A Strategy for Improved System Assurance

October 24, 2007

Kristen Baldwin
Deputy Director,
Software Engineering and System Assurance
Office of the Under Secretary of Defense
Acquisition, Technology and Logistics

Assurance Efforts Update

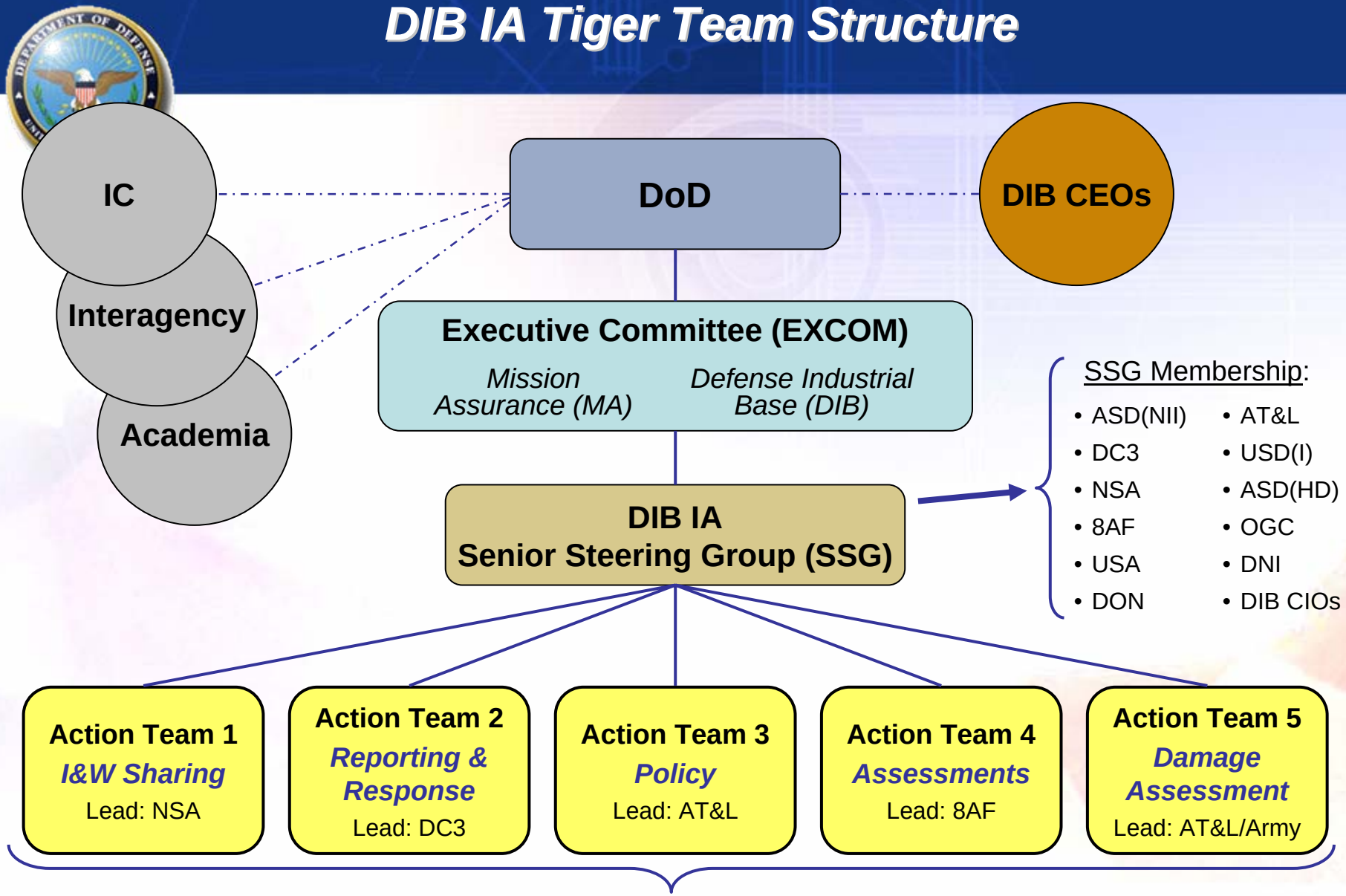
- **Defense Industrial Base Information Assurance Policy Team Efforts**
- **System Assurance Working Group Efforts**
  - Current Tasking
  - 6-bar construct
  - Progress
- **System Assurance Guidebook**
  - Intent
  - Current Status and Way Ahead
- **Program Protection Policy**
- **Software Assurance Initiative**
  - Software Engineering Institute
- **Overall Systems Assurance Progress Report**

