# *New Context, Visibility for Anti-Tamper*

***May 1, 2007***

**Kristen Baldwin**

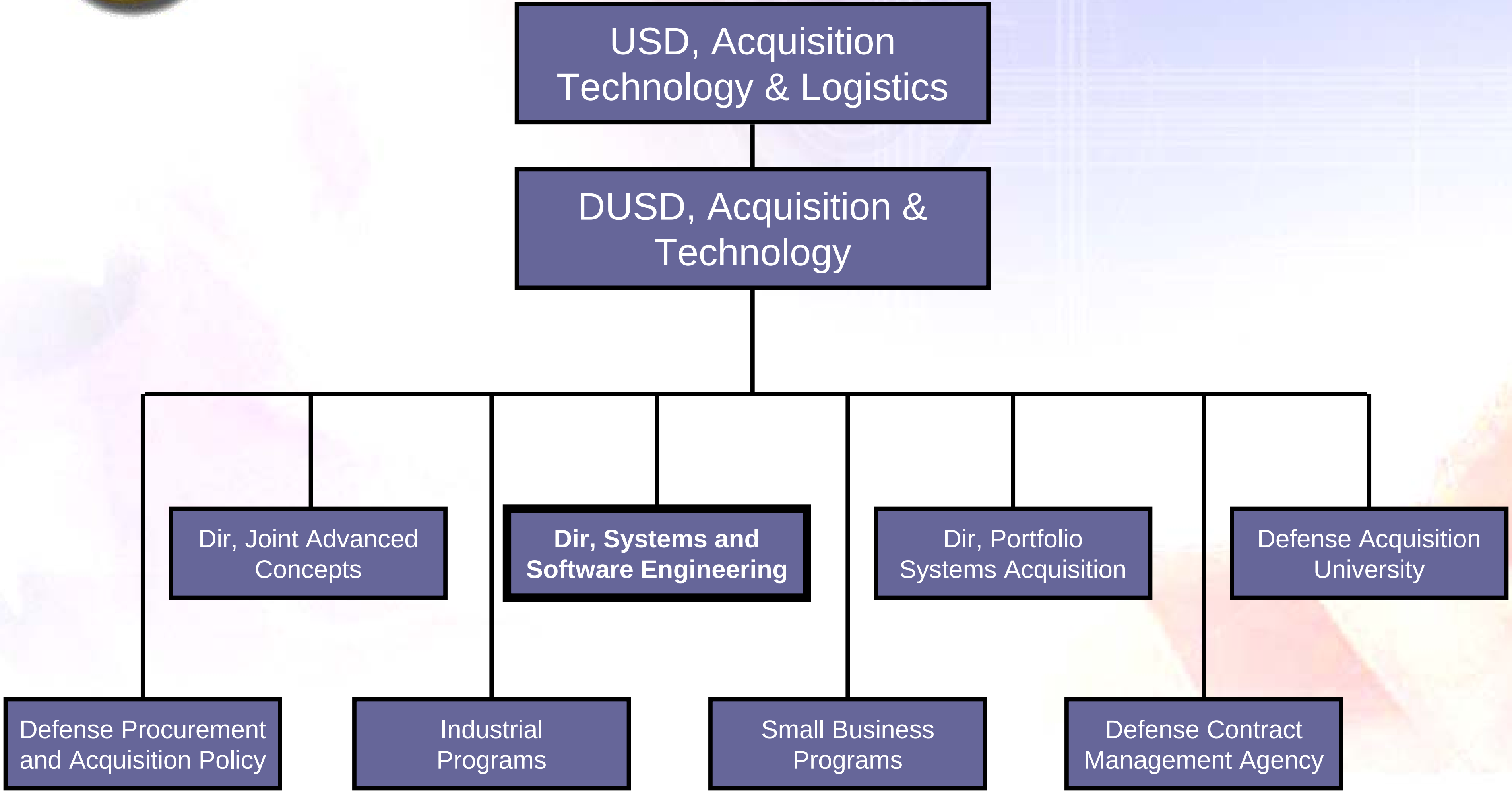
**Deputy Director,**

**Software Engineering and System Assurance**

**Office of the Under Secretary of Defense**

**Acquisition, Technology and Logistics**

# OUSD (AT&L) Organization
# May 2006



USD, Acquisition Technology & Logistics

