



DoD Strategy for Cyber Resilient Weapon Systems

Melinda K. Reed

**Office of the Deputy Assistant Secretary of Defense
for Systems Engineering**

**NDIA Systems Engineering Conference
October 2016**



Goal



Goal: Improve resiliency of weapons system designs to cyber attack*

- **Action: Develop a new enclosure to the 5000.02***
 - DTM-118: Cybersecurity and Program Security in the Defense Acquisition System
- **Action: Review system security engineering design processes and methods and recommend standardization or other approaches to improve cybersecurity of designs***
 - DASD(SE), in partnership with the Services, CIO, other stakeholders have identified multiple activities to improve security of engineering designs. An opportunity exists to collaborate, mature efforts, and move toward common approaches

Key Objectives:

- Determine set of engineering design patterns, standards and methods for cyber resilient weapon systems, addressing both systems in development and systems in sustainment
- Establish a foundation to grow the engineering practices and strengthen engineering agility

***extract from Better Buying Power 3.0 Implementation Guidance**

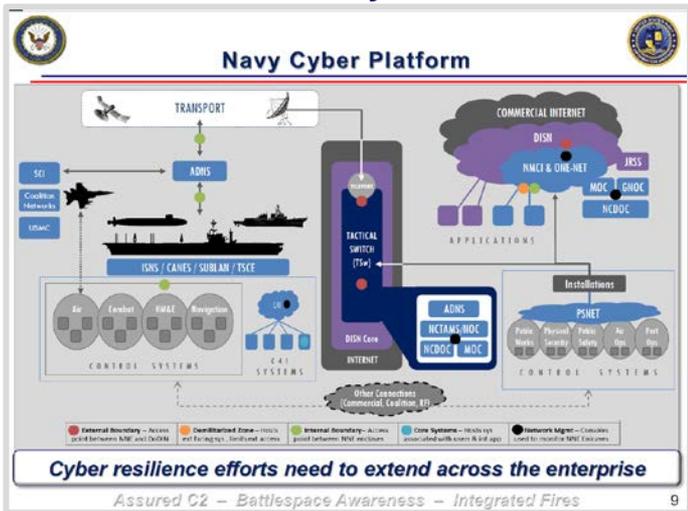


Military Departments Are Responding



Each MILDEP is moving forward to meet its organizational needs

Navy



Army

Cyber Integrator Application

Home Cyber Integrator Admin JFAC Portal

Compliance					Recommended Guidance					
Requirements	Documentation	RMF	Testing	MEC	Evaluation Criteria	SWA	VA	AT	EW	SCS
MSA	Done	Done	Done	Done	Requirements Defined	On Track	Done	Done	Done	On Track
TMRR	Done	Done	Done	Done	Contractual Language Defined	On Track	Done	Behind	Done	Done
EMD	On Track	On Track	Behind	On Track	Plan Defined	Done	Done	Behind	Done	Behind
P&D	NS	NS	NS	NS	Cost Planned	On Track	Done	N/A	Done	Done
SUS	NS	NS	NS	NS	Other	Done	Done	N/A	Done	Done

Air Force

LOA1: Mission Threat Analysis	LOA2: Integrate into SE Process	LOA3: Cyber Workforce Development	LOA4: Enhance Adaptability	LOA5: Develop Common Security Environment	LOA6: Assess and Fix Legacy Systems	LOA7: Intelligence for Cyber Security	Mission Assurance End State
End-to-end operational process supporting a mission	Incorporates systems security engineering into all phases of the acquisition life cycle	A cyber-savvy workforce capable of integrating cyber security measures into all phases of the acquisition process	Vigorously enhances the adaptability of our weapon systems to rapidly respond to threats	Facilitates the integration of cyber security measures into all phases of the acquisition process	Prioritizes legacy systems to fix existing and future cyber vulnerabilities	Strengthen acquisition cyber security through improved intelligence collection, analysis, and application	

