DoD Approach for Engineering Cyber-Resilient Weapon Systems

Melinda Reed
Office of the Under Secretary of Defense for Research and Engineering

SAE Cyber Physical Systems Security Committee Meeting
LMI, Tysons, VA | February 6, 2019
Cybersecurity and Security Is Everyone’s Responsibility

Everyone must take responsibility for cybersecurity from the *earliest research and technology development through system concept, design, development, test and evaluation, production, fielding, sustainment, and disposal*

Scope of cybersecurity includes:

- **Program information** Data about acquisition, personnel, planning, requirements, design, test data, and support data for the system. Also includes data that alone might not be unclassified or damaging, but in combination with other information could allow an adversary to compromise, counter, clone, or defeat warfighting capability

- **Organizations and Personnel** Government program offices, prime and subcontractors, along with manufacturing, testing, depot, and training organizations

- **Networks** Government and Government support activities, unclassified and classified networks, contractor unclassified and classified networks, and interfaces among Government and contractor networks

- **Systems and Supporting Systems** The system being acquired, system interfaces, and associated training, testing, manufacturing, logistics, maintenance, and other support systems
Ensuring Cyber Resilience In Defense Systems and Technologies

**Threat:**
- Adversary who seeks to exploit vulnerabilities to:
  - Acquire program and system information;
  - Disrupt or degrade system performance;
  - Obtain or alter US capability

**Vulnerabilities:**
- Found in programs, organizations, personnel, networks, systems, and supporting systems
- Inherent weaknesses in hardware and software can be used for malicious purposes
- Weaknesses in processes can be used to intentionally insert malicious hardware and software
- Unclassified design information within the supply chain can be aggregated
- U.S. capability that provides a technological advantage can be lost or sold

**Consequences:**
- Loss of technological advantage
- System impact – corruption and disruption
- Mission impact – capability is countered or unable to fight through

**Access points are throughout the acquisition life cycle...**

...and across numerous supply chain entry points
- Government
- Prime, subcontractors
- Vendors, commercial parts manufacturers
- 3rd party test/certification activities
# Program Protection Planning to Improve Cyber Resiliency

## Program Protection & Cybersecurity Policies and Programs

<table>
<thead>
<tr>
<th>Technology</th>
<th>Components</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Protection Activities:</strong></td>
<td><strong>Key Protection Activities:</strong></td>
<td><strong>Key Protection Activities:</strong></td>
</tr>
<tr>
<td>• Anti-Tamper</td>
<td>• Software Assurance</td>
<td>• Classification</td>
</tr>
<tr>
<td>• Defense Exportability Features</td>
<td>• Hardware Assurance/Trusted Foundry</td>
<td>• Export Controls</td>
</tr>
<tr>
<td>• CPI Protection List</td>
<td>• Supply Chain Risk Management</td>
<td>• Information Security</td>
</tr>
<tr>
<td>• Acquisition Security Database</td>
<td>• Anti-counterfeits</td>
<td>• Joint Acquisition Protection &amp; Exploitation Cell (JAPEC)</td>
</tr>
</tbody>
</table>

**Goal:** Prevent the compromise or loss of critical technologies

**Goal:** Protect critical system components (hardware, software) from malicious exploitation

**Goal:** Ensure critical system and program data is protected from adversary collection

---

**Protecting Warfighting Capability Throughout the Lifecycle**

Policies, guidance and white papers are found at our initiatives site: [http://www.acq.osd.mil/se/initiatives/init_pp-sse.html](http://www.acq.osd.mil/se/initiatives/init_pp-sse.html)
Weapon System Ecosystem
From Concept to Sustain and Maintain

Defining Themes
- WS Characteristics
- WS Quality Properties
- WS Engineering Methods
- WS Types

Weapon Systems
- Level of Rigor
- Engineering Methods, Processes, Tools
- Configurations, States, Modes, Transitions
- Networked, Distributed
- Adaptive, Predictive, Intelligent
- Manual, Automated, Semi-Autonomous, Autonomous
- Real Time, Event-driven, Time Synchronized
- Execution, Size, Weight, Power, Environment, Connectivity
- Instrumentation, Sensors
- Performance, Interoperability, Reliability, Resilience, Safety, Security, Survivability
- Disruptions
- Malicious
- Non-malicious
- Dependability, Fit for Purpose, Nuclear Surety
- Certifications, Risk Acceptance
- Scalability and Complexity Management
- Modularity, Composability, Synthesis
- Specification
- Architecture, Design
- Modeling, Analysis
- Verification, Validation
- Maximum Reasonable Assurance
- Self-sufficient Strategic or Tactical Systems
- What confidence do we have in our
  - Methodologies
  - Risk Decisions
  - Results of design
  - Analysis

Weapon Systems Deliver Lethal Force with the Intent to Cause Harm

SAE CPS Meeting
Feb 2019

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-1517 applies. Distribution is unlimited.
Allocate cybersecurity and related system security requirements to the system architecture; design and assess for vulnerabilities. The system architecture and design will address, at a minimum, how the system:

- **Manages access** to and use of the system and system resources
- Is structured to **protect and preserve system functions** or resources, (e.g., through segmentation, separation, isolation, or partitioning)
- 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.
- **Monitors, detects, and responds** to security anomalies.
- **Maintains priority system** functions under adverse conditions; and
- **Interfaces** with DoD Information Network (DoDIN) or other external security services

---

**Key Design Activities to Mitigate Cybersecurity Risks to the System**
Design Order of Precedence (MIL-STD-882E)

1. Eliminate hazards through design selection
   - Ideally, the hazard should be eliminated by selecting a design or material alternative that removes the hazard altogether

2. Reduce risk through design alteration
   - Design changes that reduce the severity and/or the probability of the mishap potential caused by the hazard(s)

3. Incorporate engineered features or devices
   - Reduce the severity or the probability of the mishap potential caused by the hazard(s) using engineered features or devices
   - In general, engineered features actively interrupt the mishap sequence and devices reduce the risk of a mishap

4. Provide warning devices
   - Detection and warning systems to alert personnel to the presence of a hazardous condition or occurrence of a hazardous event.