DUSD, Acquisition & Technology

Dir, Joint Advanced Concepts

**Dir, Systems and Software Engineering**

Dir, Portfolio Systems Acquisition

Defense Acquisition University

Defense Procurement and Acquisition Policy

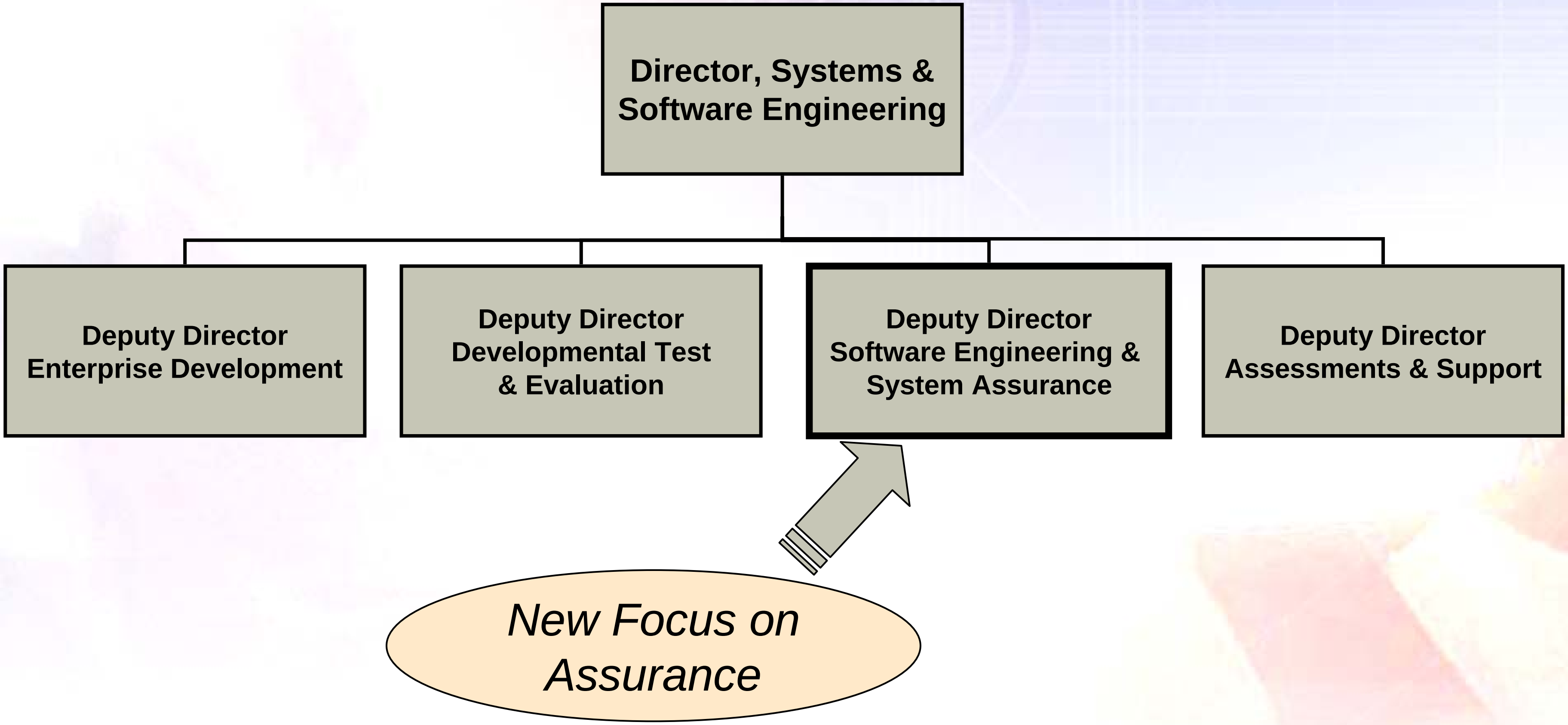
Industrial Programs

Small Business Programs