System Assurance

- **We continue to be concerned with assurance of our critical DoD assets:**
  - Critical information
  - Critical technologies
  - Critical systems
- **Observations:**
  - Increasing numbers of network attacks (internal and external to DoD)
  - Broader attack space
- **Trends that exacerbate our concerns:**
  - Globalization of our contracts, expanding the number of international participants in our system developments
  - Complex contracting arrangements that further decrease transparency below prime, and visibility into individual components

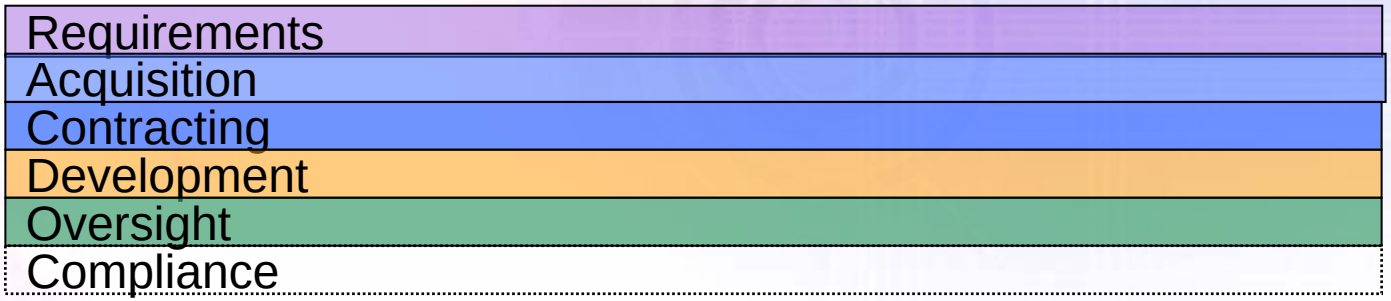
These trends increase the opportunity for access to our critical assets, and for tampering

DIB IA Tiger Team Structure



Matrixed participation by DoD and DIB representatives in all 5 Action Teams

System Assurance Working Group Update: 6-bar approach



- **“Holistic” approach, end-to-end spectrum to capture the most stakeholders**
  - Note: Intelligence Stakeholder is embedded in and across all “bars”
- **Concentrate on six areas of interest, which also happen to be logical grouping of discipline interest and existing policies**
- **Within each “bar”, identify processes, policies to leverage for system assurance**

Systems Assurance Implementation Strategy

JCIDS

- Joint Publications & Definitions (existing process)
- ICD, CDD, CPD boiler plate (existing process)
- NR KPP Attributes (existing process)

Acquisition

- "Cost of Doing Business" (existing process)
- Guidance for SEP, ISP, TEMP (existing process)
- CPI pre-work in FAA and Functional Needs Analysis (FNA) (existing process)
- Combine Plans where possible (e.g., OPSEC<>PPP) (existing process)
- Threat and risk collaboration (existing process)

Six task blocks shown for breakout purposes only.
Not aligned with timeline, yet

Contracting

- Terms & Conditions (existing process)
- Standard Contract Language (existing process)
- SDP, PPP (existing process)

