Cybersecurity in Program Acquisition

Kristen J. Baldwin

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

NDIA Cybersecurity for Advanced Manufacturing Joint Working Group

August 18, 2016

Cybersecurity in Acquisition

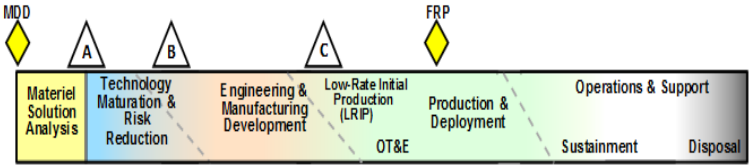
- **Acquisition program activities must take responsibility for cybersecurity from earliest research and technology development through system concept, design, development, test and evaluation, production, fielding, sustainment, and disposal**
- **Scope of program cybersecurity includes:**
  - Program information Data about acquisition, personnel, planning, requirements, design, test data and support data for the system. Also includes data that alone might not be 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

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

The intentional insertion of malicious hard/soft coding, or defect to enable physical attacks or cause mission failure; includes logic bombs, Trojan 'kill switches' and 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

What Are We Protecting?

Program Protection & Cybersecurity

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:

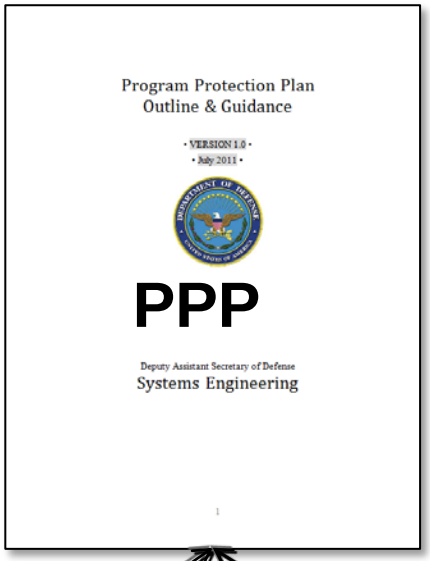
- Classification
- Export Controls
- Information Security

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

Protecting Warfighting Capability Throughout the Lifecycle

Policies, guidance and white papers are found at our initiatives site: http://www.acq.osd.mil/se/initiatives/init_pp-sse.html

Program Protection Relationship to Key Acquisition Activities



SEP

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

TEMP

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

Acq Strat/ Contract

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

AT Plan

Cyber-security Strategy/ RMF Security Plan

Tailor to specific program situations

Excerpt from University of Virginia System-Aware Cybersecurity Presentation*

Illustrative Examples of Illogical Control

- Navigation waypoint changed, but no corresponding communication received by UAV
- Automobile sensor shows distance between cars reducing, but collision avoidance control system speeds up the following car
- Selected material to create part of a 3D printed object does not match what the executing design calls for
- Mode of Fire Control System changed, but no touch screen input from operator

3D Printer YouTube Video

***Source: Dr. B. Horowitz, University of Virginia, PowerPoint presentation, July 2016**

Intelligence & Counterintelligence Support to Program Protection

- **Effective program protection planning is enabled by intelligence and counterintelligence (CI) support**
  - Threat and CI information can help programs determine what potential protection measures would be most effective for the program's circumstances
  - Program managers should expect to be informed by intelligence and CI throughout the acquisition lifecycle

- **Key information provided by Intelligence and CI sources**
  - Cyber reports
  - Threat reports and assessments
  - Foreign collection methods
  - Suspicious contact reports received from cleared industry
  - Insider threats
  - NISPOM related reporting

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. Publication of final rule is planned in the 3rd/4th QTR FY16.

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

The Program Office should pay particular attention to DoD unclassified information provided to, and developed by, the contractor

Summary

- **Continue R&D efforts to determine technological approaches to address risk**
- **Develop specific guidance to enable policy implementation**
- **Develop use case scenarios to help educate and train our community**

Rely on expertise from government, industry, and academia to chart a path forward