Defense Contract Management Agency

# Systems and Software Engineering

## *An Organizational Construct*



Director, Systems & Software Engineering

Deputy Director Enterprise Development

Deputy Director Developmental Test & Evaluation

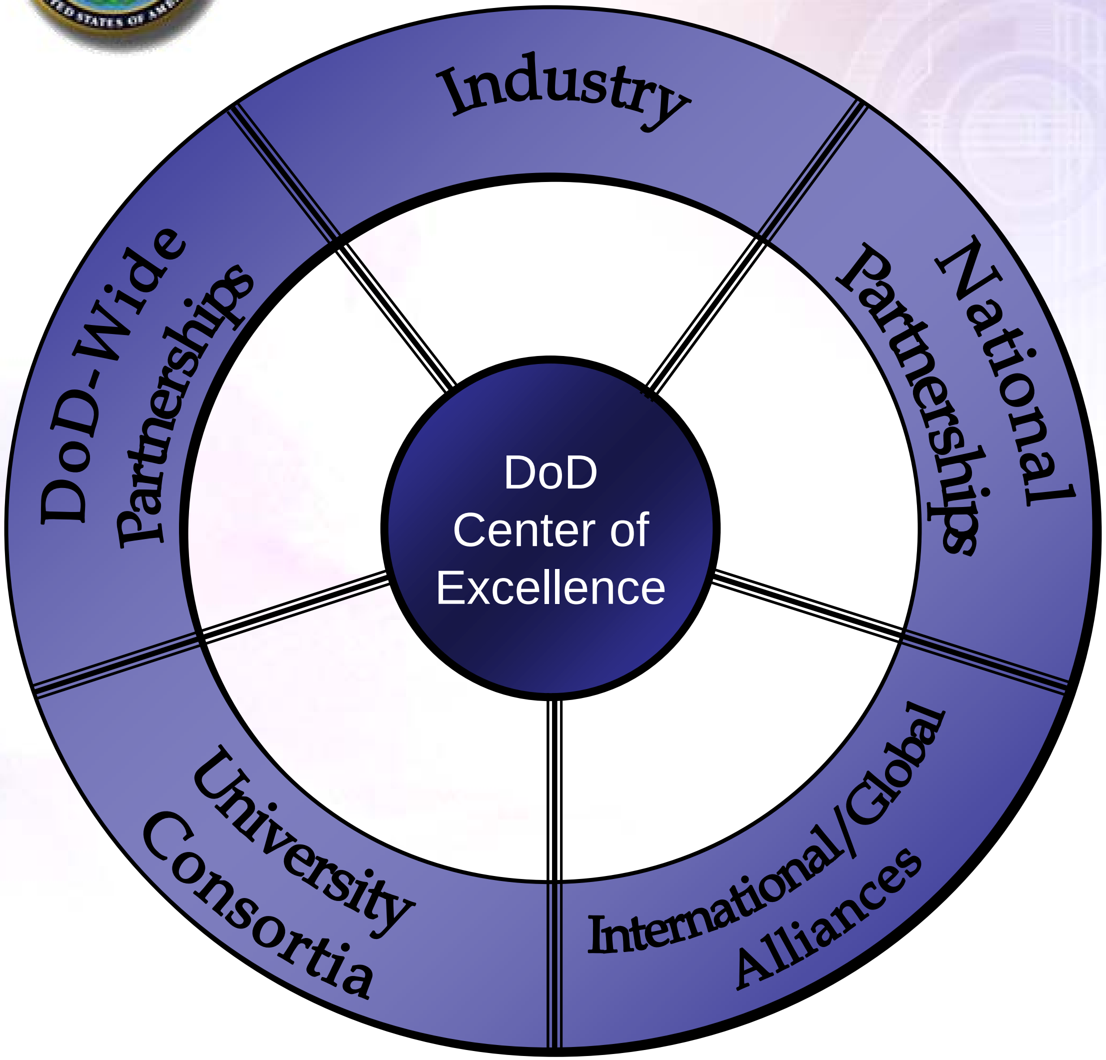
Deputy Director Software Engineering & System Assurance