Development

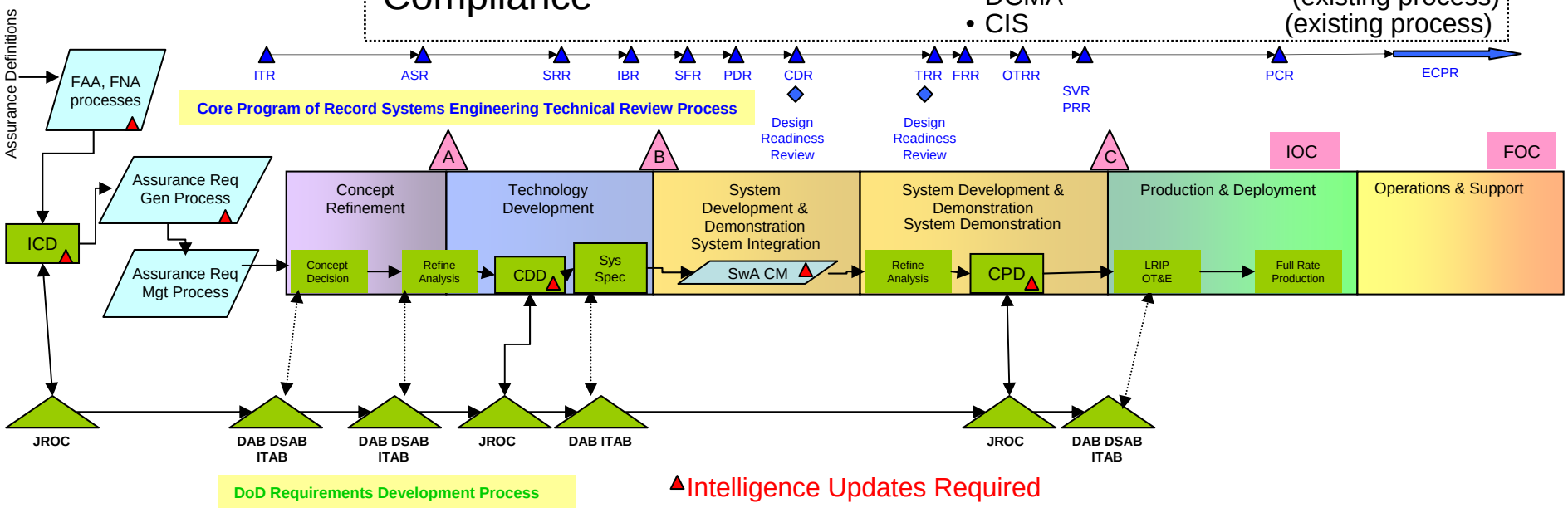
- Technical Requirements (existing process)
- Mitigation Guidance (NII, DSS) (existing process)
- Software tools (CPI-ID'd, Assess) (existing process)

Oversight

- SEP and SETR (existing/new)
- PM Checklist (existing process)
- MDA, Milestone, PSR tools (existing process)

Compliance

- Acquisition Integrity Office (existing process)
- DCMA (existing process)
- CIS (existing process)



Acquisition Path Forward

- **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

Raise the bar:	
Awareness	- Knowledge of the supply chain - Who has access to our critical assets
Protection	- Protect critical assets through security practices - Engineer our systems for assurance

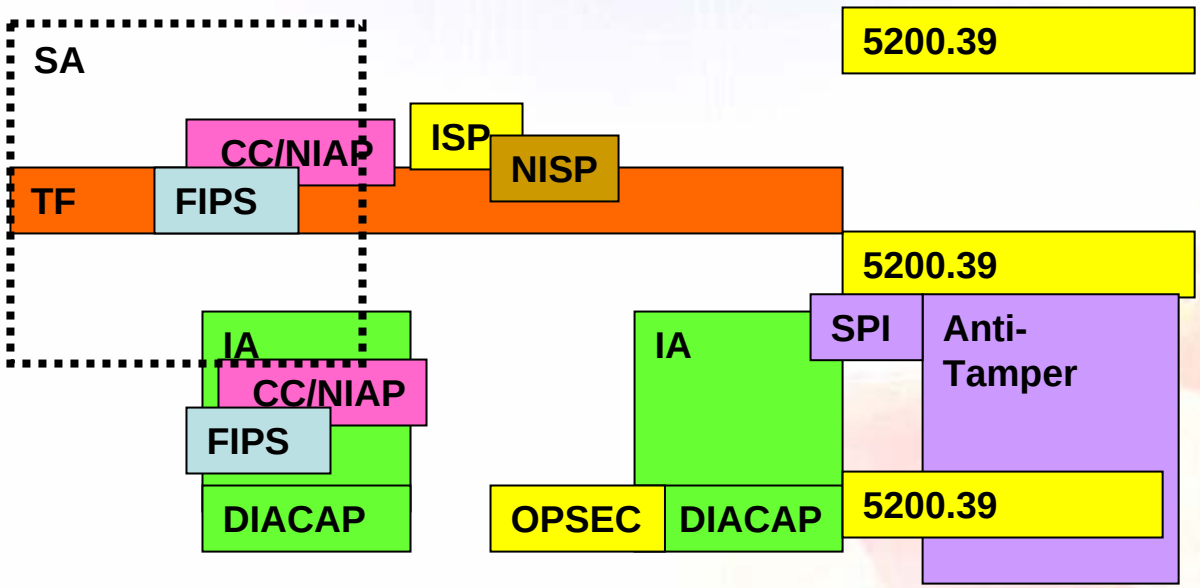
Current Systems Security Policies

Defense-In-Depth

- **Intelligence**
- **Supply Chain**
- **Engineering**
- **Certification**
- **Documented Plan**

Component Protection Sought

Critical Functionality		Critical Information		Critical Technology	
Non-Security	Security	Classified	Un-Classified	Software	Hardware/ Firmware



