



Cybersecurity in Acquisition

Kristen J. Baldwin

**Acting Deputy Assistant Secretary of Defense
for Systems Engineering (DASD(SE))**

**Federal Cybersecurity Summit
September 15, 2016**



Cybersecurity in Acquisition



- **Acquisition program activities must take responsibility for cybersecurity from earliest research and technology development through system concept, design, development, test and evaluation, production, fielding, sustainment, and disposal**
- **Scope of program 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 classified 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

Cybersecurity is a requirement for all DoD programs



Ensuring Cyber Resilience in Defense Systems



- **Threat**

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

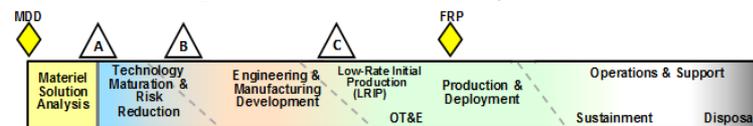
- **Vulnerabilities**

- 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
- US 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 lifecycle...



...and across numerous supply chain entry points

- Government
- Prime, subcontractors
- Vendors, commercial parts manufacturers
- 3rd party test/certification activities



Spectrum of Supply Chain Risks



Quality Escape

Product defect/ inadequacy introduced either through mistake or negligence during design, production, and post-production handling resulting in the introduction of deficiencies, vulnerabilities, and degraded life-cycle performance.

Reliability Failure

Mission failure in the field due to environmental factors unique to military and aerospace environment factors such as particle strikes, device aging, hot-spots, electro-magnetic pulse, etc.

Fraudulent Product

Counterfeit and other than genuine and new devices from the legally authorized source including relabeled, recycled, cloned, defective, out-of-spec, etc.

Malicious Insertion

Intentional insertion of malicious hard/soft coding, or defect to enable physical attacks or cause mission failure; includes logic bombs, Trojan kill switches, backdoors for unauthorized control and access to logic and data.

Reverse Engineering

Unauthorized extraction of sensitive intellectual property using reverse engineering, side channel scanning, runtime security analysis, embedded system security weakness, etc.

Information Losses

Stolen data provides potential adversaries extraordinary insight into US defense and industrial capabilities and allows them to save time and expense in developing similar capabilities.

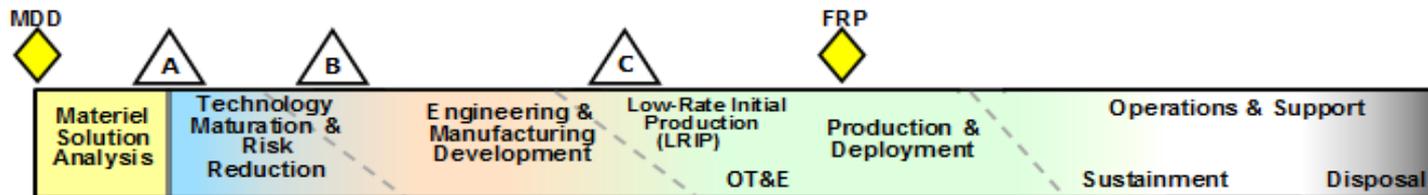
DoD Program Protection focuses on risks posed by malicious actors



Program Protection in DoDI 5000.02 Acquisition Policy



- **DoDI 5000.02 requires Program Managers to employ system security engineering practices and prepare a Program Protection Plan (PPP) to manage the security risks to the program and system elements that are vulnerable and can be exposed to targeting**
 - Critical Program Information
 - Mission-critical functions and critical components
 - Information about the program and within the system
- **PPPs are required at all major milestones**
 - PPPs inform program acquisition strategies, engineering, and test and evaluation plans
 - PMs incorporate appropriate PPP requirements into solicitations





What Are We Protecting?

