Engineering Cyber Resilient Weapon Systems

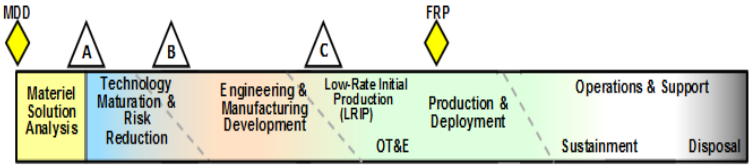
Melinda K. Reed
Office of the Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE))

20th Annual NDIA Systems Engineering Conference
Springfield, VA | October 25, 2017

Ensuring Cyber Resilience in Defense Acquisition 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

Key Protection Activities to Improve Cyber Resiliency

Program Protection & Cybersecurity

DoDI 5000.02, Enclosures 3 & 14

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 (Critical Program Information (CPI))

Key Protection ActivityU

- Anti-Tamper
- Defense Exportability Features
- CPI Protection List
- Acquisition Security Database

Goal: Prevent the compromise and loss of CPI

Components

What: Mission-critical functions and components

Key Protection Activity:

- Software Assurance
- Hardware Assurance/Trusted Foundry
- Supply Chain Risk Management
- Anti-counterfeits
- Joint Federated Assurance Center (JFAC)

Goal: Protect key mission components from malicious activity

Information

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

Key Protection Activity:

- Classification
- Export Controls
- Information Security
- Joint Acquisition Protection & Exploitation Cell (JAPEC)

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

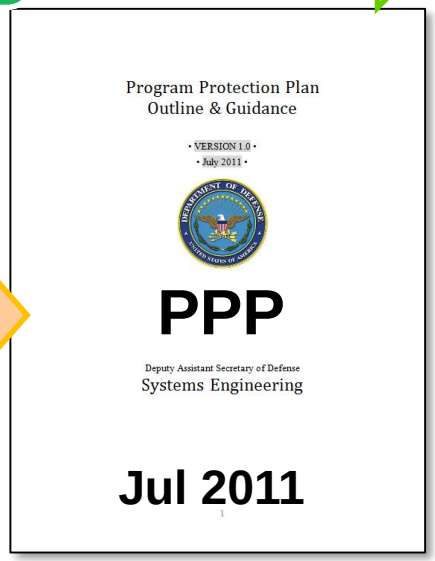
Program Protection and Cybersecurity Relationship to Key Acquisition Activities

COCOMS
- IPLS
- S&T IPLs

JCIDS
- Operational Needs
- Performance Criteria
- Operational Threats

Threats
- CI
- Intel

- TTRA
- ITA
- DIA TAC
- STAR
- Others



- **Security Classification Guide**
- **Counterintelligence Support Plan**
- **Criticality Analysis**
- **Anti-Tamper Plan (If Applicable)**
- **Cybersecurity Strategy**

Acq Strat/ Contract
- Trusted supplier requirements
- Acquisition regulations (Security, Safeguarding Covered Defense Information, Counterfeits, etc.)
- Foreign/International Engagement

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 Assessments
- Adversarial Assessments

LCSP
- Informs full life cycle protection activities for the program
- Lists critical components that require attention

Program Protection and Cybersecurity Considerations Are Integrated In All Aspects of Acquisition

Cybersecurity Is Everyone's Responsibility

Significant Efforts by Military Departments to Address Cybersecurity

Each MILDEP is moving forward to meet its organizational needs

Navy

Army

Air Force

An Opportunity Exists Across the Services to:

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

National Cyber Security Summit
8/7/2017 | Page-4

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-1517 applies. Distribution is unlimited.

Cybersecurity is not just an IT / network issue. We must translate Cyber IT / Network practices, standards, etc. into physical system requirements.

