclave Design
  - Platform Certifications

Objective of CYBERSAFE is to provide mission assurance

CYBERSAFE Certification Documentation



CYBERSAFE Certification Activity Items

CYBESAFE System Design Certification

S1 CYBERSFE Criticality Analysis/Grade Determination

S2 CYBERSAFE Security Control Selection

a. Overlay Requirements

b. SRTM/RTM

S3 System DFIA Compliance

a. System network diagrams

b. System security policies

S4 CYBERSAFE Security Control Implementation

RMF (POA&M/SAR/RAR)

S5 RMF Certification

S6 CYBERSAFE System Design Activity Items and Recommendation

S7 CYBERSAFE System Design Certification Letter

CYBESAFE Enclave Design Certification

E1 Enclave CYBERSAFE System Certifications

E2 Enclave DFIA Compliance

a. Enclave network diagrams

b. Enclave security policies

E3 Enclave Cyber Risk Assessments

CRA Reports

E4 Enclave Penetration Assessment

Enclave Penetration Report

E5 Enclave Cyber Conditions of Readiness Assessment (On HOLD)

E6 CYBERSAFE Enclave Design Activity Items and Recommendation

E7 CYBERSAFE Enclave Design Certification Letter

CYBESAFE Platform Design Certification

P1 Platform CYBERSAFE System/Enclave Certifications

P2 Platform DFIA Compliance

a. Platform network diagrams

b. Platform security policies

P3 Platform Cyber Risk Assessments

CRA Reports

P4 Platform Penetration Assessment

Platform Penetration Report

P5 Platform Cyber Conditions of Readiness Assessment (ON HOLD)

P6 CYBERSAFE Platform Design Activity Items and Recommendation

P7 CYBERSAFE Platform Design Certification Letter

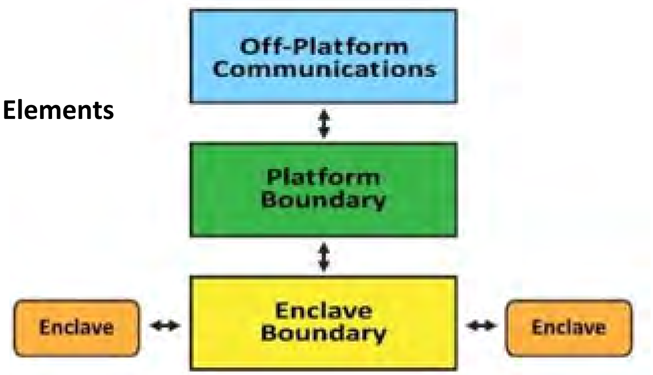
- The Certification Design Report is initiated after all CYBERSAFE activity items have been verified and approved.
- The Certifications recommendation is granted after review of the Certification Design Report.

Defense-in-Depth Functional Implementation Architecture (DFIA)

- What is DFIA?
  - Navy’s solution to implement a comprehensive defense-in-depth IA across SYSCOM boundaries
  - A layered Defense-in-Depth approach that enables inheritance
  - Greater interoperability and improved cyber situational awareness across Navy networks

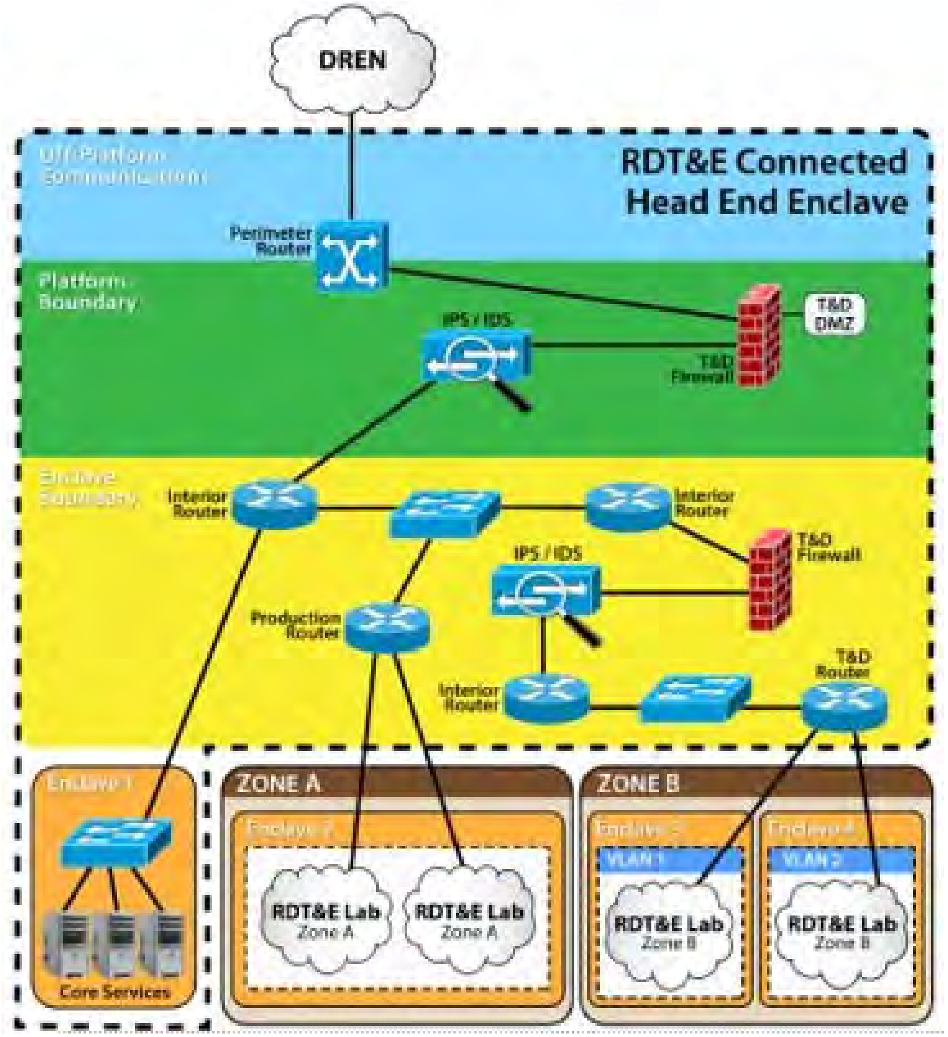
- The overall goal of DFIA is to provide a uniform security framework to:
  - Support interoperability
  - Reduce cost
  - Improve Cybersecurity
  - Eliminate duplication of effort