Deputy Director Assessments & Support

*New Focus on Assurance*

*Acquisition program excellence through sound systems and software engineering*

# Establishing a DoD Engineering Center of Excellence



**DoD Engineering Center of Excellence**

- Support Acquisition Success
- Improve State-of-the-Practice of Engineering
- Leadership, Outreach and Advocacy
- Foster Resources to Meet DoD Needs

# Getting Started – What are we Doing?

- Identifying issues, needs
  - Software Industrial Base Study
  - NDIA Top SE and Software Issue Workshops
  - Defense Software Strategy Summit
- Creating opportunities, partnerships
  - Established network of Government software POCs
  - Co-chair NDIA System Assurance Committee
  - Chair, DoD Systems Assurance Working Group
  - Information exchanges with Government, Academia, and Industry
  - Sponsoring the Systems & Software Technology Conference, 18-21 Jun 07, Tampa, FL
- Executing focused initiatives
  - Handbook on Engineering for System Assurance
  - SoS Systems Engineering Guide
  - CMMI Integrity, CMMI-ACQ, CMMI Guidebook
  - Providing support to acquisition programs

# Top Software Issues*

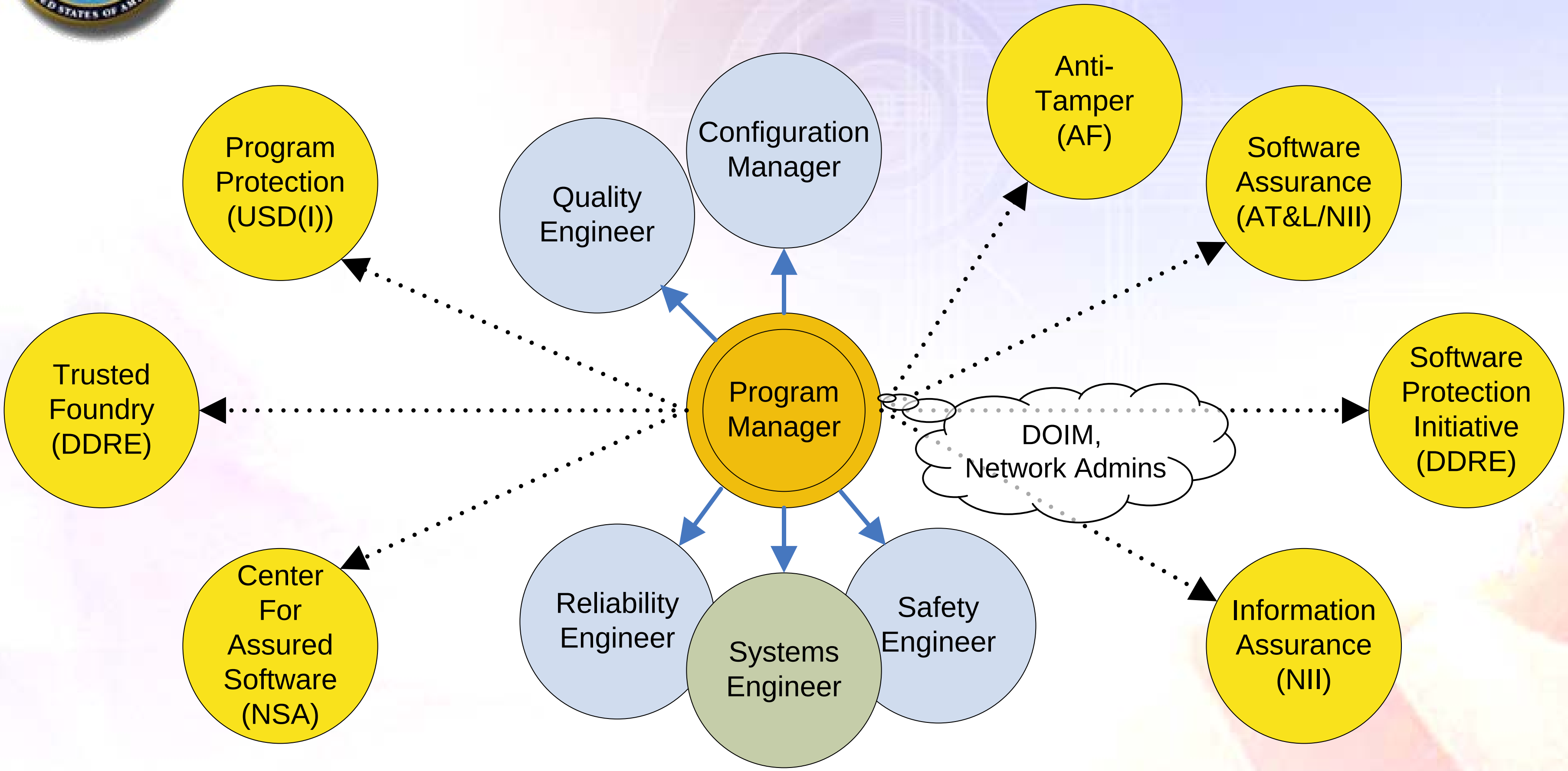
1. The impact of requirements upon software is not consistently quantified and managed in development or sustainment.
2. Fundamental system engineering decisions are made without full participation of software engineering.
3. Software life-cycle planning and management by acquirers and suppliers is ineffective.
4. The quantity and quality of software engineering expertise is insufficient to meet the demands of government and the defense industry.
5. Traditional software verification techniques are costly and ineffective for dealing with the scale and complexity of modern systems.
6. There is a failure to assure correct, predictable, safe, secure execution of complex software in distributed environments.
7. Inadequate attention is given to total lifecycle issues for COTS/NDI impacts on lifecycle cost and risk.

*NDIA Top Software Issues Workshop
August 2006

# Increasing Importance of Anti-Tamper and Assurance

- **Emphasis on cooperative system development with foreign partners**
  - AT measures needed to protect critical technologies from foreign exploitation or reverse engineering
- **Higher incidence of network attacks**
  - Increased risk of DoD Intellectual Property, weapon system designs, etc., falling into the wrong hands
- **Globalization of the industrial base has led to more contracts (below prime) with the international community**
  - More access to critical program information

# System Assurance Context for the PM



System Assurance Definition

*Level of confidence* that a system functions as intended, is free of exploitable vulnerabilities, and protects critical program information