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

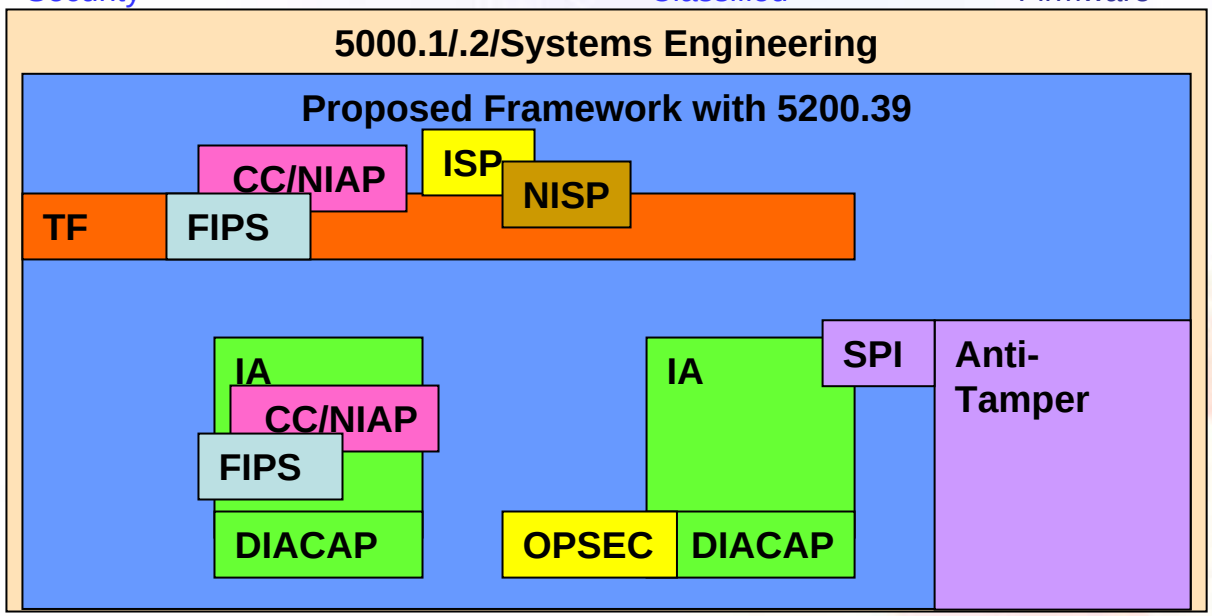
Proposed Framework for Security Policies

Defense-In-Depth

- **Intelligence**
- **Supply Chain**
- **Engineering**
- **Certification**
- **Documented Plan**

Component Protection Sought

Critical Functionality		Critical Information		Critical Technology	
Non-Security	Security	Classified	Un-Classified	Software	Hardware/ Firmware



Policy Ownership		
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.**

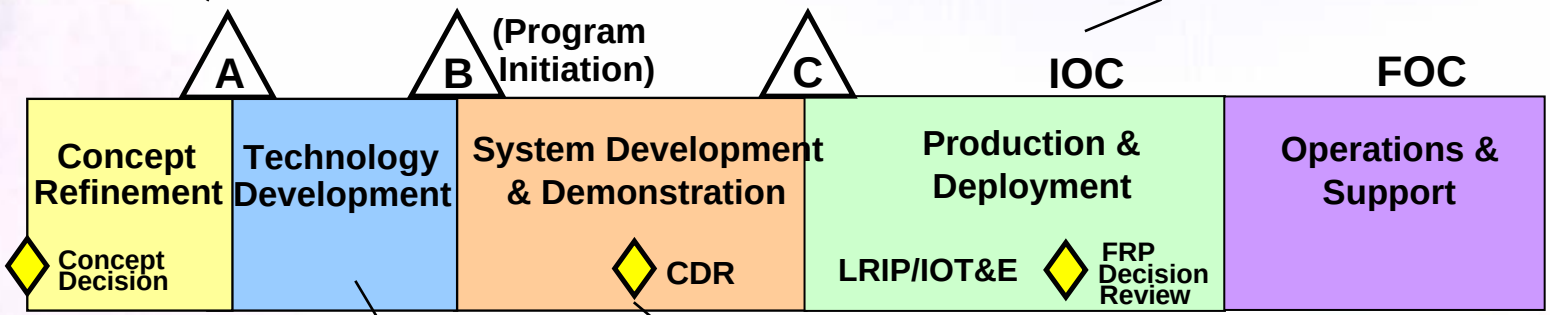
Notional Assurance Implementation

- Identify CPI
- Identify threats
- Develop Plans (SEP, TES)