Recommendations from Defense Science Board

Summary of Recommendations

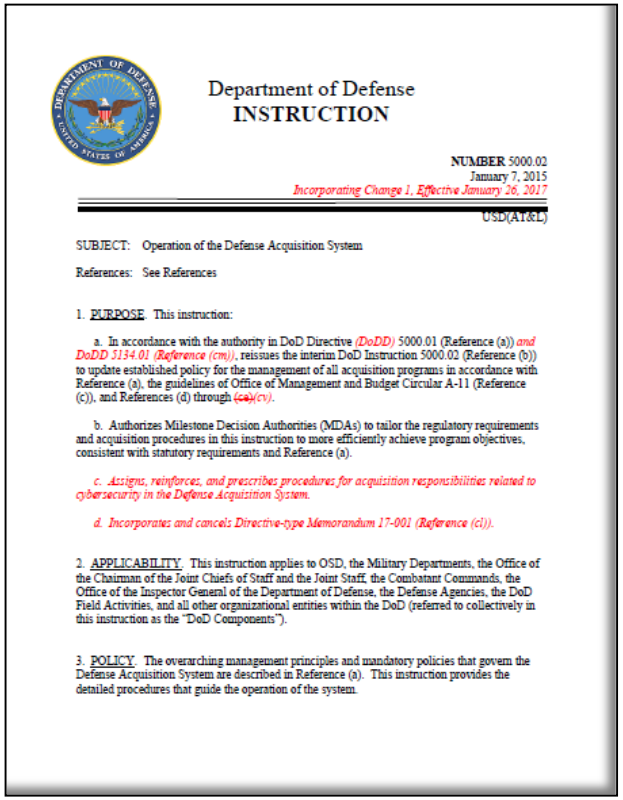
Five categories for improvement

1. Understand supply chain risk
   - Expand vulnerability assessments
2. Mitigate potential vulnerabilities
   - Improve detection and reporting
3. Approach acquisition differently
   - Enhance program protection planning
   - Improve timeliness of supplier vetting
   - Improve system engineering
   - Use JFAC and JAPEC effectively
   - Consider cybersecurity impact of COTS products and components
4. Support life-cycle operations
   - Establish sustainment PPPs for fielded systems
   - Collect and act on parts vulnerabilities
5. Pursue technical solutions

DSB TASK FORCE ON CYBER SUPPLY CHAIN 11

Publicly-released report published Feb 2017
Available at: https://www.acq.osd.mil/dsb/reports/2010s/DSBCyberSupplyChain_ExecSummary_Distribution_A.PDF

Cybersecurity in Acquisition



Department of Defense
INSTRUCTION

NUMBER 5000.02
January 7, 2015
Incorporating Change 1, Effective January 26, 2017
USD(AT&L)

SUBJECT: Operation of the Defense Acquisition System

References: See References

1. PURPOSE. This instruction:

a. In accordance with the authority in DoD Directive *(DoDD)* 5000.01 (Reference (a)) *and DoDD 5134.01 (Reference (cm))*, reissues the interim DoD Instruction 5000.02 (Reference (b)) to update established policy for the management of all acquisition programs in accordance with Reference (a), the guidelines of Office of Management and Budget Circular A-11 (Reference (c)), and References (d) through ~~(ca)~~*(cv)*.

b. Authorizes Milestone Decision Authorities (MDAs) to tailor the regulatory requirements and acquisition procedures in this instruction to more efficiently achieve program objectives, consistent with statutory requirements and Reference (a).

c. Assigns, reinforces, and prescribes procedures for acquisition responsibilities related to cybersecurity in the Defense Acquisition System.

d. Incorporates and cancels Directive-type Memorandum 17-001 (Reference (cl)).

2. APPLICABILITY. This instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

3. POLICY. The overarching management principles and mandatory policies that govern the Defense Acquisition System are described in Reference (a). This instruction provides the detailed procedures that guide the operation of the system.

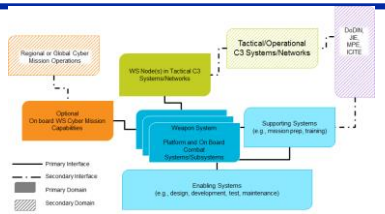
Acquisition workforce must take responsibility for cybersecurity from the earliest research and technology development through system concept, design, development, test and evaluation, production, fielding, sustainment, and disposal

Scope of program cybersecurity includes:

- Program information Data about acquisition, personnel, planning, requirements, design, test data, and support data for the system.
- Organizations and Personnel Government program offices, prime and subcontractors, along with manufacturing, testing, depot, and training organizations
- Networks Government, Government support activities, and contractor owned and operated unclassified and classified networks
- Systems and Supporting Systems The system being acquired, system interfaces, and associated training, testing, manufacturing, logistics, maintenance, and other support systems

Codified in DoDI 5000.02, Enclosure 14, Jan 26, 2017

Design for Cyber Threat Environments



Activities to mitigate cybersecurity risks to the system include:

- **Allocate cybersecurity and related system security 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 structured to protect and preserve system functions or resources, (e.g., through segmentation, separation, isolation, or partitioning).
  3. 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.
  4. Monitors, detects and responds to security anomalies.
  5. Maintains priority system functions under adverse conditions; and
  6. Interfaces with DoD Information Network (DoDIN) or other external security services.

