Technology and Program Protection Resilient Systems Overview

Melinda Reed
Director, Resilient Systems
Office of the Under Secretary of Defense for Research and Engineering

National Defense Industrial Association
Systems & Mission Engineering Conference
December 6-8, 2021

The Challenge

The Challenge

Problem: Cyber threats are outpacing weapon system designs for safe, effective, resilient, secure operations; lack engineering bench for secure cyber resilient engineering design decisions

- Policy compliance / requirements derivation
- Cyber risk aversion / technical implication
- Legacy system compatibility

The Portfolio

Strategic and Tactical

Legislation: Inform cybersecurity/supply chain actions

Regulation: Influence outcomes to reduce burden

Policy: Enable tailoring to support warfighter needs

Procedures: Inclusive of engineering requirements

Guidance: Expand S&T manager and engineer knowledge

Workforce: Grow engineering cyber expertise

Risk Assessment: Refine technical assessment approaches

PARTNERS
Industry
Interagency
International
OSD Stakeholders
Military Services
PEO
PM

Key Engineering Cyber/Program Protection Initiatives

- Secure cyber resilient engineering primer and standards
- Influence EO 14028 Enhancing Software Supply Chain Security
- Safeguarding unclassified controlled technical information implementation
- Enhance software supply chain security, including through the Joint Federated Assurance Center
- Provide tools to tailor technology and program protection planning for technical workforce
- Creation of Secure Cyber Resilient Engineering Credential Program / updates to program protection courseware at DAU
- Expand safeguarding requirements for critical programs

Ideal End State

1. Knowledgeable engineering bench
2. Measurable test outcomes
3. Informed technical design decisions across levels of application
4. Tailored to operational needs with clear, concise implications
5. Reduced burdensome compliance activities
6. Innovative mitigations for fielded systems

Strategic Technology Protection & Exploitation

Deputy Director
Strategic Technology Protection & Exploitation (STP&E)
Dr. Robert Irie

D, Maintaining Technology Advantage
Dr. Jesse Appler

Maintain Leadership in Critical Technology Modernization Areas

- Implement new procedures for Technology Area Protection
- Update DoD and Government-wide procedures to strengthen U.S. research enterprise
- Mitigate exploitation in academia, labs, FFRDCs, and UARCs
- Focus security, counterintelligence, and law enforcement actions to deter adversaries

D, Resilient Systems
Ms. Melinda Reed

Foster Assured Resilient Missions, Systems and Components

- Set the technical and policy direction for technology and program protection
- Grow DoD capability/capacity to evaluate and mitigate software component vulnerabilities
- Establish secure cyber resilient weapons, engineering methods and workforce competency

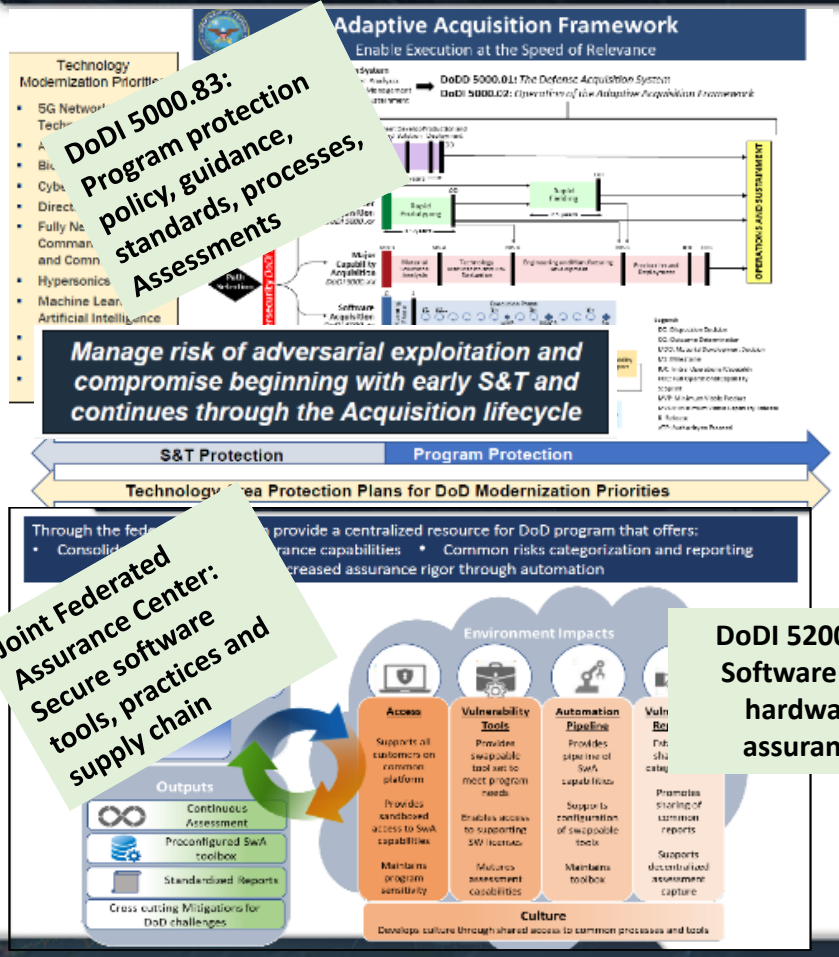
D, Technology and Manufacturing Industrial Base
Mr. Robert Gold

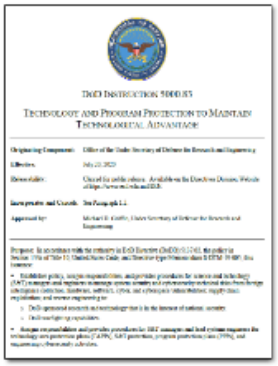
Advance Domestic Innovation Base to Deliver Modernization Goals

- Assess and monitor emerging technology, workforce, engineering, test, & infrastructure base
- Facilitate USG mechanisms and tools to close gaps, foster enabling domestic technology development and manufacturing capability, and counter strategic competitor actions
- Manage the OSD Manufacturing Technology program and Manufacturing Innovation Institutes

MISSION: Promote and protect technology advantage and counter unwanted technology transfer to ensure warfighter dominance through superior, assured, secure and resilient systems, and a healthy viable national security innovation base.