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

- Conduct PSRs for Program
- Protection Plans

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



- Source selection consideration of supplier FOCI and security practices
- Technology Readiness Assessment
- CPI entered in Horizontal Protection
- Database

- Write Program Protection Plan (PPP)
- Designs meet assurance plans
- Initial verification and validation of critical components

Total Lifecycle Approach to Assured Systems

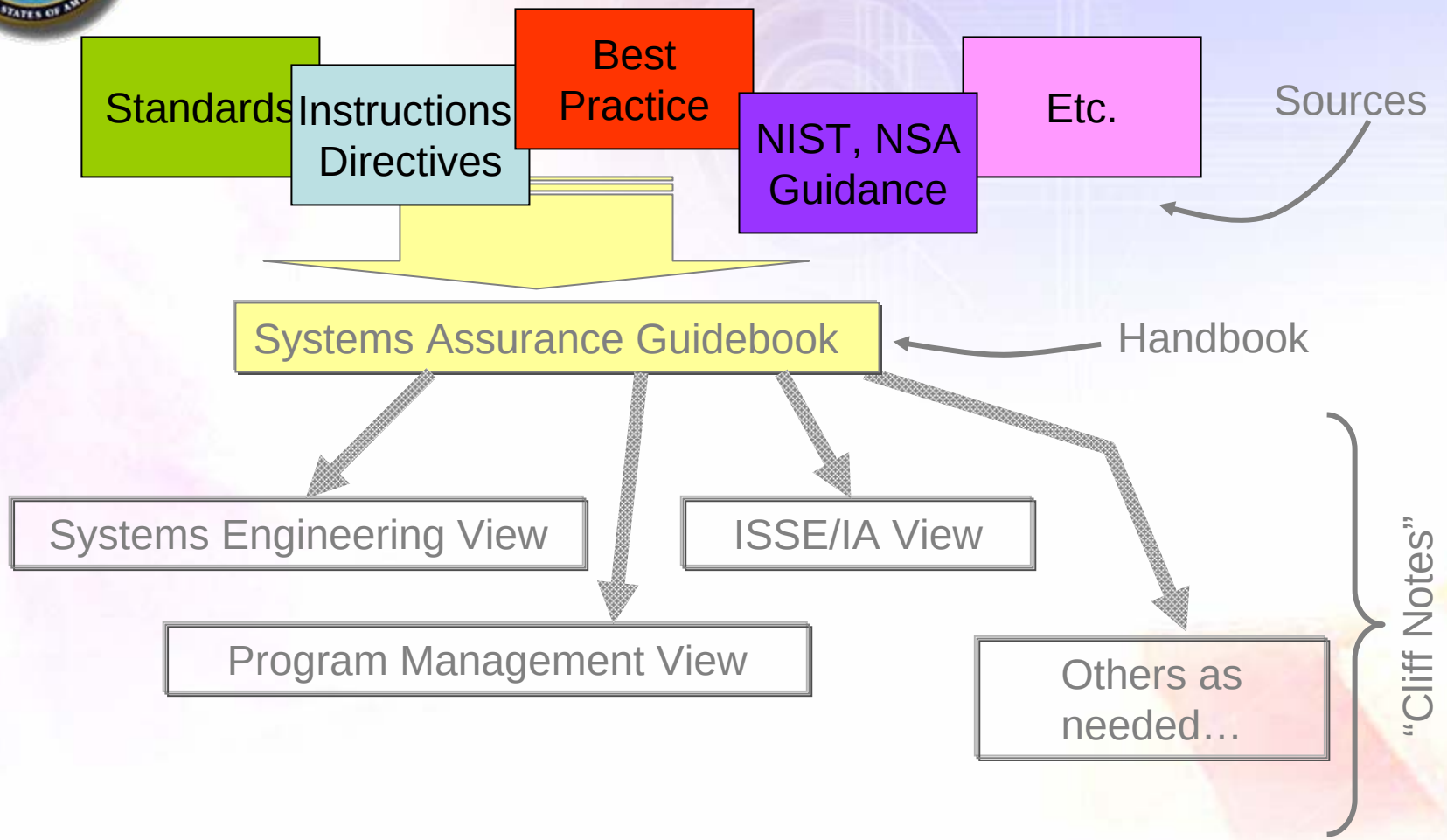
Program Protection Plans

- Policy
  - Revised DoD 5200.39 policy
  - DoD 5000.2 – Deliverable at MS B
- Guidance
    - DAG Chapter 4 and 8, modified to reflect policy changes
    - NDIA System Assurance Guidebook
    - Revised SEP and TEMP Guides
- Support
  - Develop on-site Training
    - Defining CPI consistent with new version of DODI 5200.39
    - Protecting CPI and documenting protection in PPP
  - Senior level support provided to assist programs in defining, implementing, and documenting protection of CPI in PPP