DoDI 5000.02, Enclosure 14 establishes a threshold for what to address

Implementation: Engineering Cyber Resilient Workshops

Workshop 1 Findings
1. Requirements derivation is a challenge area
2. Require clarity on Risk Acceptance
3. Assessments should be integrated with and driven by SE Technical Reviews

Workshop 2 Findings/Actions
1. Definitions, Taxonomy & Standards Framework
2. Knowledge Repository
3. Consolidated Risk Guide
4. Assessment Methods
5. Needs Forecasting
6. Industry Outreach

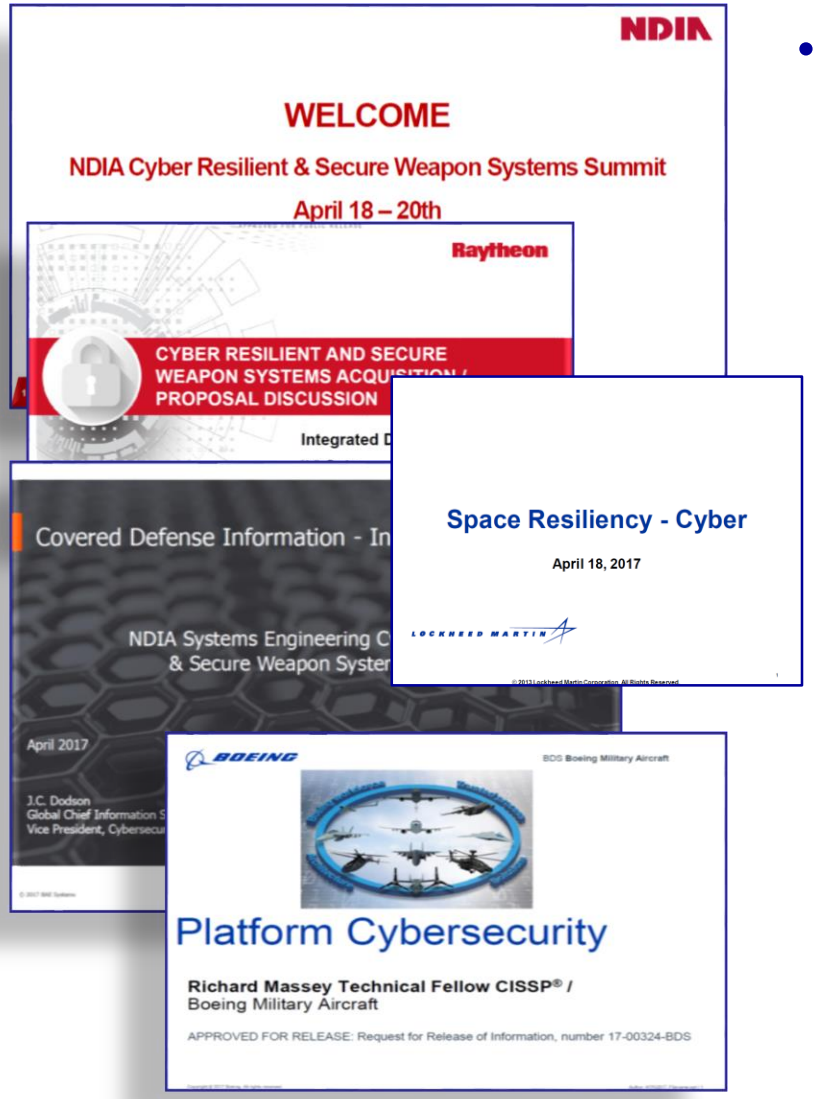
Workshop 3 Findings/Actions
1. Establish DAU CRWS CoP; facilitate definitions, taxonomy standards
2. Develop Risk, Issues, & Opportunities engineering cyber appendix
3. Align assessment approaches
4. Explore S&T opportunities
5. Address Workforce needs
6. Industry Outreach

Workshop 4 (Aug 2017)
Theme: Changing the Culture / Method: Leverage existing engineering approaches