Resilient Systems Initiatives

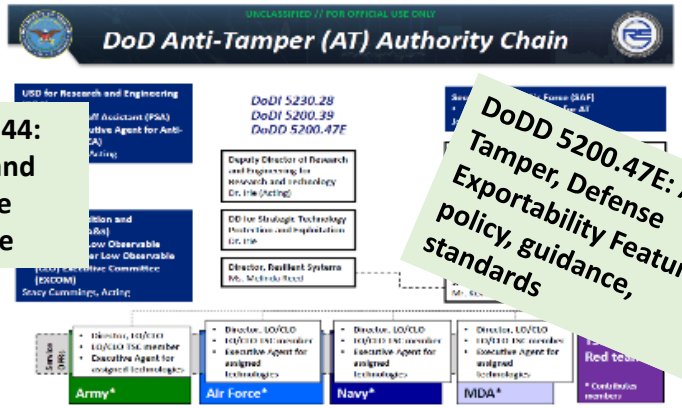




- Safeguard inform
- Control DoD-sp research
- Design for s cyber resili
- Protect the s cyber attacks from enabling and supporting systems
- Protect fielded systems
- Enhance protection for critical programs and technologies

Secure Cyber Resilient Engineering (SCRE): requirements derivation, standards and workforce

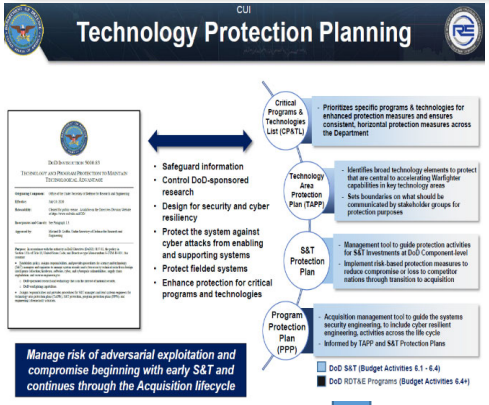
Ability to deliver required capability in a secure manner under the presence of adverse conditions



DoDI 5200.44: Software and hardware assurance

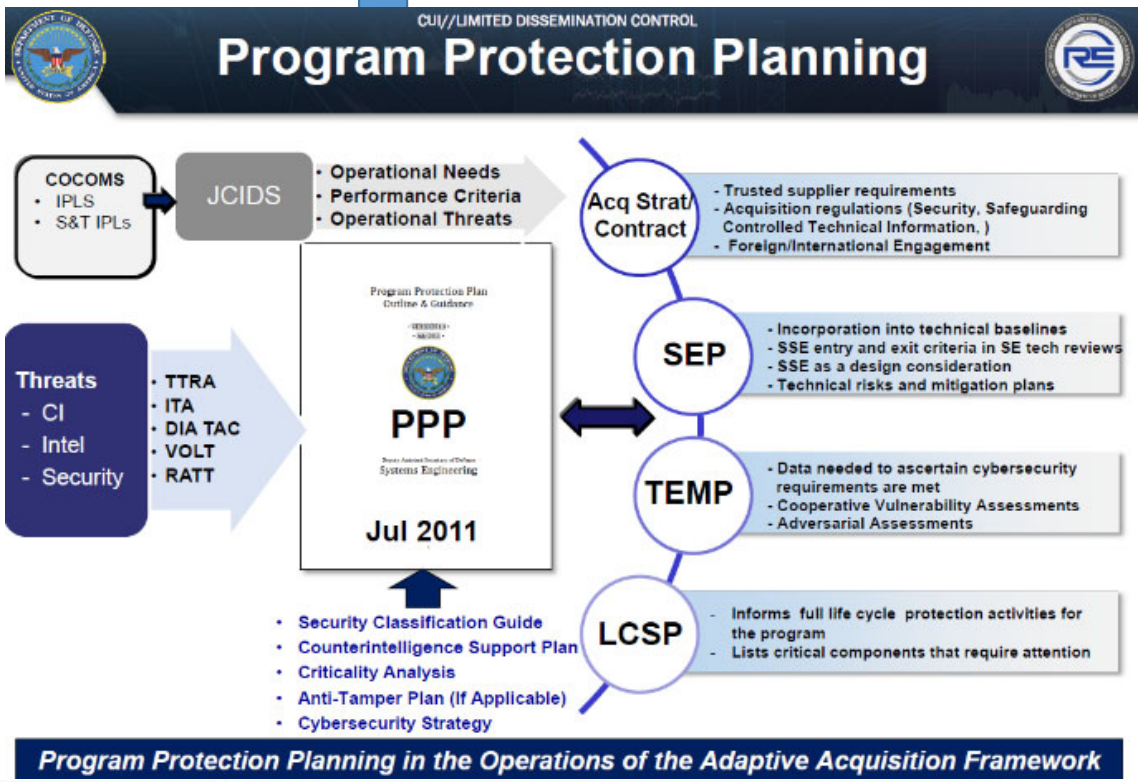
DoDD 5200.47E: Anti-Tamper, Defense Exportability Features: policy, guidance, standards

Program Protection
S&T and Acquisition Activities



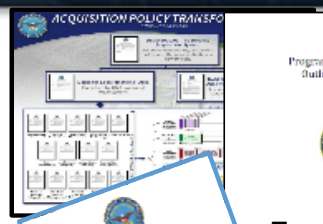
- Provides mechanism to maintain and transition implemented protections applied in S&T
- Informs Secure Cyber Resilient Engineering Design trade off decisions

- Informs S&T protections

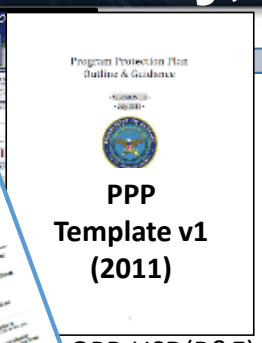


Program Protection Planning in the Operations of the Adaptive Acquisition Framework

DoDI 5000.83: Policy, Guidance, Transformation

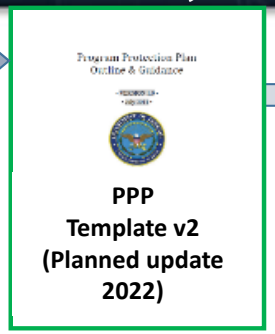


DoDI 5000.83: OPR: USD(R&E)/RS (2020)