Development Path Forward - SA Guidebook

- **Augments system engineering from documentation through engineering processes and technical reviews**
  - Introduced as early as possible - Where there is the greatest impact
  - Continue through the life cycle
- **Consistent with international standard and current best practices**
  - E.g., Guidebook approach, presentation of process / procedure consistent with ISO/IEC 15288 standard for System Engineering
  - Integrates consideration and leverages numerous existing program protection or security disciplines (e.g., IA, AT, SwA, SPI, PPP)
  - Existing information security / assurance material is summarized, and leveraged by reference, not repeated
    - Enhanced vulnerability detection techniques
    - SwA Body of Knowledge
- **Intent is to provide *practical guidance* on augmenting systems engineering practice for system assurance**
  - Defines “Engineering-in-Depth”!

Guidebook Strategy



Future: Link to Acquisition Guidance, Evolve/Implement into training, education

Guidebook Construct

- **Table Of Contents**
  - 1. Introduction and Organization
    - Definition of System Assurance
    - 1.1 Scope
    - 1.2. Purpose
    - 1.3 Audiences and Applications
    - 1.4 Related Disciplines
    - 1.5 Relationships of Policies, Standards and Efforts
    - 1.6 Organization of Document
  - 2. Context of Systems Assurance
  - 3. Guidance (mapped to ISO/IEC 15288
    - 3.1 Agreement Process (ISO/IEC 15288 section 5.2)
    - 3.2 Enterprise Process (ISO/IEC 15288 section 5.3)
    - 3.3 Project Processes (ISO/IEC 15288 section 5.4.1)
    - 3.4 Technical Processes (ISO/IEC 15288 section 5.5)
  - 4. Examples
    - 4.1 Guidebook Implementation Examples
    - 4.2 Assurance Case Development Example
  - 5. Documentation Examples
  - 6. Glossary & Acronyms
  - 7. Bibliography

Contact us to participate in stakeholder review

Guidebook Construct con't

- **Table Of Contents**
  - Additional Material
    - Section A: Systems Assurance Concept and Methodology
    - Section B: Correspondence with Existing Documentation, Standards efforts, etc.
    - Section C: Contacts in Communities of Interest and Practice
    - Section D: Anti-Tamper
    - Section E: Enterprise Processes
    - Section F: Technical Guidance Research & Development (R&D)
    - Index

Contact us to participate in stakeholder review

Guidebook Status

- **Stakeholder review – Comments due 31 Oct 07**
  - Request copy for comment ATL-SSA@osd.mil
- **Comment adjudication and release by 31 Dec 07**
  - Version 0.9 of the Guidebook, to be updated over time
- **Pilots**
  - Systems Assurance innovators and areas where comprehensive expertise in one or more relevant domains exists
  - Starting Summer, 2007
- **Write specific stakeholder views**
  - Focus: Derived from the Guidebook, “get the right content” (by audience)

Contact us to participate in stakeholder review

System Assurance Overall Progress Report

System Assurance Progress Report --a sampling of activities

Requirements - JCIDS

- Modify Joint Publications & Definitions to include SA
- Modify ICD, CDD, CPD boiler plate to incorporate SA
- CPI pre-work in FAA and Functional Needs Analysis (FNA)
- Modify NR KPP Attributes to address SA
- Develop text to discuss Systems Assurance within JCIDS documents

☒ Sample boiler plate presented at SAWG meeting – 7 June 2007

Acquisition – Program Protection Planning (PPP) Process

- Define process required to identify CPI components

☒ Submitted edits to DODI 5200.39 with definition of CPI to incorporate SA interests – May 2007

☒ Drafted formal PPP review process slide set – 18 May 2007

☒ Conducted review of Component PPP processes, tools – 1 Aug 2007

☒ Developed and submitted PPP process resource estimate – 30 Aug 07

☐ Draft common PPP development process – due October 2007

System Assurance Progress Report

Development - Guidance for SEP, ISP, TEMP

- ☒ Updated Systems Engineering Plan (SEP) Guide to include system assurance – Aug 2007
- ☒ Modified Defense Acquisition Guide (DAG) Chapter 4 on systems engineering
- ☐ Modifying DAG Chapter 8