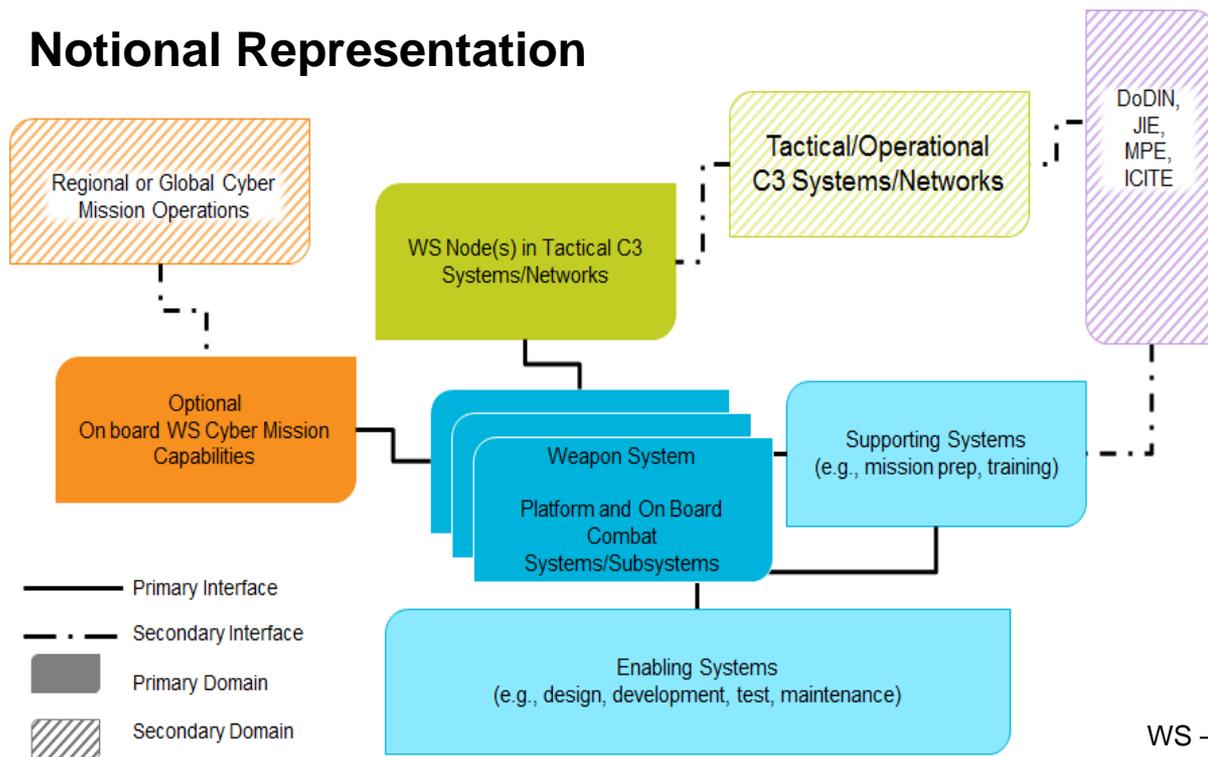
An Opportunity Exists Across the Services to:

- Collaborate
- Mature efforts, and
- Move toward common approaches



Weapon System Complexity

Notional Representation



The Engineering approach is driven by the following constraints:

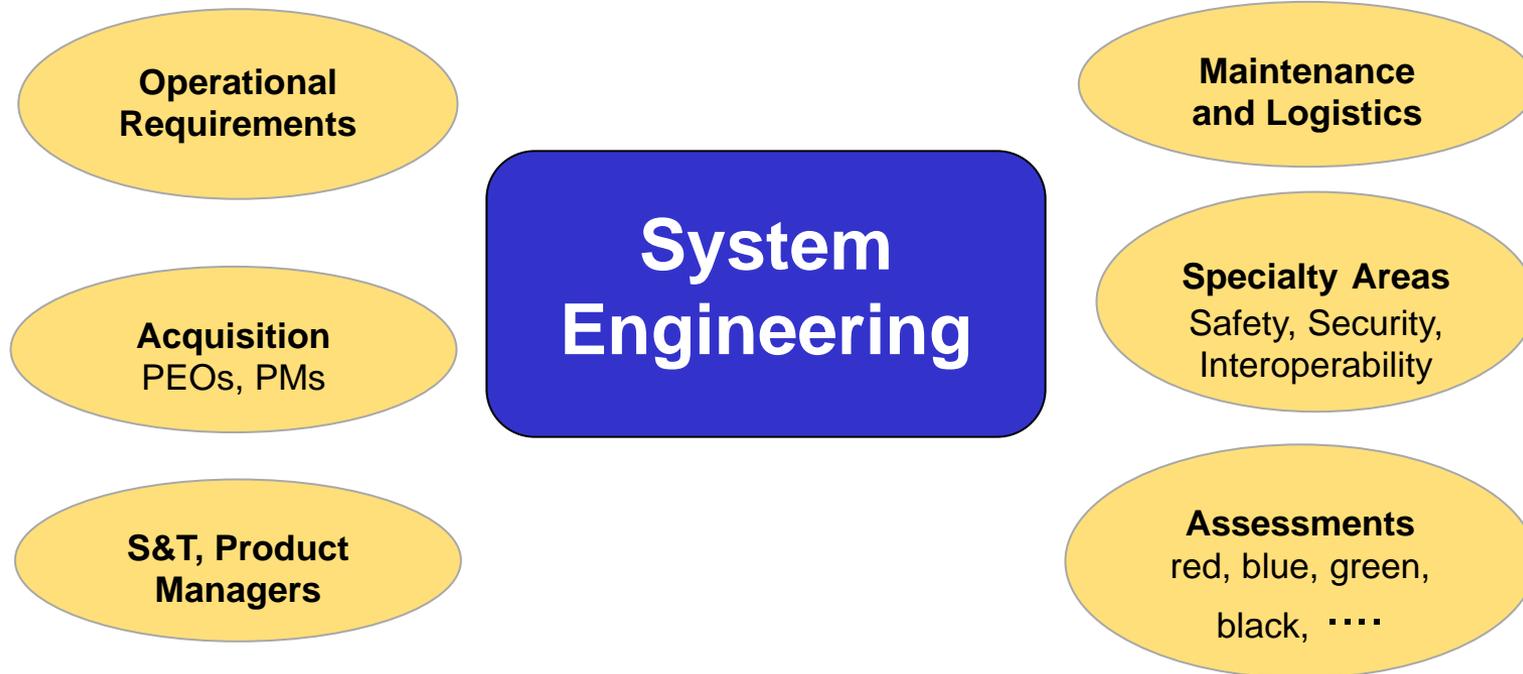
- Complexity
- Performance requirements
- Operational