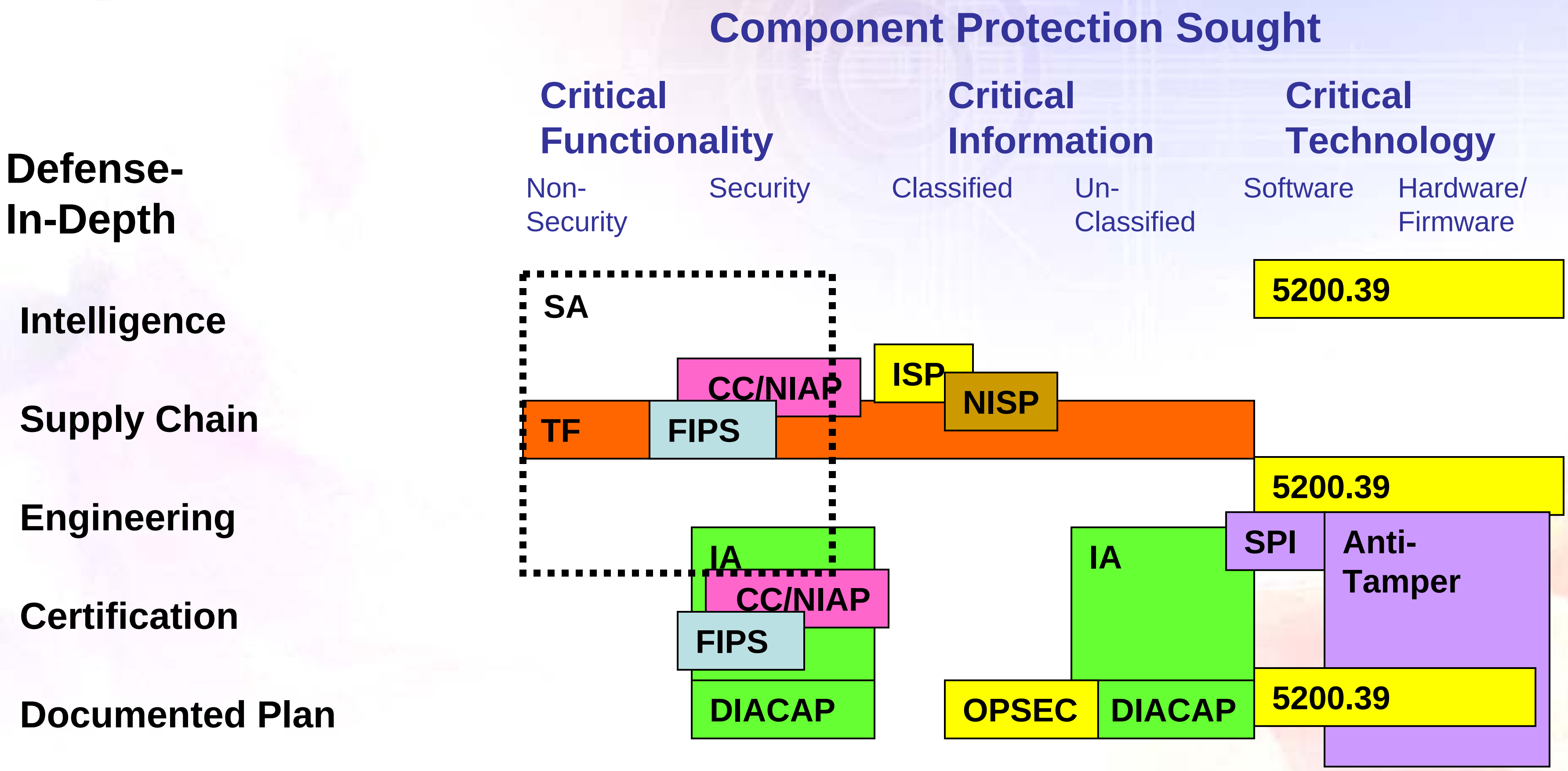
# Consequences of Fragmented Systems Assurance Initiatives

- Lack of Coherent Direction for PMs, and others acquiring systems
  - Numerous, uncoordinated initiatives
  - Multiple constraints for PMs, sometimes conflicting
  - Loss of time and money and lack of focus on applying the most appropriate engineering for systems assurance for each system
- Synergy of Policy – Multiple ownership
  - Failure to capitalize on common methods, instruction among initiatives
- DoD Risk Exposure
  - Lack of total life cycle view
  - Lack of a focal point to endorse system assurance, resolve issues, advocate PM attention
  - Lack of system-of-systems, architecture perspective on system assurance
  - Potential for gaps in systems assurance protection