PPP Template v1 (2011)

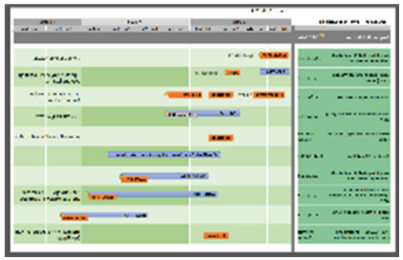
OPR:USD(R&E)/RS



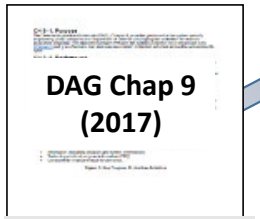
PPP Template v2 (Planned update 2022)

OPR:USD(R&E)/RS

PPP Review and Approval Process



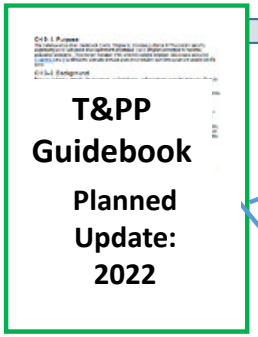
USD(R&E) Assessments for program protection and cyber technical risks



DAG Chap 9 (2017)

Guidance for DoDI 5000.02 Enclosure 13

OPR:USD(R&E)/RS



T&PP Guidebook

Planned Update: 2022

OPR:USD(R&E)/RS

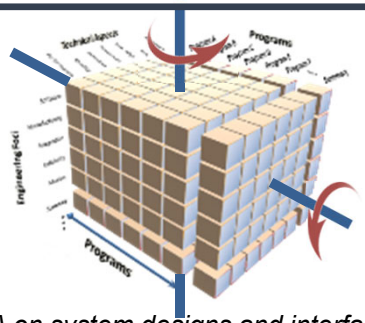
Guidance for S&T Managers and Engineers

OPR:USD(R&E)/MTA

S&T Protection Plan Outline and Guidance under development

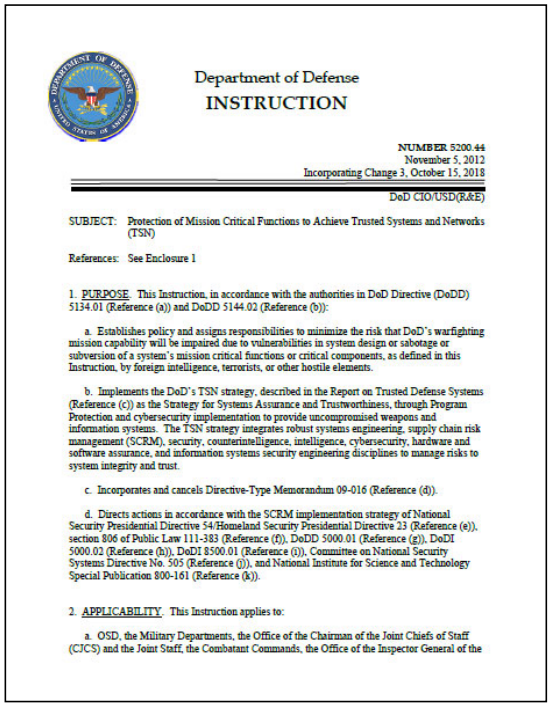
Secure Cyber Resilient Engineering Primer under development

OPR:USD(R&E)/RS



"ITRA on system designs and interfaces for adversarial risks, program protection, and cyber vulnerabilities; results inform technical baselines and risk management activities."

DoDI 5200.44: Trusted Systems and Networks



Department of Defense
INSTRUCTION

NUMBER 5200.44
November 5, 2012
Incorporating Change 3, October 15, 2018

DoD CIO/USD(R&E)

SUBJECT: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

References: See Enclosure 1

1. PURPOSE. This Instruction, in accordance with the authorities in DoD Directive (DoDD) 5134.01 (Reference (a)) and DoDD 5144.02 (Reference (b)):

a. Establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, as defined in this Instruction, by foreign intelligence, terrorists, or other hostile elements.

b. Implements the DoD's TSN strategy, described in the Report on Trusted Defense Systems (Reference (c)) as the Strategy for Systems Assurance and Trustworthiness, through Program Protection and cybersecurity implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, cybersecurity, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust.

c. Incorporates and cancels Directive-Type Memorandum 09-016 (Reference (d)).

d. Directs actions in accordance with the SCRM implementation strategy of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (e)), section 806 of Public Law 111-383 (Reference (f)), DoDD 5000.01 (Reference (g)), DoDI 5000.02 (Reference (h)), DoDI 8500.01 (Reference (i)), Committee on National Security Systems Directive No. 505 (Reference (j)), and National Institute for Science and Technology Special Publication 800-161 (Reference (k)).

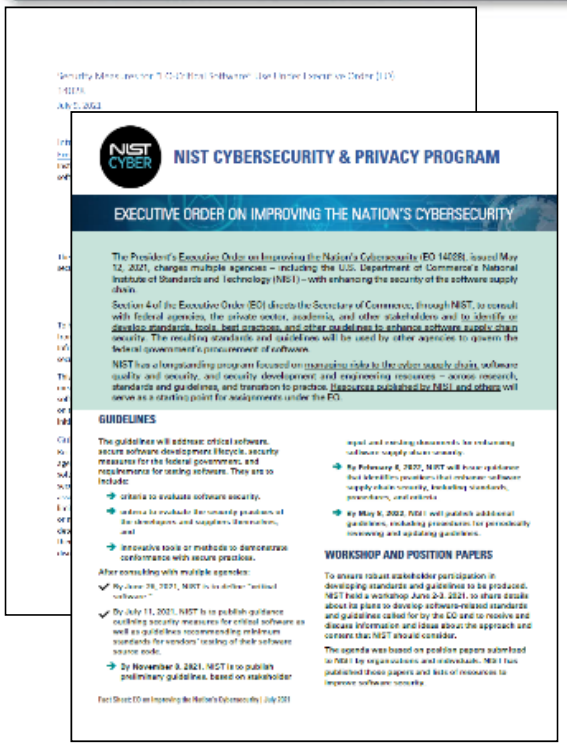
2. APPLICABILITY. This Instruction applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the