- **Technical Performance Measures and Metrics**
  - Develop Engineering Guidebook
  - Identify TPMs affected by Cyber actions
- **System Engineering Technical Reviews**
  - Validate that existing SETR criteria is sufficient for secure and resilient system design and sustainment
- **Leveraging System Safety**
  - Identify threshold of acceptable risk
  - Quantify the security-driven risk
- **Cyber Resilient Software**
  - Establish an outline to identify engineering design and analysis considerations for the software in secure and resilient weapon systems
- **Risk, Issues, and Opportunity (RIO) Guide**
  - Develop appendix for Cyber Risk

Addressing Recurring Challenges:
Design Guidelines, Implementation, Engineering Assessment

NDIA SE Cyber Resilient Summit and Secure Weapon System Summit
April 18-20, 2017



- **Initial Industry Outreach Aligned with CRWS Series**
  - Industry implementation lessons learned
  - Emphasized need for consistency across communities
  - Discussed approaches to risk acceptance
  - Offered thoughts on implementing safeguards on manufacturing floor
  - Offered areas for improvements to methods, standards, processes, and techniques for cyber resilient & secure weapon systems
  - Thoughts on addressing sustainment challenges

Joint Federated Assurance Center: Software and Hardware Assurance

- **JFAC is a federation of DoD software and hardware assurance (SwA/HwA) capabilities and capacities to:**
  - Provide SW and HW inspection, detection, analysis, risk assessment, and remediation tools and techniques to PM's to mitigate risk of malicious insertion
- **JFAC Coordination Center is developing SwA tool and license procurement strategy to provide:**
  - Enterprise license agreements (ELAs) and ELA-like license packages for SwA tools used by all DoD programs and organizations
    - Initiative includes coordinating with NSA's Center for Assured Software to address potential concerns about the security and integrity of the open source products
  - Automated license distribution and management system usable by every engineer in DoD and their direct-support contractors
- **Lead DoD microelectronic hardware assurance capability providers**
  - Naval Surface Warfare Center Crane
  - Army Aviation & Missile Research Development and Engineering Center
  - Air Force Research Lab

Moving Towards Full Operational Capability
JFAC Portal: https://jfac.army.mil/ (CAC-enabled)

US Microelectronics Security and Innovation

Strategic National Security Applications

Secure IoT

Financial & Data Analytics

Autonomous Systems + AI

Robust + Agile Communicators

Commercial Space

Biomedical

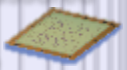
Strategic National Economic Competitiveness Applications

Proactive Awareness & Security

- Supply Chain track
- Proactive Authorities
- Intelligence & CI

Access & Assurance

- Secure Design
- IP, EDA, experts
- Foundry assured Access
- Prototype Demonstrations



Enabling Manufacturing

- SoP Back-end parity with SotA
- SotA on 200mm tools at SoP
- Mini fabrication for high-mix low vol.

Incentives & Market Growth

- Acquisition reform & incentives
- Tax, policy, regulation reform
- R&D and domestic fab incentives

Strategic Alliances

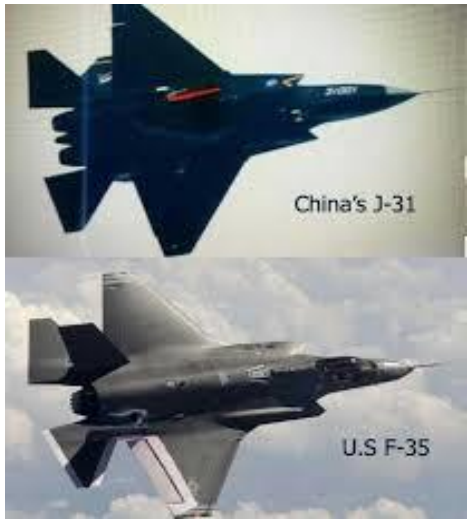
- Cooperative R&D
- Trade & FMS
- Americas
- Europe
- Asia partners

Disruptive Research & Development

Materials, devices, circuits | **Architectures** | **Design tools for Complexity**

