A Strategy for Improved System Assurance

April 2008

Bruce Amato

Acting Deputy Director,

Software Engineering and System Assurance

Office of the Under Secretary of Defense

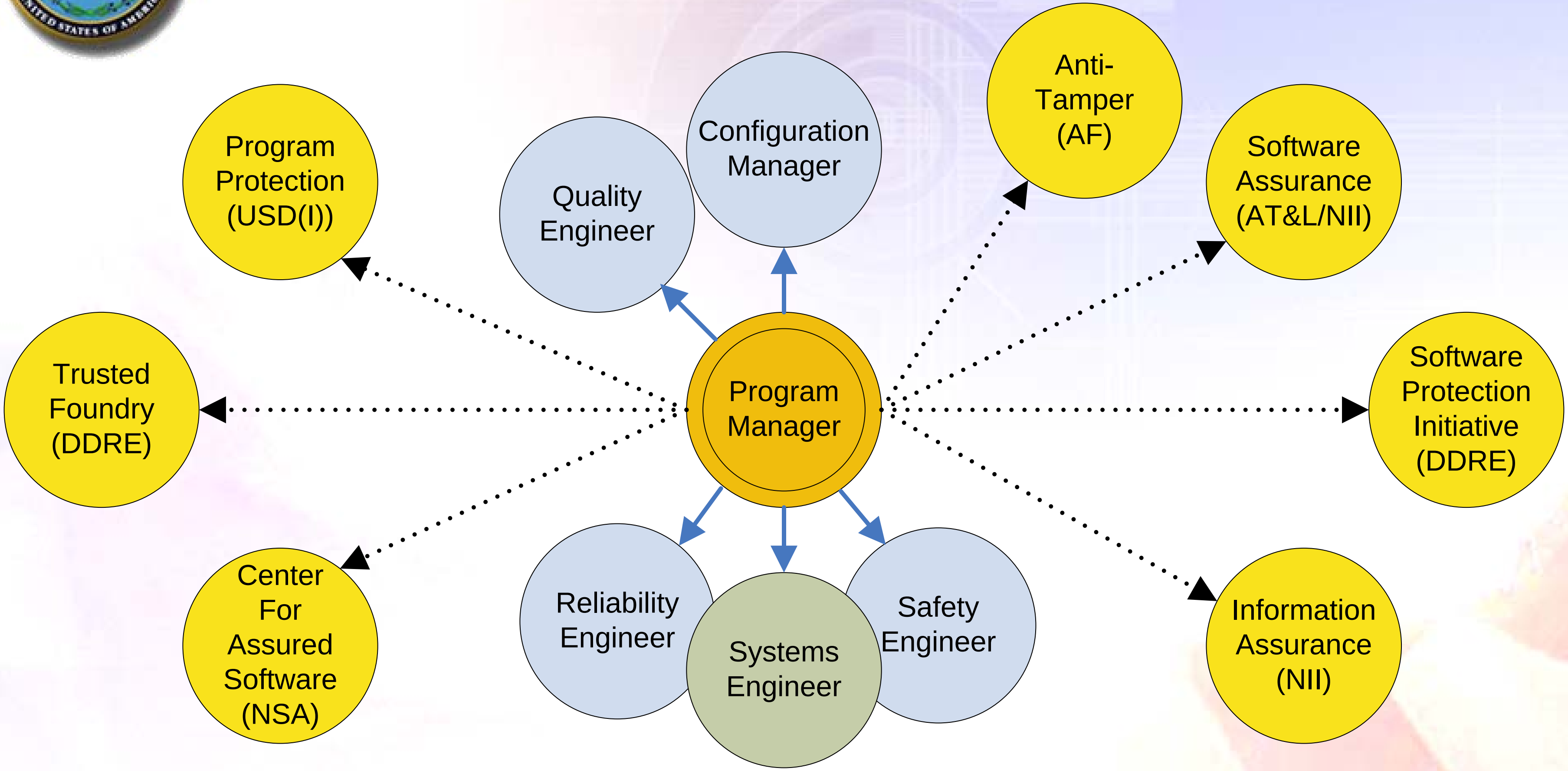
Acquisition, Technology and Logistics

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

System Assurance Context for the PM


Program Protection (USD(I))
Quality Engineer
Configuration Manager
Anti-Tamper (AF)
Software Assurance (AT&L/NII)
Trusted Foundry (DDRE)
Program Manager
Software Protection Initiative (DDRE)
Center For Assured Software (NSA)
Reliability Engineer
Systems Engineer
Safety Engineer
Information Assurance (NII)