# Path Forward: Integrate Security Policies

- **Create a 'framework' to integrate multiple security disciplines and policies**
  - Leverage 5200.39: expand CPI definition to include system assurance and total life cycle
- **Use the Program Protection Plan (PPP) to identify CPI and address assurance for the program**
  - Link plans (e.g., Anti-Tamper, Software Protection, System Engineering, Assurance Case)
- **Modify Acquisition and System Engineering guidance to integrate system assurance across the lifecycle**
  - Milestone Decision Authority visibility
  - Guidebook on Engineering for Assurance for program managers/engineers

# Current Systems Security Policies



## Component Protection Sought

Critical Functionality: Non-Security, Security

Critical Information: Classified, Un-Classified

Critical Technology: Software, Hardware/ Firmware

Defense-In-Depth

Intelligence

Supply Chain

Engineering

Certification

Documented Plan

Policy Ownership

- DoD - CIO/DSS
- DoD – AT&L
- DoD – AT&L/S&T
- DoD - CIO/DISA
- CC/NSA
- DoD – NSA
- DoD - USD(I)
- NIST

# Proposed Framework for Security Policies

## Component Protection Sought

Critical Functionality: Non-Security, Security

Critical Information: Classified, Un-Classified

Critical Technology: Software, Hardware/ Firmware

**Defense-In-Depth**

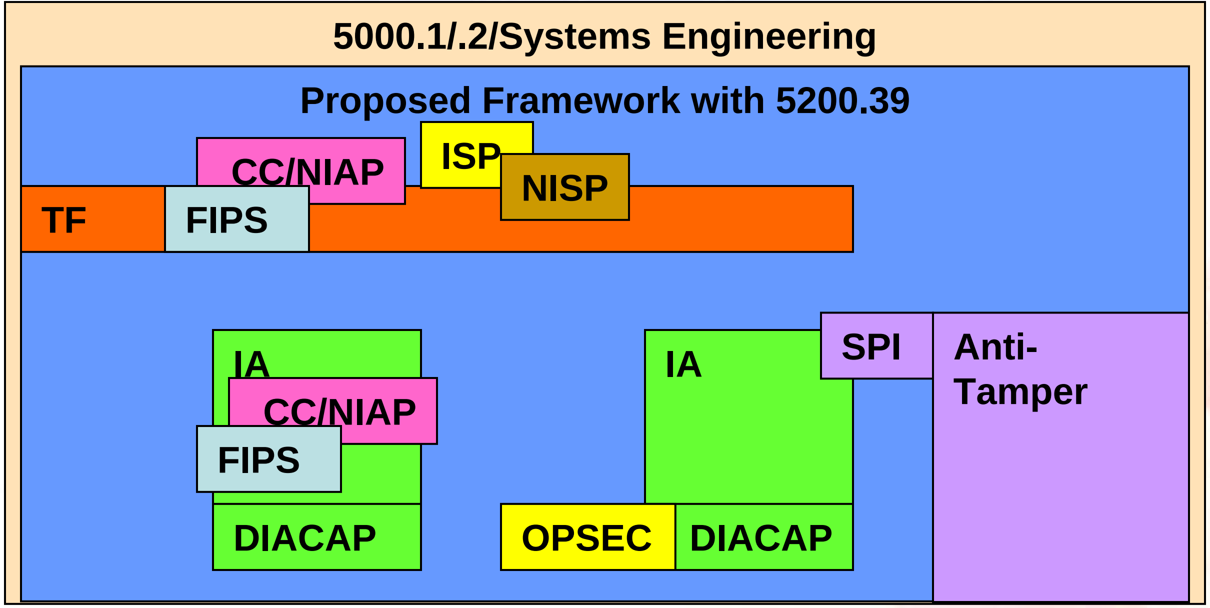
**Intelligence**

**Supply Chain**

**Engineering**

**Certification**

**Documented Plan**



5000.1/.2/Systems Engineering

Proposed Framework with 5200.39

CC/NIAP

ISP

NISP

TF

FIPS

IA

CC/NIAP

FIPS

DIACAP

IA

SPI

Anti-Tamper

OPSEC

DIACAP

Policy Ownership

DoD - CIO/DSS

DoD – AT&L

DoD – AT&L/S&T

DoD - CIO/DISA

CC/NSA

DoD – NSA

DoD - USD(I)