5. Incorporate signage, procedures, training, and PPE
   - Incorporate signage, procedures, training, and personal protective equipment (PPE), along with appropriate warnings and cautions

“When a hazard cannot be eliminated, the associated risk should be reduced to the lowest acceptable level within the constraints of cost, schedule, and performance”

MIL-STD 882E System Safety
Cybersecurity Requirements Derivation

Security requirements are the by-product of engineering requirements activities

Traceability demonstrates the basis for the existence of the requirements

Validated Baselines reflect requirements-based agreement at key “checkpoints”, such as
- Functional Baseline: basis for contracting and controlling the system design.
- Allocated Baseline: performance requirements for each configuration item of the system
- Product Baseline: detailed design specification for system elements

Validation of the Implementation
Validation demonstrates that the implementation satisfies the stakeholder requirements.
“Did we build the right thing?”

Decomposition and derivation refines requirements to enable implementation.

Verification demonstrates that the implementation satisfies the design requirements.
“Did we build it right?”

Implementation of the Design

Security requirements are the by-product of engineering requirements activities
Weapon System Assurance

- Claims are stated relative to
  - Design intent (the norm)
  - Cases of disruption and subversion (deviation from norm)

- Insufficient confidence translates to risk
  - DoD MIL-STD-882E
  - NASA System Safety

Assurance is: Justified confidence that a claim has been or will be achieved [IEEE 15026]
Loss-Driven Engineering Approach

- Scope of loss includes:
  - Death, injury, or occupational illness
  - Damage to or loss of equipment or property
  - Damage to or loss of capability, function, or process
  - Damage to the environment
  - Damage to or loss of data or information

- Loss is the basis for security activities and judgments
  - Security protection needs arise in direct response to a loss effect
    - Avoid and prevent
    - Minimize the extent and/or duration of
    - Recover from

Drive Engineering into Cybersecurity
Security Requirements Derivation
Analysis Opportunities

**Need**
- Capability needs, loss concerns, acceptance
  - Mission
  - System
  - Regulatory, statutory, certification, policy
  - Assurance

**Structure**
- System architecture, design, interfaces, interconnections
  - Exposure, hazards, vulnerabilities
  - Critical functions
    o Mission
    o System
    o Security
    o Safety

**Adversity**
- Loss scenarios
  - Causal factors
    o Attack, subversion
    o Error, fault, failure
    o Abuse, misuse
  - Conditions
    o Exposure, hazard, vulnerability
  - Adversarial threat informed
    o Threat data-dependent
    o Threat data-independent

**Design**
- System function, interfaces, data, interconnections
  - Functional, data, control flow interactions
  - Interactions not anticipated by the system requirements
  - Exposure, hazards, vulnerabilities

**Implementation of the Design**
Engineering Requirements Rules to Translate Security Controls

Derive Security Requirements:

- To satisfy the following security protection objectives:
  - Protect advanced technology from loss due to adversarial activity
  - Protect component capability from loss due to adversarial activity
  - Protect information from loss due to adversarial/unauthorized activity

- To reduce exposure and vulnerabilities:
  - Introduced by architecture, design, and implementation decisions
  - Introduced by hardware and software
  - Identified by system functional security analysis
  - Identified by system data security analysis
  - Identified by system interface security analysis

- That impose constraints on system requirements driven by architecture, design, and implementation decisions
- That result in architecture, design, and implementation decisions

Translation of Security Controls:

- Based on requirements in a baseline
  - Requirements recorded in a baseline have stakeholder consensus and are subject to strict configuration control

- Must be validated as constituting an accurate and complete representation of its basis
  - This ensures that the translation does not add or remove anything relative to its basis

- Must be traced to its requirements basis
  - This ensures that any change to the requirements basis can be correlated to a change in the translation

- Must be subjected to formal change control process that addresses:
  - A change in the requirements basis that drives a change in the translation
  - Identification of an unacceptable difference between the requirements basis and the translation
  - Identification of an issue when using the translation for its intended purpose

Equivalence to the translation source must be maintained
Summary

- CPS assurance and resilience is a serious challenge
  - This is different than traditional cybersecurity, and includes physical effects and the possibility of physical attacks
  - We need to move beyond network security controls to achieve cyber resilient physical systems

- Measurable assurance of CPS software and hardware is needed
  - Hardware is a challenge; difficult to find vulnerabilities, and patches are not simple in-field updates
  - Security must come from a root-of-trust
  - Comprehensive solutions must be based in industry-wide standards

- Opportunities for government, industry and academia to engage:
  - We see a unique opportunity to align common interests in security and assurance
  - Military, automotive, communications, finance, medical sectors all require assurance
  - Partnered with industry, DoD will promote security and assurance standards as differentiators over foreign products for critical industrial sector applications such as autonomous vehicles, secure data, and medical devices
  - DoD, aligned with Government Agency partners, is intent on public-private partnership, fostering commercial and government alliances to maintain the U.S. as the global source for hi-end, secure and reliable microelectronics and software
DoD Research and Engineering Enterprise
Solving Problems Today – Designing Solutions for Tomorrow

DoD Research and Engineering Enterprise
https://www.acq.osd.mil/chieftechnologist/

Defense Innovation Marketplace
https://defenseinnovationmarketplace.dtic.mil

Twitter
@DoDInnovation
For Additional Information

Melinda Reed
Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E))
571.372.6562 | melinda.k.reed4.civ@mail.mil