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

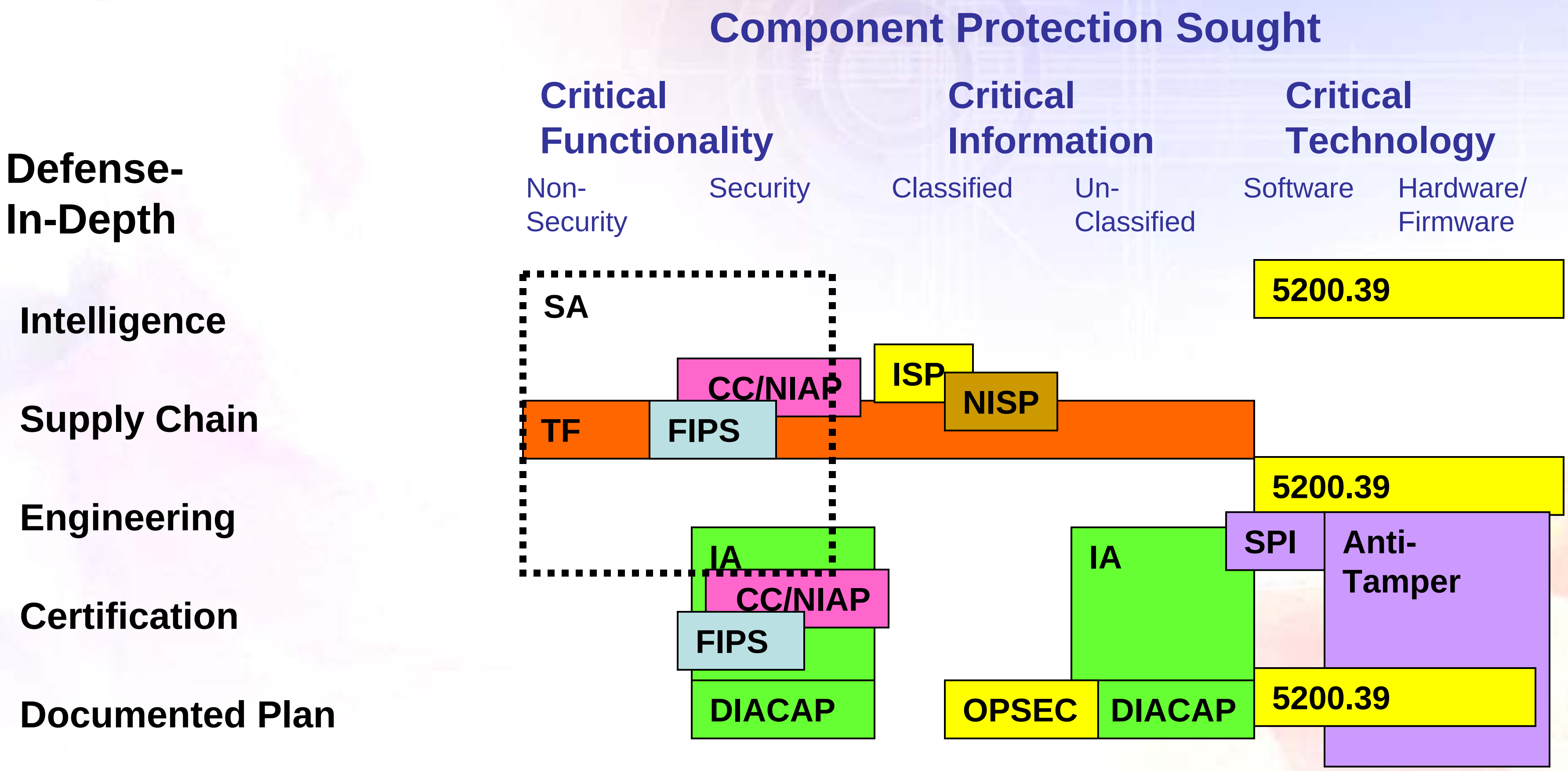
Acquisition Path Forward –
Implementing the Requirement for Assurance

Raise the bar:

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

- **Create a framework to integrate multiple security policies and guidance**
  - Leverage Program Protection requirement for all acquisition programs as set by 5200.39 policy
  - Integrate all assurance oversight, planning, and risk mitigation activity at the system level
- **Develop Guidance on Engineering for System Assurance**
  - Guidebook on Engineering for Assurance for program managers/engineers
  - Defines how assurance can be incorporated into system engineering and design:
    - e.g. Isolation, Redundancy, Quality and Fault Analysis