Program Protection & Cybersecurity

http://www.acq.osd.mil/se/initiatives/init_pp-sse.html

DoDI 5000.02

DoDM 5200.01, Vol. 1-4

DoDM 5200.45

DoDI 8500.01

DoDI 5200.39

DoDI 5200.44

DoDI 5230.24

DoDI 8510.01

Technology

What: A capability element that contributes to the warfighters' technical advantage (CPI)

Key Protection Measure Types:

- Anti-Tamper
- Exportability Features

Goal: Prevent the compromise and loss of CPI

Components

What: Mission-critical functions and components

Key Protection Measure Types:

- Software Assurance
- Hardware Assurance/Trusted Microelectronics
- Supply Chain Risk Management
- Anti-counterfeits

Goal: Protect key mission components from malicious activity

Information

What: Information about the program, system, designs, processes, capabilities and end-items

Key Protection Measure Types:

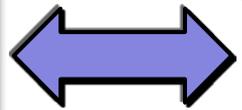
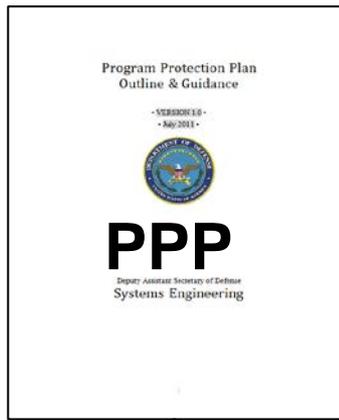
- Classification
- Export Controls
- Information Security

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

Protecting Warfighting Capability Throughout the Lifecycle



Program Protection Relationship to Other Formal Acquisition Activities



Systems Engineering Plan

- Incorporation into technical baselines
- SSE entry and exit criteria in SE tech reviews
- SSE as a design consideration
- Technical risks and mitigation plans

T&E Master Plan

- Data needed to ascertain cybersecurity requirements are met
- Cooperative Vulnerability Identification and Penetration Assessments
- Adversarial Assessments

Acq Strategy

- Trusted supplier requirements
- Acquisition regulations (Safeguarding Covered Defense Information, Counterfeits, etc.)

Anti-Tamper Plan

**Cyber-security Strategy/
RMF Security Plan**

Tailored to specific program situations



Contract Regulation for Safeguarding Covered Defense Information



DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

- 2nd interim rule published December 30, 2015, to provide contractors with additional time to implement NIST 800-171 security requirements

Purpose

- Establish minimum requirements for contractors and subcontractors to safeguard DoD unclassified covered defense information and report cyber incidents on their contractor owned and operated information systems

Requires Contractors to

- Flow down only to Subcontractors where their efforts will involve covered defense information or where they will provide operationally critical support
- Fully comply with security requirements in the NIST SP 800-171, "Protecting Controlled Unclassified Information in **Nonfederal** Information Systems and Organizations" NLT Dec 31, 2017
- Report cyber incident and compromises affecting covered defense information
- Submit malware that they are able to discover and isolate in connection with a reported cyber incident
- Support DoD damage assessment as needed

Final rule anticipated to be published in Fall 2016



Joint Federated Assurance Center (JFAC)



- **Federation of DoD software and hardware assurance (SwA/HwA) capabilities**
 - Support programs in addressing current and emerging threats and vulnerabilities
 - Facilitate collaboration across the Department and throughout the lifecycle of acquisition programs
 - Maximize use of available resources
 - Assess and recommend capability and capacity gaps to resource
- **Seek innovation in SW and HW inspection, detection, analysis, risk assessment, and remediation tools and techniques to mitigate risk of malicious insertion**
 - R&D is key component of JFAC operations
 - Focus on improving tools, techniques, and procedures for SwA and HwA to support programs
- **Federated Organizations**
 - Army, Navy, AF, NSA, DMEA DISA, NRO, MDA laboratories and engineering support organizations; and Department of Energy

JFAC mission is to support programs with SwA and HwA needs



Summary



- **Cybersecurity is an essential element of acquisition, engineering, test, and sustainment activities**
 - We will embed cybersecurity risk mitigation activities into the acquisition program lifecycle
- **We must bring to bear policy, tools, and expertise to enable cyber resiliency in our systems**
 - Translate IT and network resiliency to weapon system resiliency
 - Establish security as a fundamental discipline of systems engineering
- **Opportunities for all of government, industry and academia to engage:**
 - Continue R&D efforts to determine technological approaches to reduce risk
 - Develop engineering and design methods, standards, and tools to enable policy implementation
 - Develop use case scenarios to help educate and train our community