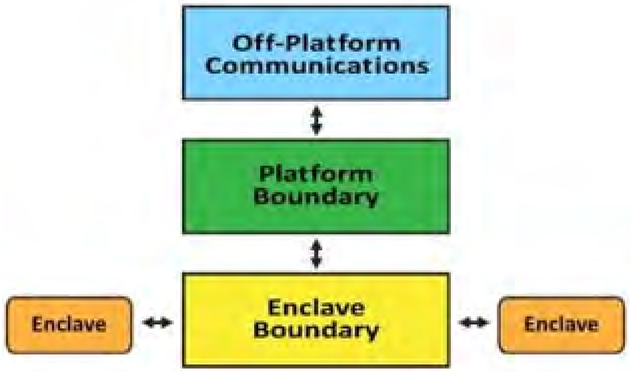
Four DFIA Elements



DFIA facilitates and standardizes the implementation of security controls through the RMF, CYBERSAFE, and Acquisition processes

Example DFIA Implementation



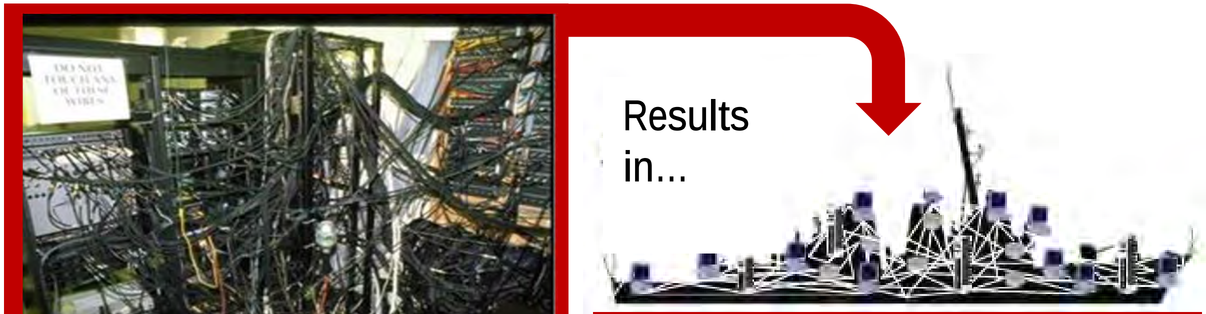


- DFIA compliant Off-Platform Communications and Platform Boundary
- Enclave Boundary uses network paths capable of supporting complete DFIA implementation
- Enclave Boundary has limited elements of a security stack (e.g., routers)
- RDT&E Enclaves implementing DFIA by using physical or logical separation

Today’s Challenge: Stove-Pipes

The Collective Result of Individual Decisions

Where We Are Today



Difficult to Manage, Defend & Operate

Infrastructure:

- ▼ Too much
- ▼ Too varied
- ▼ Too old

Software & Applications:

- ▼ Too many
- ▼ Too varied to maintain it all

Holistic Enterprise Approach to Drive Interoperability & Cybersecurity

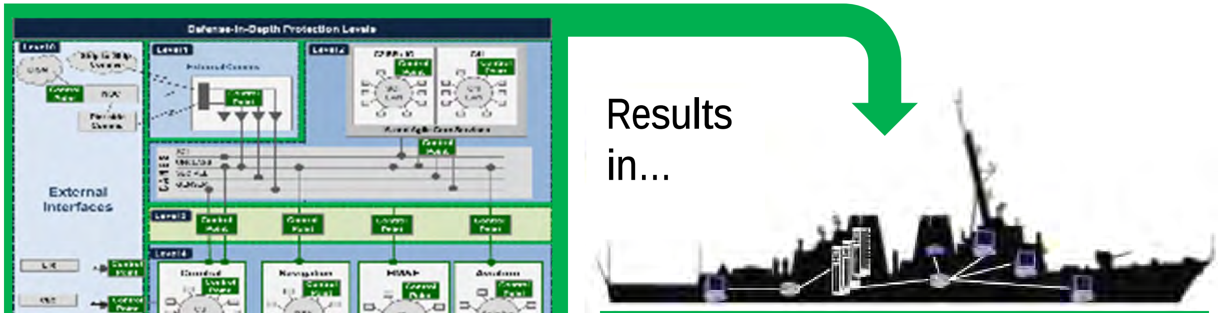
Infrastructure:

- ▼ Rapid hardware refresh as a requirement
- ▼ Decouple hardware from Software & Applications

Software & Applications:

- ▼ Quality Assurance
- ▼ Configuration Management

Where We Need To Go



Easier to Manage, Defend & Operate

Today’s infrastructure: Vulnerable to cyber attack; difficult to achieve interoperability