- **Implements the DoD's Trusted Systems and Networks (TSN) strategy**
- **Manage risk of mission-critical function and component compromise throughout lifecycle of key systems by utilizing:**
  - Criticality Analysis as the systems engineering process for risk identification
  - Countermeasures: Supply chain risk management, software assurance, secure design patterns
  - Intelligence analysis to inform program management
  - Codify trusted supplier requirement for DoD-unique application-specific integrated circuits (ASICs)
- **Document planning and accomplishments in program protection and information assurance activities**

Draft update incorporates procedures to implement information communication technology (ICT) exclusion authorities, and quantitative assurance approach

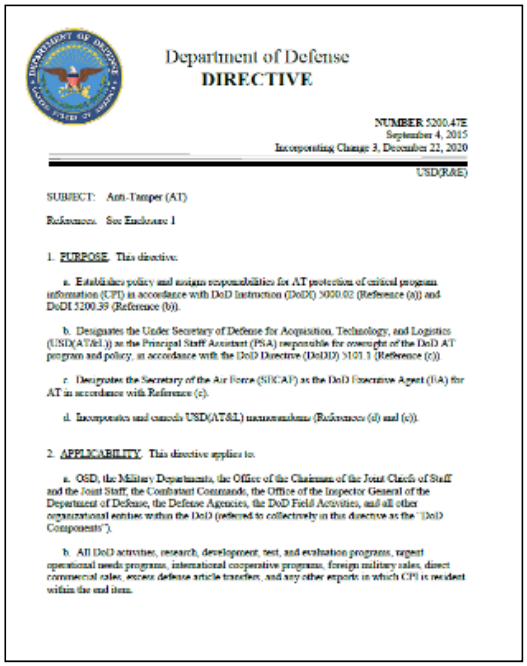
Executive Order (EO) 14028
Improving the Nation's Cybersecurity



Partnerships with DHS and NIST

- **Section 4. Enhancing Software Supply Chain Security**
- **Sec. 4(n)**. Within 1 year of the date of this order, the **Secretary of Homeland Security**, in consultation with the **Secretary of Defense**, the Attorney General, the Director of OMB, and the Administrator of the Office of Electronic Government within OMB, shall recommend to the FAR Council contract language *requiring suppliers of software available for purchase by agencies to comply with, and attest to complying with, any requirements issued pursuant to subsections (g) through (k) of this section*.
- Resources published by NIST and others will serve as a starting point for assignments under the EO
  - Security Measures for "EO-Critical Software" use under EO 14028
  - Guidance/practices to enhance software supply chain security
  - The Minimum Elements For a Software Bill of Materials (SBOM)
  - Revision to NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations; public comments due December 3, 2021

DoDD 5200.47E: Anti-Tamper/Defense Exportability Features



Department of Defense
DIRECTIVE

NUMBER 5200.47E
September 4, 2015
Incorporating Change 3, December 22, 2020
USD(R&E)

SUBJECT: Anti-Tamper (AT)

References: See Enclosure 1

1. PURPOSE. This directive:

a. Establishes policy and assigns responsibilities for AT protection of critical program information (CPI) in accordance with DoD Instruction (DoDI) 5000.02 (Reference (a)) and DoDI 5200.39 (Reference (b)).

b. Designates the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) as the Principal Staff Assistant (PSA) responsible for oversight of the DoD AT program and policy, in accordance with the DoD Directive (DoDD) 5101.1 (Reference (c)).

c. Designates the Secretary of the Air Force (SECAF) as the DoD Executive Agent (EA) for AT in accordance with Reference (c).

d. Incorporates and cancels USD(AT&L) memorandums (References (d) and (e)).

2. APPLICABILITY. This directive applies to:

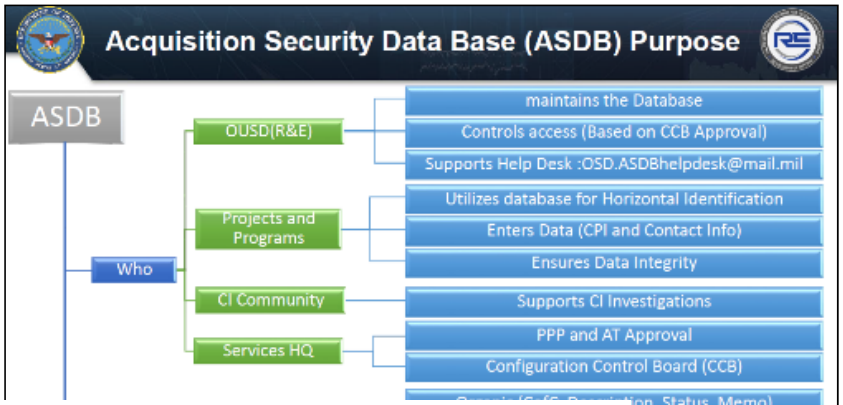
a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD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

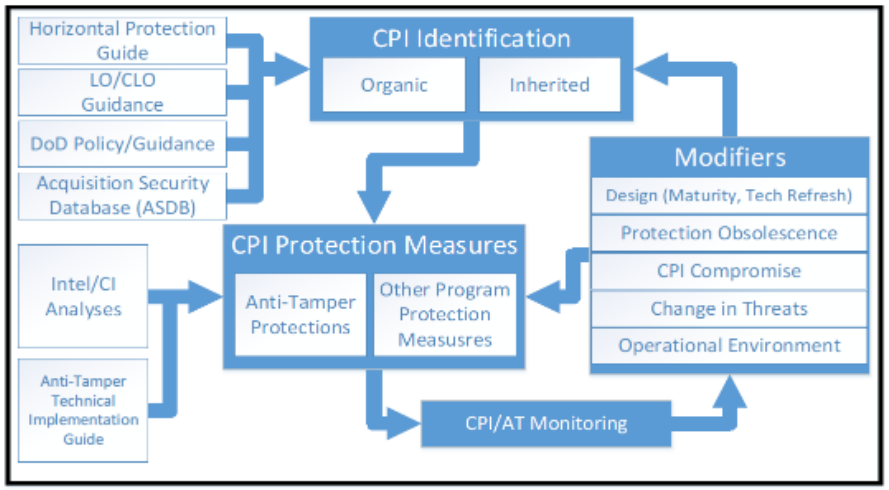
b. All DoD activities, research, development, test, and evaluation programs, urgent operational needs programs, international cooperative programs, foreign military sales, direct commercial sales, export defense article transfers, and any other exports in which CPI is resident within the end item.