WS – Weapon System
 C3 – Command, Control, Communication
 JIE – Joint Information Environment
 MPE – Mission Planning Environment
 ICITE - Intelligence Community Information Technology Enterprise

Weapon System(s) can be complex – performance requirements and operational environment must also be considered



Many Stakeholders Involved in the Acquisition Process



The Program Manager, with support from the Lead Systems Engineer, will embed systems engineering in program planning and execution to support the entire system life cycle. DoDI 5000.02



Recurring Challenges

- **PEOs, PMs are reporting that implementation is problematic**
 - Acquisition programs are seeking clear and specific cyber resiliency guidance
- **Services and Agencies, PEOs/Programs, and Industry partners are each working to determine cyber resiliency solutions**
 - No common implementation of rules or principles. Solutions beginning to diverge.
- **Test community continues to identify vulnerabilities**
 - Findings in legacy systems indicate that cybersecurity must be designed in, not tested in, nor patched in
 - Developmental T&E is shifting left, Engineering needs to lay the foundation for the shift

Core Recurring Challenges

**Design
Guidelines**

Implementation

**Engineering
Assessment**



Workshop Series to Facilitate Cross-Cutting Approach



Baseline Community Understanding

Workshop 1
August 2016

Establish a baseline understanding of:

- The landscape of engineering design for cyber resilient weapons systems
- Strategies for implementation and engineering assessments
- Areas needing focus

Determine Framework

Workshop 2
October 2016

Review alternative approaches for:

- Design Guidelines
- Implementation
- Engineering Assessment

Chart Path Forward

Workshop 3
January 2017

Discuss

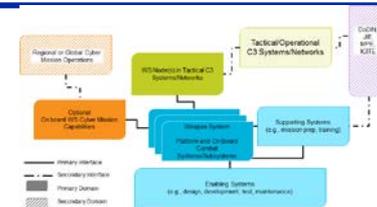
- Institutionalization
- Supporting research
- Partnerships
- Workforce



Design Patterns, Standards and Methods



What system elements or properties do we acquire?



Allocate cybersecurity requirements to the system architecture and design and assess for vulnerabilities. The system architecture and design will address, at a minimum, how the system:

1. Manages access to, and use of the system and system resources;
2. Is configured to minimize exposure of vulnerabilities that could impact the mission, including through techniques such as design choice, component choice, security technical implementation guides and patch management in the development environment (including integration and T&E), in production and throughout sustainment;
3. Is structured to protect and preserve system functions or resources, e.g., through segmentation, separation, isolation, or partitioning;
4. Monitors, detects and responds to security anomalies;
5. Maintains priority system functions under adverse conditions; and
6. Interfaces with DoD Information Network or other external security services.