Experts, Infrastructure, Venture Capital | **Science & Technology, R&D**

These Are Not Cooperative R&D Efforts



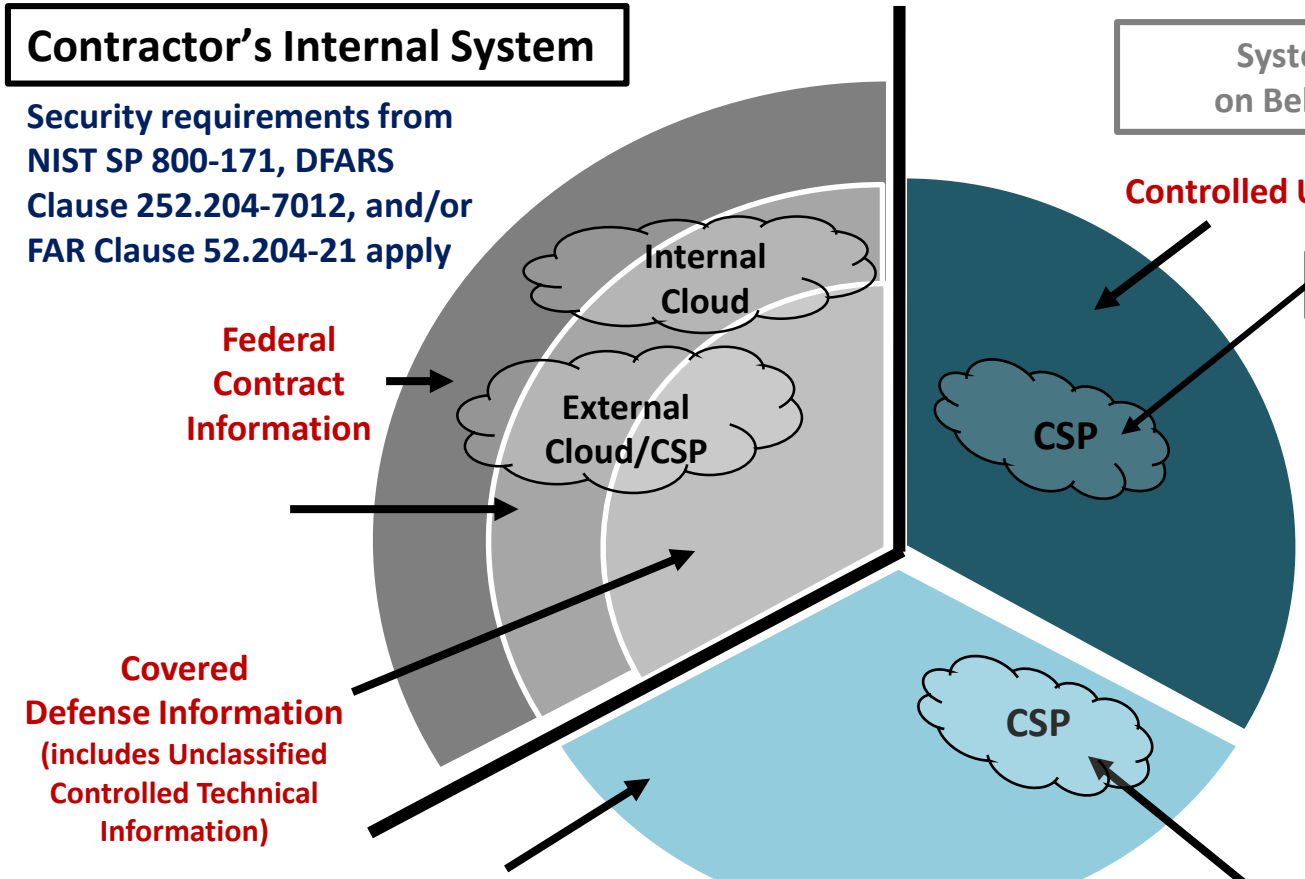
U.S. HUMVEE

China's Dongfeng EQ2050

U.S. Reaper

China's Yìlóng-1

Protecting DoD's Unclassified Information



Contractor's Internal System

Security requirements from NIST SP 800-171, DFARS Clause 252.204-7012, and/or FAR Clause 52.204-21 apply

Federal Contract Information

Covered Defense Information (includes Unclassified Controlled Technical Information)

Controlled Unclassified Information

System Operated on Behalf of the DoD

Controlled Unclassified Information

Cloud Service Provider

When cloud services are used to process data on the DoD's behalf, DFARS Clause 252.239-7010 and DoD Cloud Computing SRG apply