USD(R&E) is the PSA for Anti-Tamper

SECAF is the DoD Executive Agent for Anti-Tamper

Partnership with OUSD(A&S) International Cooperation





Draft update clarifies critical program information as technology advantage elements

Secure Cyber Resilient Engineering

Background

Goal: Improve resiliency of weapons system designs to cyber attack*

- ✓ **Action: Develop a new enclosure to DoD Instruction 5000.02 Operation of the Defense Acquisition System***
  - DoDI 5000.02, Enclosure 14 Cybersecurity in the Defense Acquisition System, 26 Jan 2017
- **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, Chief Information Officer (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

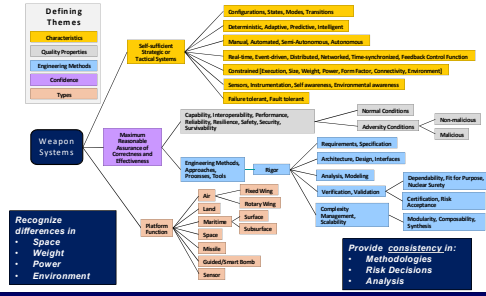
DoD w

Implementing Cybersecurity into Weapons System Programs: Summary of Observations

- **PEOs, PMs are reporting that implementation is problematic**
  - Acquisition programs are seeking clear and specific cyber resiliency guidance
  - Risk Management Framework (RMF) for Information Technology (IT) governance and compliance schemes don't possess weapons and tactical domain expertise
- **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
- **Operational Test community, Red Teams, COCOM exercises continue 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		
Design Guidelines	Engineering Assessment	Implementation

Weapon Systems Characteristics



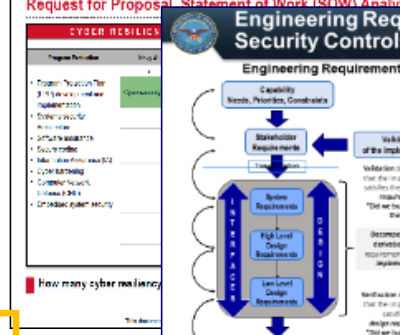
Weapon Systems Deliver Lethal Force with the Intent to Cause Harm

A secure and cyber resilient system is one that can deliver required capability in a secure manner under the presence of adverse conditions

RFP SOW Analysis Results Summary

Raytheon

Request for Proposal, Statement of Work (SOW) Analysis Results Summary



Engineering Requirements and Security Controls Comparison

Design Guidelines and Standards

Addressing Recurring Challenges: Processes, Standards, Workforce

Implementation: Engineering Cyber Resilient Weapon Systems Workshop Series

1 Baseline Understanding
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

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

3 Chart Path Forward
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

4 Engineering Methods
1. Cyber effects on Technical Performance Measures and Metrics
2. Examine cyber requirements and SETR criteria
3. Leverage System Safety
4. Identify considerations for embedded software
5. Inform RIO based on cyber effects

5 Supply Chain Risk Management
1. Integrate supply chain mitigation approaches in standards, guidance and assessment methods
2. Consider approach for systems in sustainment
3. Plan for sustainment
4. Use available validated Intel and CI to make risk informed decisions

6: Cybersecurity Engineering
Identify skill sets and curriculum needs for our current and future engineering workforce
1. Develop a BoK
2. Establish a cyber engineering competency model
3. Establish a practice

7: Move the Ball, Move the Chain
Establish roadmap for engineering standardization of J6 Cyber Survivability Endorsement
1. Fundamental challenge is preventing losses
2. Establish a cyber engineering competency model
3. Scope of cyber loss

8: Engineering Design Activities
Identify skill sets and curriculum needs for our current and future engineering workforce
1. Need Loss Control Objectives
2. Refine Design Materials
3. System Analysis of Loss Guidance

Collaboration Forum with Government, Industry, and Academia that builds upon each workshop to address challenges and lessons learned

9: Technical Exchange
Virtual sharing of ongoing activities to shape the landscape
1. Army Practices
2. Air Force Practices
3. Navy Practices

9a: CYBER Mission Forces
Planning for integration of CYBER Mission Forces capability
1. Mission Level / System Level
2. Actionable Mission information needed
3. CYBERCOM requirements / system requirements

10: Fill the "Building Code"| Void
Establish roadmap for secure cyber resilient engineering practice to for standardization
1. Define building code criteria,
2. Identify secure cyber resilient engineering activities
3. Inform SCRE Credential Program