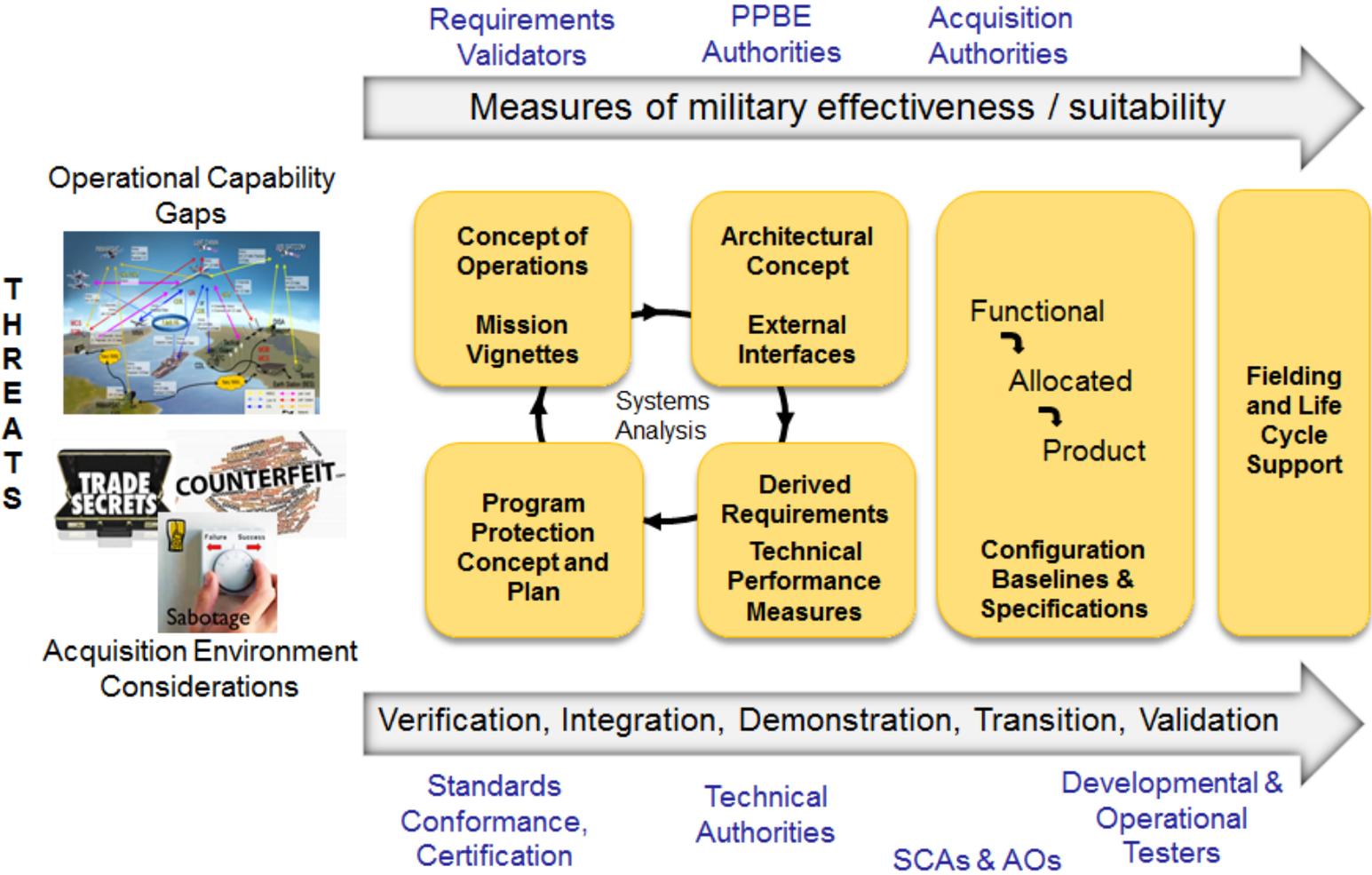
Draft DTM 118 “Cybersecurity in the Defense Acquisition System” establishes a threshold for what to address



Implementation Processes, Roles and Relations



How do we organize and inform design makers?





Engineering Assessment Standards and Methods



How do we know approach works?

Assessing Performance Across the System Life Cycle



Strawman Goals

1. Structured standards and methods to evaluate requirements for testability, traceability, and de-confliction
2. Traceable evidence for appropriate decisions at every level of design
3. Cumulative evidence through RDT&E, DT, and OT – progressive sequential modeling, simulation, and analysis
4. Operational Behavior Prediction and Recovery: real time monitoring, just-in-time prediction, and mitigation of undesired decisions and behaviors
5. Reusable assurance arguments based on previous evidence “building blocks”

-- Adapted from DoD Autonomy TEVV Investment Strategy



Next Steps



Internal Workshops

- Review recommended alternative frameworks and approaches for: **Design Guidelines, Implementation, Engineering Assessment**
- **Develop Way Ahead**
- **Supporting innovation**
- **Partnerships**
- **Empowered Workforce**

Engage Industry

- **NDIA Committees**
- **NDIA Summit (Proposed)**
- **Other Standards Opportunities**