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

SA

5200.39

CC/NIAP

ISP

NISP

TF

FIPS

5200.39

IA

SPI

Anti-Tamper

IA

CC/NIAP

FIPS

DIACAP

OPSEC

DIACAP

5200.39

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

Defense-In-Depth

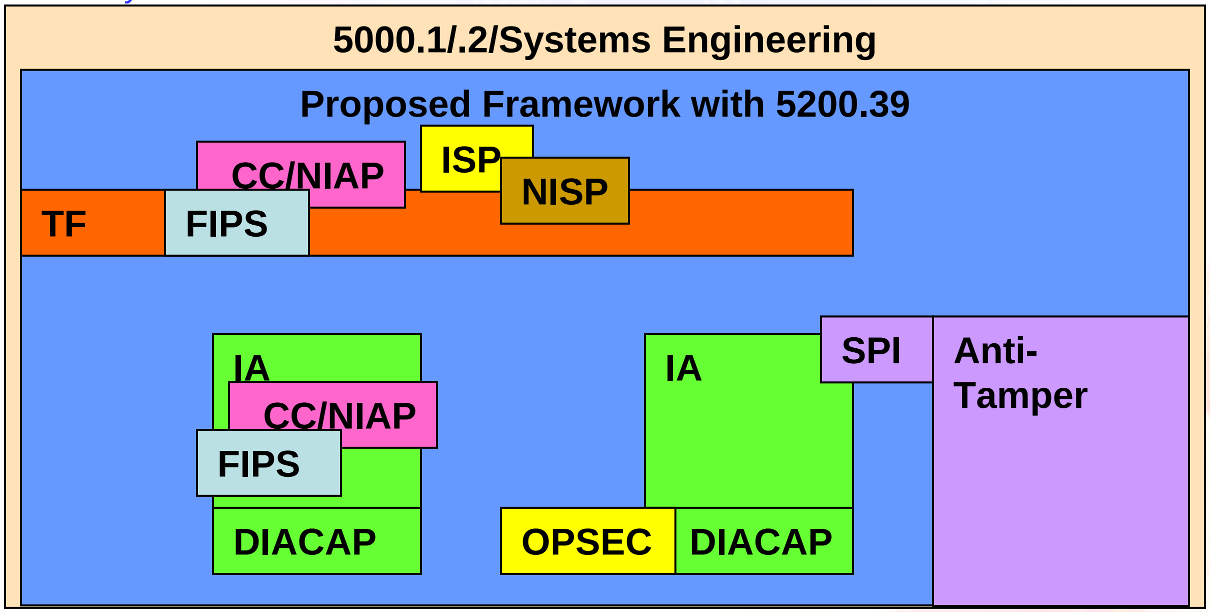
Intelligence

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

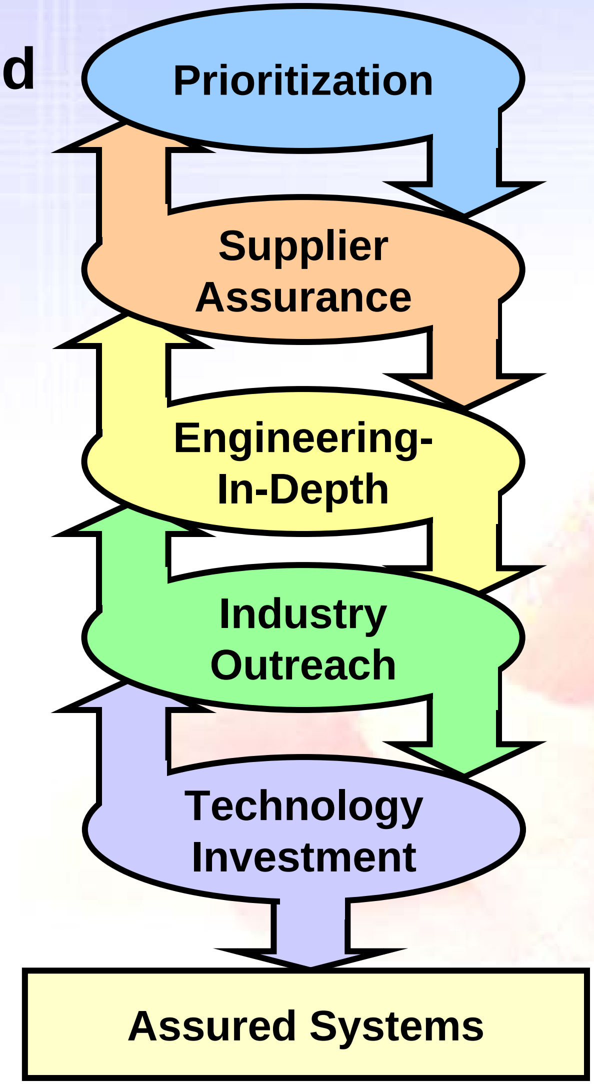
Critical Program Information

New Definition - Draft DoDI 5200.39:

- E3.6. Critical Program Information (CPI). Elements or components of an Acquisition 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.