DoD Information System

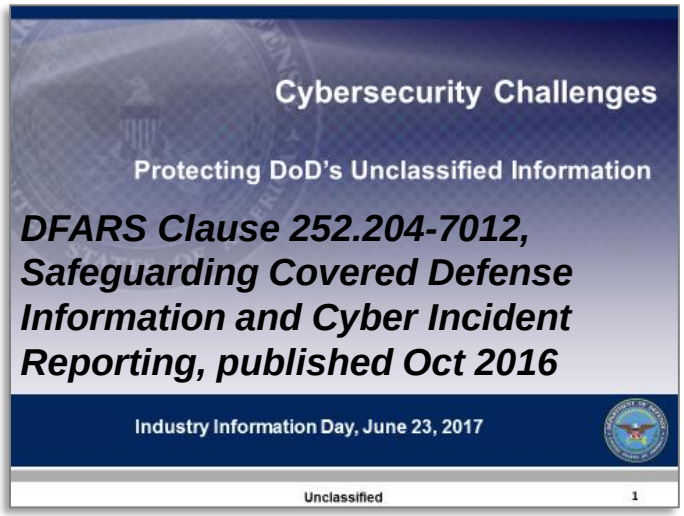
Security requirements from CNSSI 1253, based on NIST SP 800-53, apply

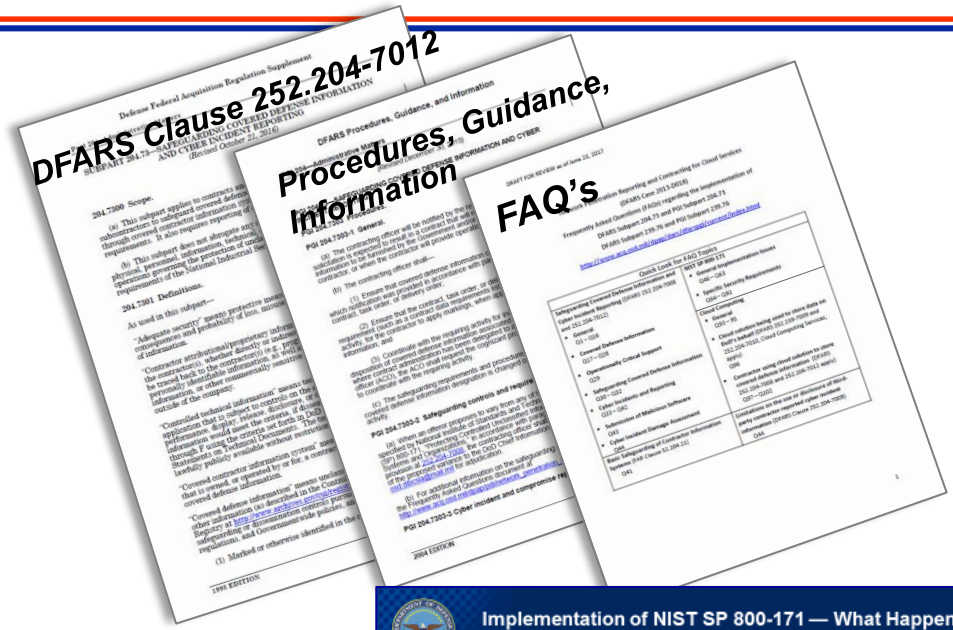
DoD Owned and/or Operated Information System

Cloud Service Provider

When cloud services are provided by DoD, the DoD Cloud Computing SRG applies

Contract Regulation for Safeguarding Covered Defense Information



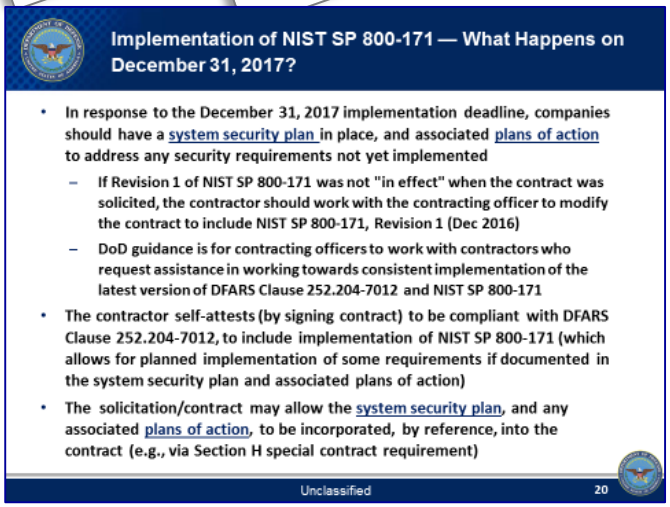


Purpose:

- 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

Contractor is required to:

- Implement NIST SP 800-171 Controls for unclassified non-Federal Information Systems
- Report cyber incidents affecting covered defense information
- Submit malware when discovered
- Submit media when requested by DoD
- Flow down Clause to subcontractors when covered defense information is on subcontractor networks



Cybersecurity in DoD Acquisition Regulations page:

http://dodprocurementtoolbox.com/ for Related Regulations, Policy, Frequently Asked Questions, and Resources

Cybersecurity for Advanced Manufacturing Systems

Operational Technology Environment

NDIA

ICS systems are long-lived capital investments (15-20 year life)

"Production mindset" with little tolerance for OT down time

Nascent cybersecurity awareness and limited workforce training

Manufacturing jobs bring executable code into system

Technical data flowing through the system is highly valued by adversaries

Challenges in DoD and the Manufacturing Environment are Cross Cutting

Cyber Community of Interest Roadmap Key Capability Areas

Embedded, Mobile, and Tactical Systems (EMT)

Assuring Effective Missions	Assess and control the cyber situation in mission context
Agile Operations	Dynamically reshape cyber systems as conditions/goals change, to escape harm

Resilient Infrastructure	Withstand cyber attacks, and sustain or recover critical functions
Trust	Establish known degree of assurance that devices, networks, and cyber-dependent functions perform as expected, despite attack or error

Cyber Modeling, Simulation, and Experimentation (MSE)

(MSE & EMT) cross-cutting areas in analysis of Joint Chiefs of Staff Cyber Gaps

Program Protection and Cybersecurity in Acquisition Workforce Training

- **ACQ 160: Program Protection Overview**
  - Distance learning (online); ~3 days
  - Provides an overview of program protection concepts, policy and processes, includes overview of DFARS 252.204-7012
  - Intended for the entire Acquisition Workforce, with focus on ENG and PM
  - **Course deployed on DAU website on 15 Aug 2016**

- **ENG 260: Program Protection Practitioner Course (est. deployment Summer 2018)**
  - Hybrid (online and in-class); ~1 week
  - Intended for Systems Engineers and System Security Engineers
  - Focuses on application of program protection concepts and processes, including PM responsibilities for implementing DFARS 252.204-7012

Defense Acquisition University

Effective program protection planning requires qualified, trained personnel

Summary

- **Each system is different; approaches must be tailored to meet the requirement, operational environment and the acquisition**
  - 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 system security as a fundamental discipline of systems engineering

- **Opportunities for government, industry and academia to engage:**
  - How can we thoughtfully integrate cybersecurity practices in existing standards for embedded software?
  - How can we better integrate program protection and cybersecurity risks into program technical risks?
  - Can we establish system requirements that restricts a system to a set of allowable, and recoverable behaviors?
  - How can we carefully engineer stronger resiliency in systems that are being modernized?

Systems Engineering: Critical to Defense Acquisition










PP/SSE Initiatives Webpage
http://www.acq.osd.mil/se/initiatives/init_pp-sse.html

JFAC Portal
https://jfac.army.mil/ (CAC-enabled)

For Additional Information

Ms. Melinda Reed

ODASD, Systems Engineering

571-372-6562

melinda.k.reed4.civ@mail.mil

Program Protection and Cybersecurity in DoD Policy

DoDI 5000.02 Operation of the Defense Acquisition System

- Assigns and prescribes responsibilities for Cybersecurity, includes security, to the acquisition community
- Regulatory Requirement for Program Protection Plan at Milestones A, B, C and FRP/FDD; PM will submit PPP for *Milestone Decision Authority approval* at each Milestone review

DoDI 5200.39 Critical Program Information Identification and Protection Within Research, Development, Test, and Evaluation

- Establishes policy and responsibilities for identification and protection of critical program information
- Protections will, at a minimum, include anti-tamper, exportability features, security, cybersecurity, or equivalent countermeasures.

DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks

- Establishes policy and responsibilities to minimize the risk that warfighting capability will be impaired due to vulnerabilities in system design or subversion of mission critical functions or components

DoDI 4140.67 DoD Counterfeit Prevention Policy

- Establishes policy and assigns responsibility to prevent the introduction of counterfeit material at any level of the DoD supply chain

DoDI 8500.01 Cybersecurity

- Establishes the DoD Cybersecurity Program, the DoD Principal Authorizing Official and Senior Information Security Officer to achieve cybersecurity through a defense-in-depth approach that integrates personnel, operations, and technology