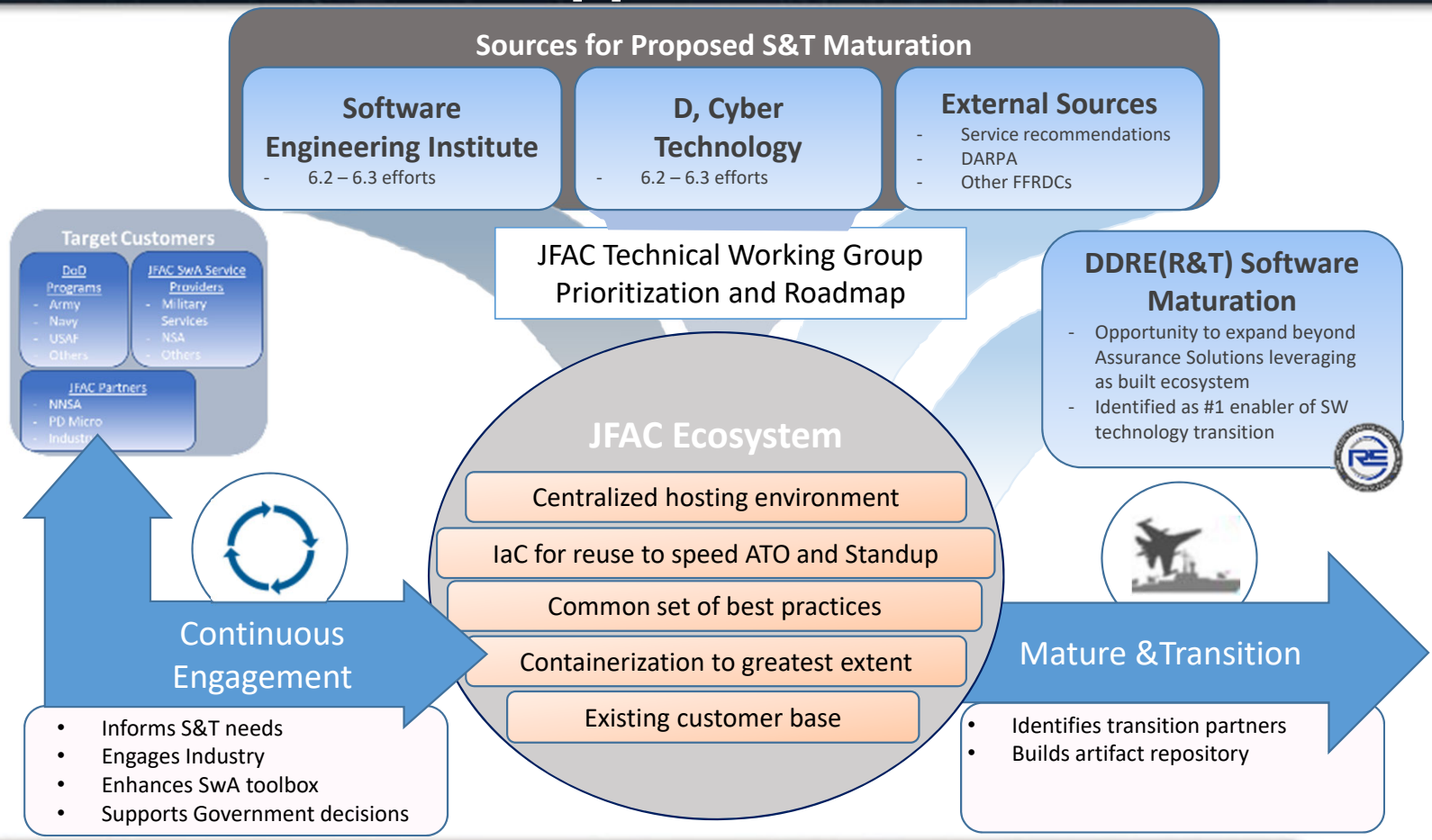
In development

Secure Software Supply Chain
Joint Federated Assurance Center

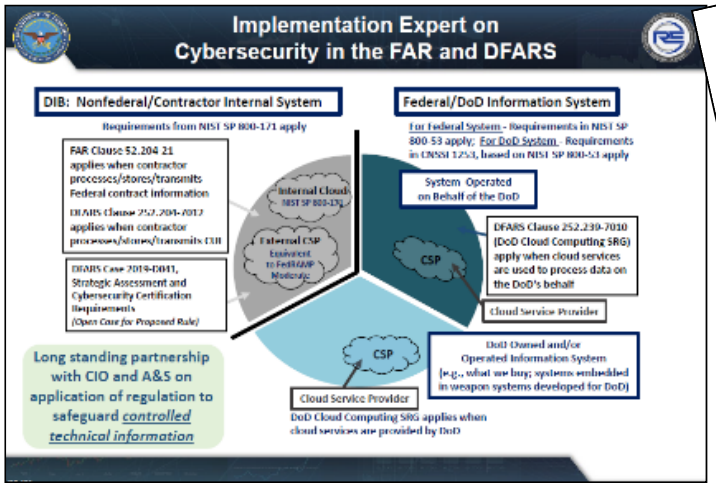
- **The Joint Federated Assurance Center (JFAC) was established to ensure the security of software and hardware developed, acquired, maintained, and used by the Department through the federation of existing DoD software and hardware assurance resources, expertise, and capabilities.**
- **Federal and Department initiatives are revolutionizing application of software assurance tools, practices and techniques**
  - DevSecOps,
  - Zero Trust Architecture
  - DoD Adaptive Acquisition Framework Software Acquisition Pathway
  - Executive Order 14028 – Improving the Nation's Cybersecurity

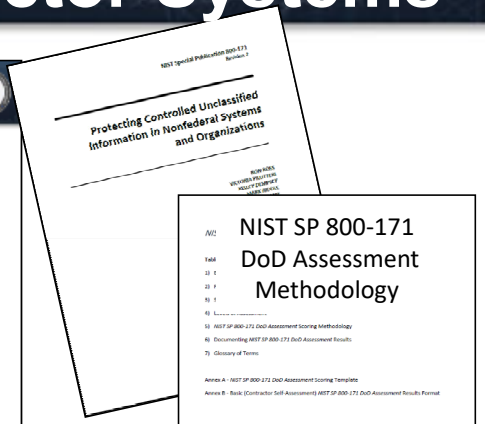
- **The JFAC Modernization Strategy for Software Assurance was developed to support the software assurance initiatives:**
  - Focus on opportunities to overcome resource limitations to provide capabilities and expertise directly to DoD programs
  - Leverage existing DoD Software Initiatives to modernize JFAC infrastructure and capabilities
  - Transition culture away from the development of capabilities to the federation and maturation of existing tools and resources

Software Assurance Technology Transition Opportunities



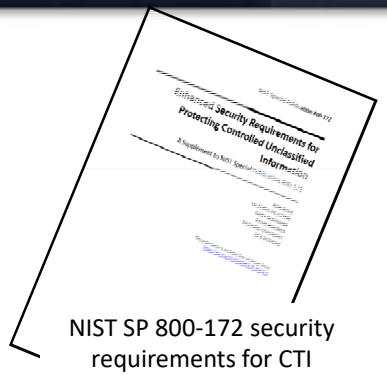
Protection of Controlled Technical Information on Contractor Systems