Development - Guidebook

- ☒ NDIA Guidebook released to stakeholders – 19 Sep 2007
- ☐ Adjudicate comments and release Version 0.9 – 31 Dec 2007

Oversight - SA Content for Program Support Reviews

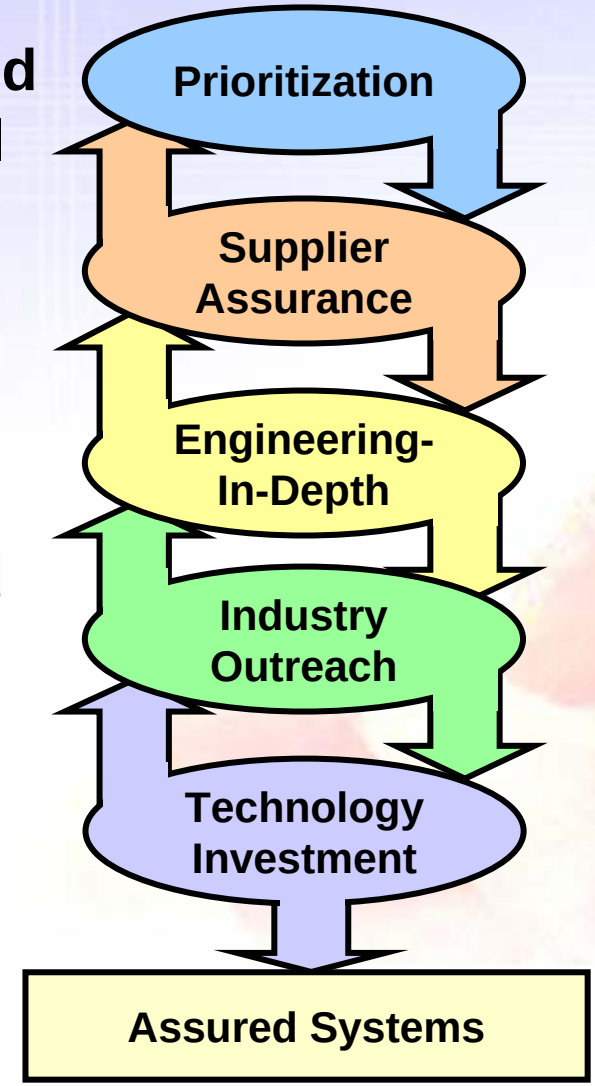
- – Define how programs should be assessed for compliance with systems assurance policy and guidance
- ☒ Developed guidance and questions – May 2007
- ☒ Conducted pilot assessment – June 2007

Intelligence Community collaboration

- ☒ Developed and submitted estimate of impact on CI resources to conduct threat assessments– May 2007

System Assurance: What does success look like?

- The requirement for assurance is allocated among the right systems and their critical components
- DoD understands its supply chain risks
- DoD systems are designed and sustained at a known level of assurance
- Commercial sector shares ownership and builds assured products
- Technology investment transforms the ability to detect and mitigate system vulnerabilities



Questions/Comments

DoD Security Policies

- **The DoD Acquisition System must develop secure weapon systems and must increase the security of the acquisition process itself.**
- **The purpose of secure warfighting systems and acquisition processes is to protect the DoD technology lead, develop warfighting systems that cannot be usurped or disabled, and ensure the secure flow of information during war and peacetime for its warfighting systems and corporate infrastructure.**
- **Primary policy concerned with securing the warfighting acquisition process and systems:**
    - DODI 5200.39 Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection

DoD Security Policies

- **Countermeasures – methods for protecting CPI**
  - System Assurance (DAG Chapter 4 & 8, MIL-HDBK-1985 Secure System Design)
  - Classification (DODD 5200.1 Information Security Program, ISP)
  - Network security (DOD8500.01E Information Assurance)
  - Secure communications (C-5200.5 Communications Security)
  - Hardcopy document markings
  - Physical security (DODI 5200.08 Security of DoD Installations and Resources)
  - Operational security (DODD 5205.02 OPSEC)