NIST

# Critical Program Information

New Definition - Draft DoDI 5200.39:

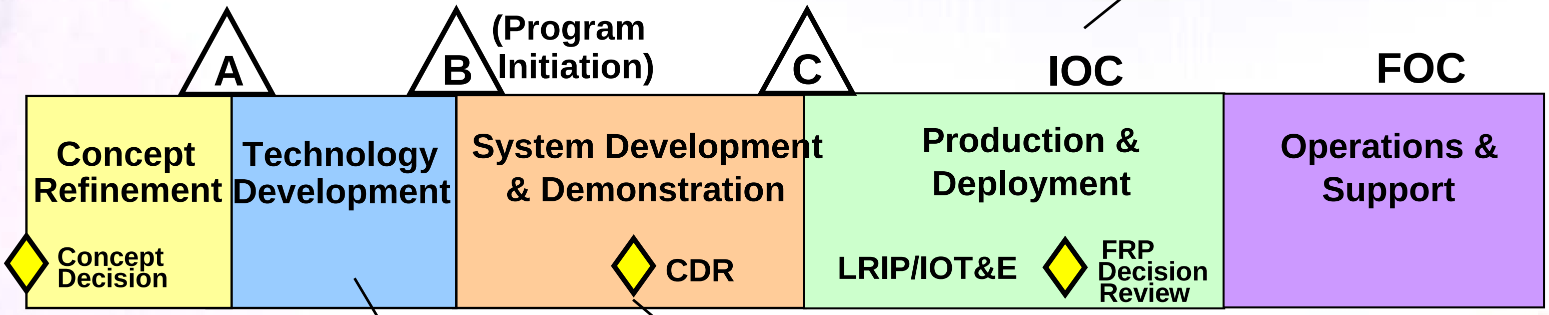
- E3.6. Critical Program Information (CPI). Elements or components of an RDA program that if compromised, could cause significant degradation in mission effectiveness, shorten the expected combat-effective life of the system, reduce technological overmatch, significantly alter program direction, or enable an adversary to counter, copy, or reverse engineer the technology or capability.
- E3.6.1. **Technologies** become eligible for CPI selection when a DoD Agency or military component invests resources to demonstrate an application for the technology in an operational setting, or in support of a transition agreement with a Program Manager.
- E3.6.2. Includes **information** about applications, capabilities, processes, and end-items.
- E3.6.3. Includes **elements or components** critical to a military system or network mission effectiveness.

# *Notional Assurance Implementation*

- Identify CPI in PPP
- Identify threats
- Develop Plans (AT, SEP, TES)

- Approved SEP with details on Assurance
- Milestone Decision approves plans, sets SDD criteria

- Sustainment security plans in place
- Maintenance providers meet security practice
- Upgraded HW/SW configuration managed, validated and verified



A

B (Program Initiation)

C

IOC

FOC

Concept Refinement

Concept Decision

Technology Development

System Development & Demonstration

CDR

Production & Deployment

LRIP/IOT&E

FRP Decision Review

Operations & Support

- Source selection consideration of supplier FOCI and security practices
- Technology Readiness Assessment
- Sensitivity Analysis
- CPI enter Horizontal Protection Database

- Final AT Plan
- Designs meet assurance plans
- Initial verification and validation of critical components

*Total Lifecycle Approach to Assured Systems*

# Moving Forward with Acquisition of Assured Systems

- Critical activities necessary to protect our National interests
- AT Executive Agent is an important and necessary focal point
- Collaboration across assurance disciplines is essential
- Together, we can make assurance a seamless process for our programs, and minimize our risk exposure