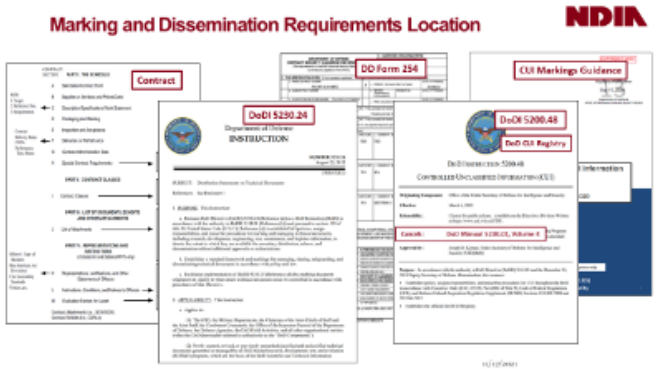


NIST SP 800-171 DoD Assessment Methodology

Standardized procedures to strategically assess NIST SP 800-171 implementation



NIST SP 800-172 security requirements for CTI associated with critical programs and technologies



Working with NDIA, DTIC and DAU to develop guidance for S&T managers and engineers to apply marking and dissemination statements and safeguard Controlled Technical Information (CTI)

Workforce Competency

- Defense Acquisition University
  - ACQ 160*: Program Protection Planning Awareness
  - ENG 260*: Program Protection for Practitioners

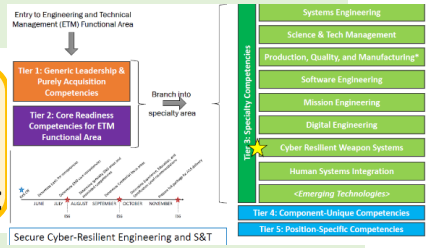
Program Protection Credential Program In place

***Update required to align with AAF**

Curriculum includes: Anti-Tamper, safeguarding CTI in the Defense Industrial Base, information communications technology supply chain risk management (ICT SCRM), software assurance and hardware assurance

- Defense Acquisition University
  - Draft Secure Cyber Resilient Engineering competency model approved by Engineering and Technical Management (E&TM) Task Force

SCRE Credential Program Under Development



Planned to include life cycle protection considerations for engineering secure, resilient, and trustworthy DoD systems, networks, and communications

- **Partnering with NDIA System Security Engineering Committee and DAU**
  - CTI Tabletop Tutorial
  - Hardware Assurance and Microelectronics Quantitative Assurance Tabletop Tutorial

Controlled Technical Information Credential Program future request

Proposal to include methods to identity, apply marking and dissemination statements to CTI; and to carve out information that is not controlled

Resilient Systems End State

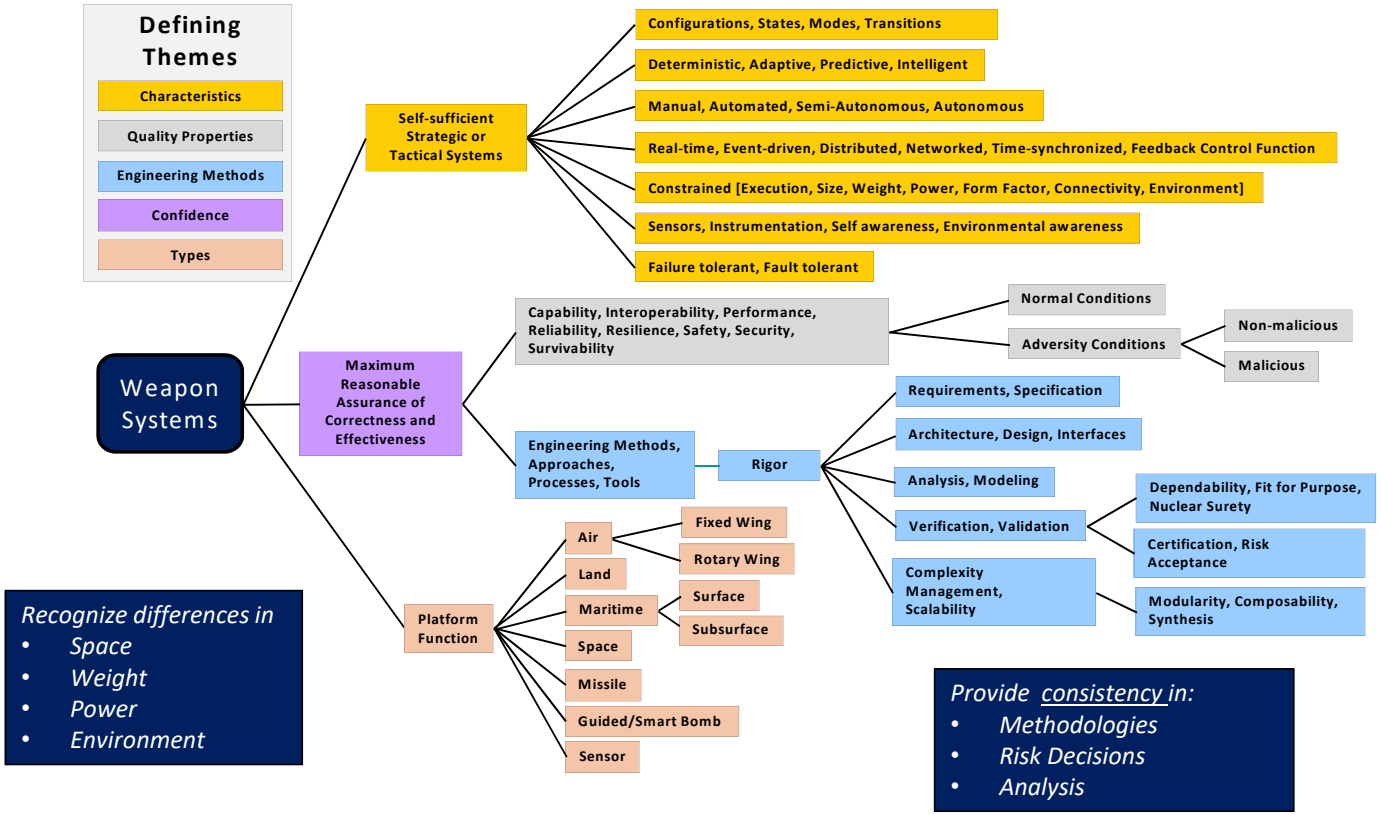
- **DoDI 5000.83 establishes roles and responsibilities for the S&T manager and the engineering workforce**
  - **Updates to guidance, standards, education and training are pending to make more consistent implementation**
- **Improve the efficiency and effectiveness of weapon systems engineering practice to deliver, and modernize, systems with the required capability in a secure manner under the presence of adverse conditions**
- **Increase consistency and repeatability of secure cyber resilient engineering methods and standards**
- **Improve the communication between government, industry, and operational stakeholders**