Backup Slides

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

Fragmented Systems Security Policies

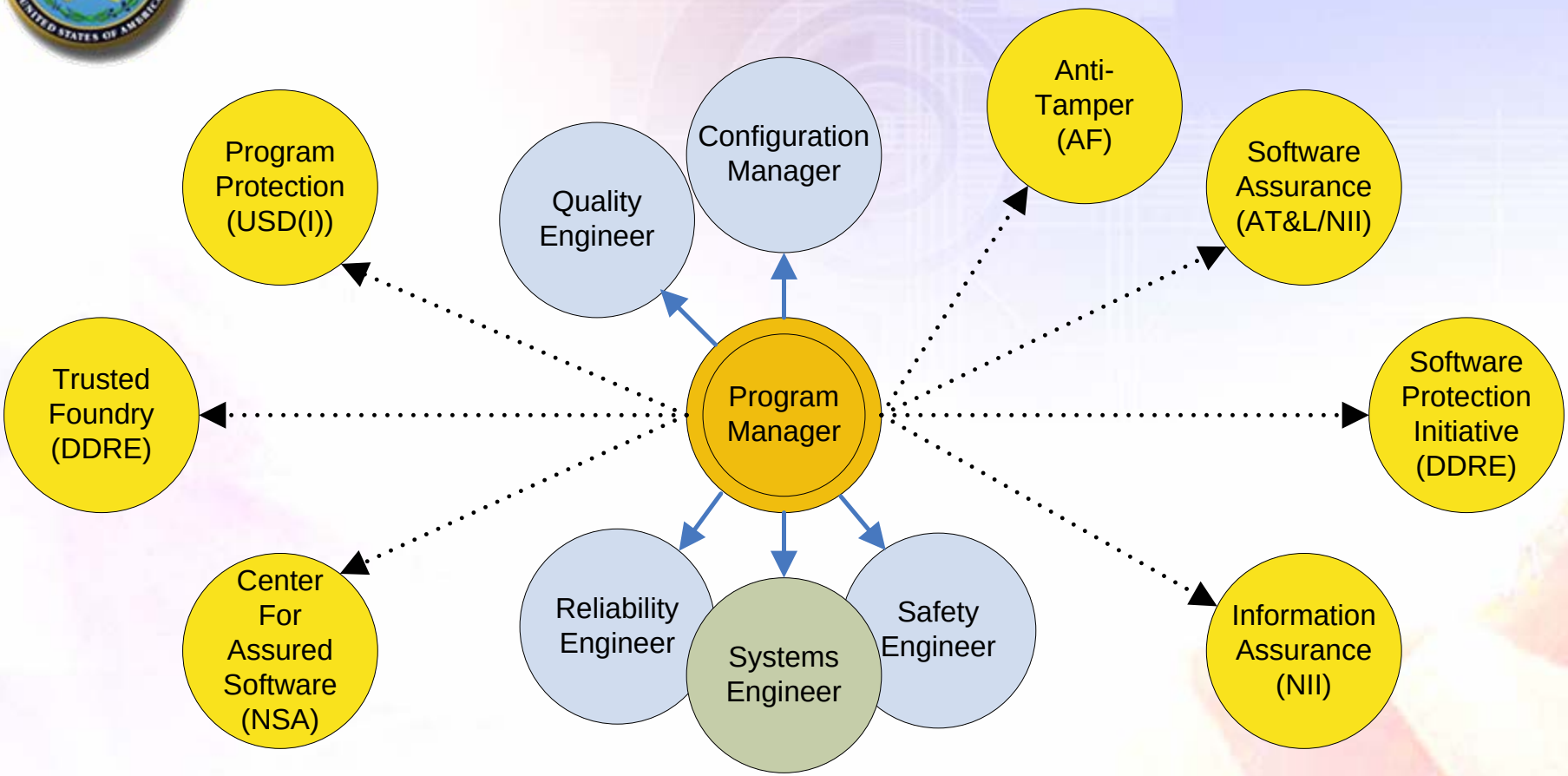
Each policy:

- **Affects different parts of the life cycle**
  - R&D, acquisition, foreign ownership
- **Applies to a different subset of DoD systems**
  - NSS, IT, MDA, ACAT 1C, etc.
- **Assures different 'type' of components**
  - information, leading technology, functionality
- **Mandates a different set of defense tactics**
  - intelligence, engineering, documented plan, certification & accreditation

- **CC – Common Criteria**
- **DIACAP – DoD Certification & Accreditation**
- **FIPS – Federal Information Processing Standards**
- **ITAR – International Traffic in Arms Regulation**
- **IA – Information Assurance**
- **ISP – Information Security Program**
- **NIAP - National Information Assurance Partnership**
- **NISP – National Industrial Security Program**
- **OPSEC – Operational Security**
- **5200.39 – DODD 5200.39 Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection**
- **SA – System Assurance**
- **SPI – Software Protection Initiative**
- **TF - Trusted Foundry**

Current approach does not have systems-of-systems perspective

System Assurance Context for the PM



System Assurance – Working 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