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:** 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

Cyber resilience efforts need to extend across the enterprise

An Opportunity Exists Across the Services to:

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

Army

Air Force
Weapon System Complexity

Notional Representation

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

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
IICITE – Intelligence Community Information Technology Enterprise

WS Node(s) in Tactical C3 Systems/Networks

Regional or Global Cyber Mission Operations

Optional On board WS Cyber Mission Capabilities

Weapon System
Platform and On Board Combat Systems/Subsystems

Supporting Systems (e.g., mission prep, training)

Enabling Systems (e.g., design, development, test, maintenance)

DoDIN, JIE, MPE, ICITE

Primary Interface
Secondary Interface
Primary Domain
Secondary Domain

Weapon System Complexity
Many Stakeholders Involved in the Acquisition Process

Operational Requirements

Acquisition PEOs, PMs

S&T, Product Managers

System Engineering

Maintenance and Logistics

Specialty Areas
Safety, Security, Interoperability

Assessments
red, blue, green, black, ....

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

<table>
<thead>
<tr>
<th>Design Guidelines</th>
<th>Implementation</th>
<th>Engineering Assessment</th>
</tr>
</thead>
</table>
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?

- Requirements Validators
- PPBE Authorities
- Acquisition Authorities

Measures of military effectiveness/suitability

Operational Capability Gaps

Threats

Acquisition Environment Considerations

Concept of Operations
Mission Vignettes
Program Protection Concept and Plan

Architectural Concept
External Interfaces
Derived Requirements
Technical Performance Measures

Functional Allocated Product
Configuration Baselines & Specifications

Fielding and Life Cycle Support

Verification, Integration, Demonstration, Transition, Validation

Standards Conformance, Certification
Technical Authorities
SCAs & AOs

Developmental & Operational Testers
Engineering Assessment Standards and Methods

How do we know approach works?

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