Customer-Focused: Outcome-Based

Questions

Backup

Weapon Systems Characteristics



Weapon Systems Deliver Lethal Force with the Intent to Cause Harm

Technology, Program Protection & Cybersecurity Related Policies

Technology

Key Protection Activities:

- Export Control
- Anti-Tamper
- Defense Exportability Features
- DoD Horizontal Protection Guide
- Acquisition Security Database

Goal: Prevent compromise or loss of critical technology transfer

- **DoDI 5200.39 Critical Program Information**
- **DoDD 5200.47E Anti-Tamper**

Mission Components

Key Protection Activities:

- Software Assurance
- Hardware Assurance
- Supply Chain Risk Management
- Anti-counterfeits
- Joint Federated Assurance Center

Goal: Protect mission-critical components (hardware, software) from malicious exploitation

- **DoDI 5200.44 Trusted Systems & Networks**
- **PL 113-66 Sec 937 (FY14 NDAA) JFAC**
- **DFARS 239.73 Requirements for information relating to supply chain risk**
- **10USC 2339a; Requirements for Information Relating to Supply Chain Risk**
- **NDAA FY18 Sec 1659. Supply Chain Risk Management of Critical Missions**
- **NDAA FY19 Sec 1655, Mitigation of Risks to National Security Posed by Providers of IT products and services who have obligations to foreign governments**

Information

Key Protection Activities:

- Classification
- Information Security
- Cybersecurity Protections and Technology Solutions
- Joint Acquisition Protection & Exploitation Cell (JAPEC)
- Damage Assessment Management

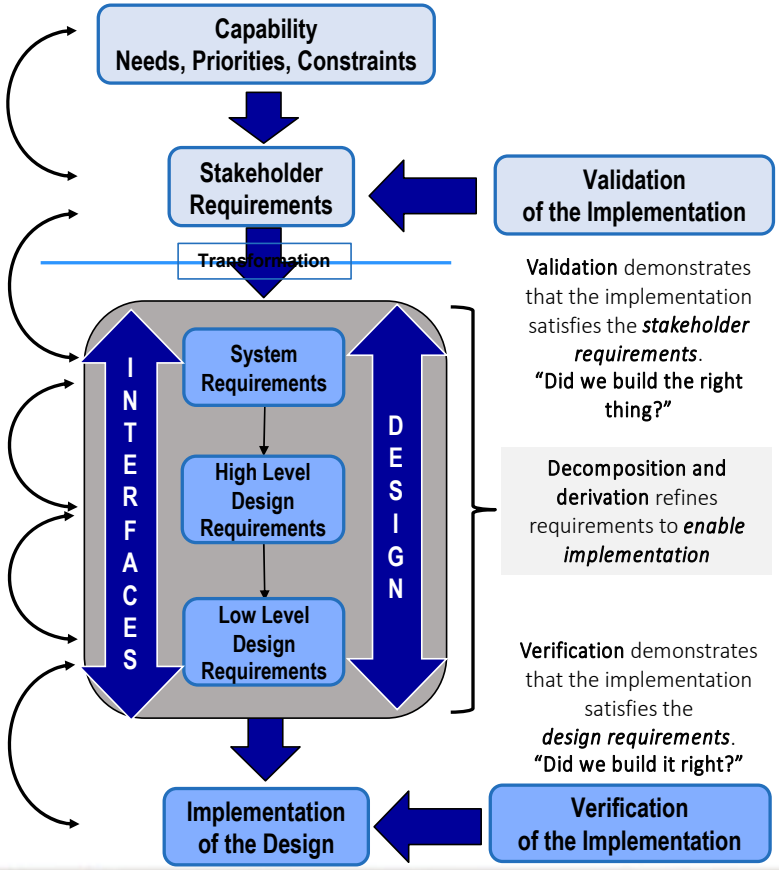
Goal: Safeguard system and technical data from adversary collection and disruption

- **DoDI 5230.24 Distribution Statements on Technical Information**
- **DoDI 5200.48 Controlled Unclassified Information**
- **DFARS 252.204-7012 Safeguarding covered defense information and cyber incident reporting (includes requirement to implement NIST SP800-171)**
- **DCMA NIST SP 800-171 Strategic Assessments**
- **32 CFR 2002: Controlled Unclassified Information**
- **Secure Cyber Resilient Engineering**
- **DoDI 8500 series**

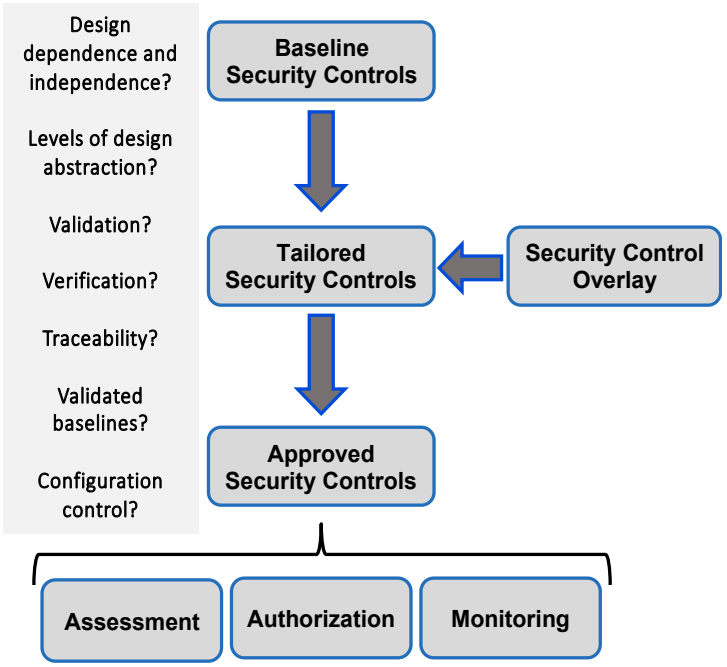
Goal: Ensure warfighter dominance through superior, assured, and resilient systems

Engineering Requirements and Security Controls Comparison

Engineering Requirements



Security Controls



Secure Cyber Resilient Engineering Practice Requirements and Design Maturity