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


Prioritization

Supplier Assurance

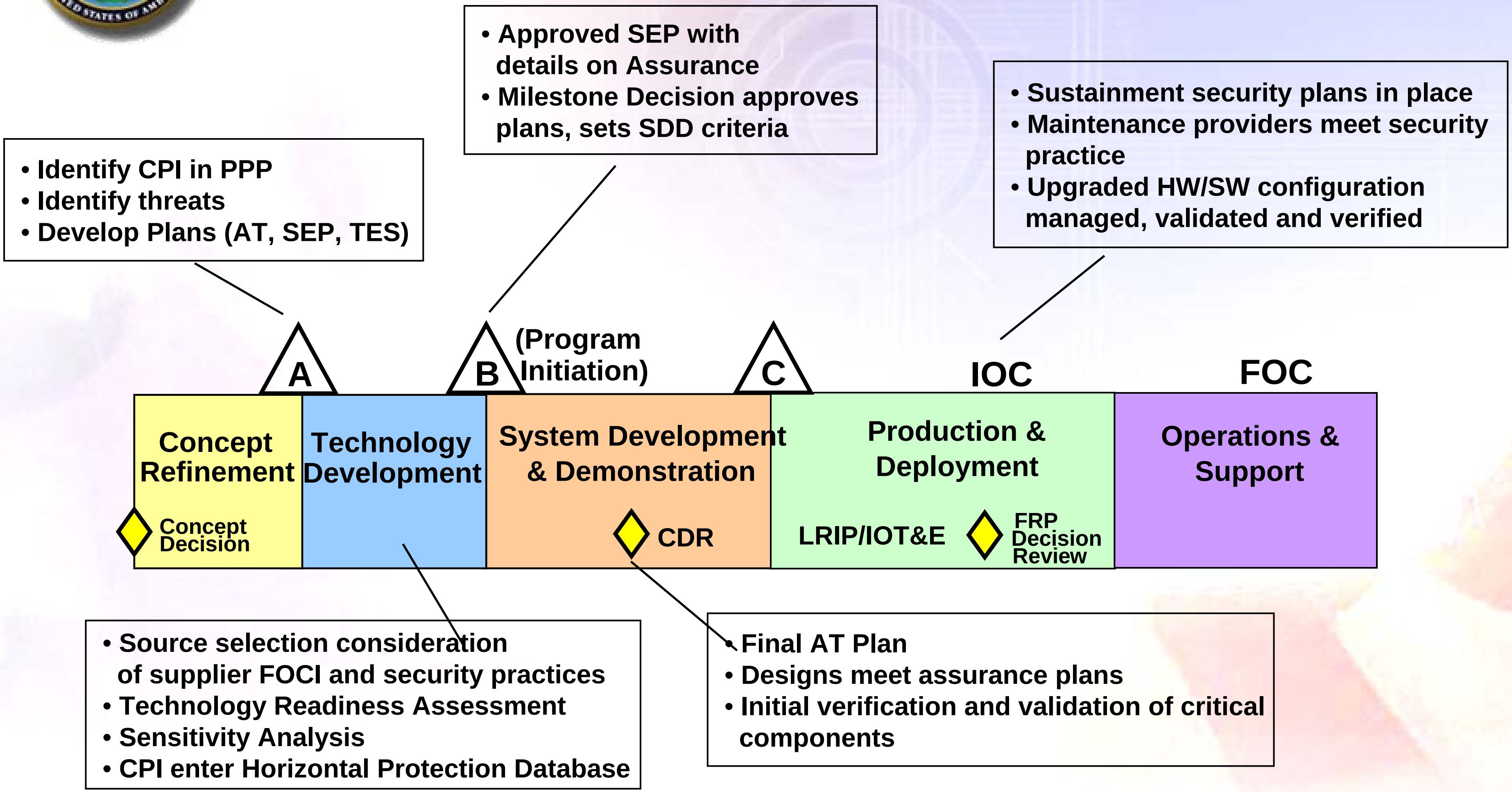
Engineering-In-Depth

Industry Outreach

Technology Investment

Assured Systems

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

Better Emphasis at writing CPI requirements

Guidebook on Engineering for System Assurance

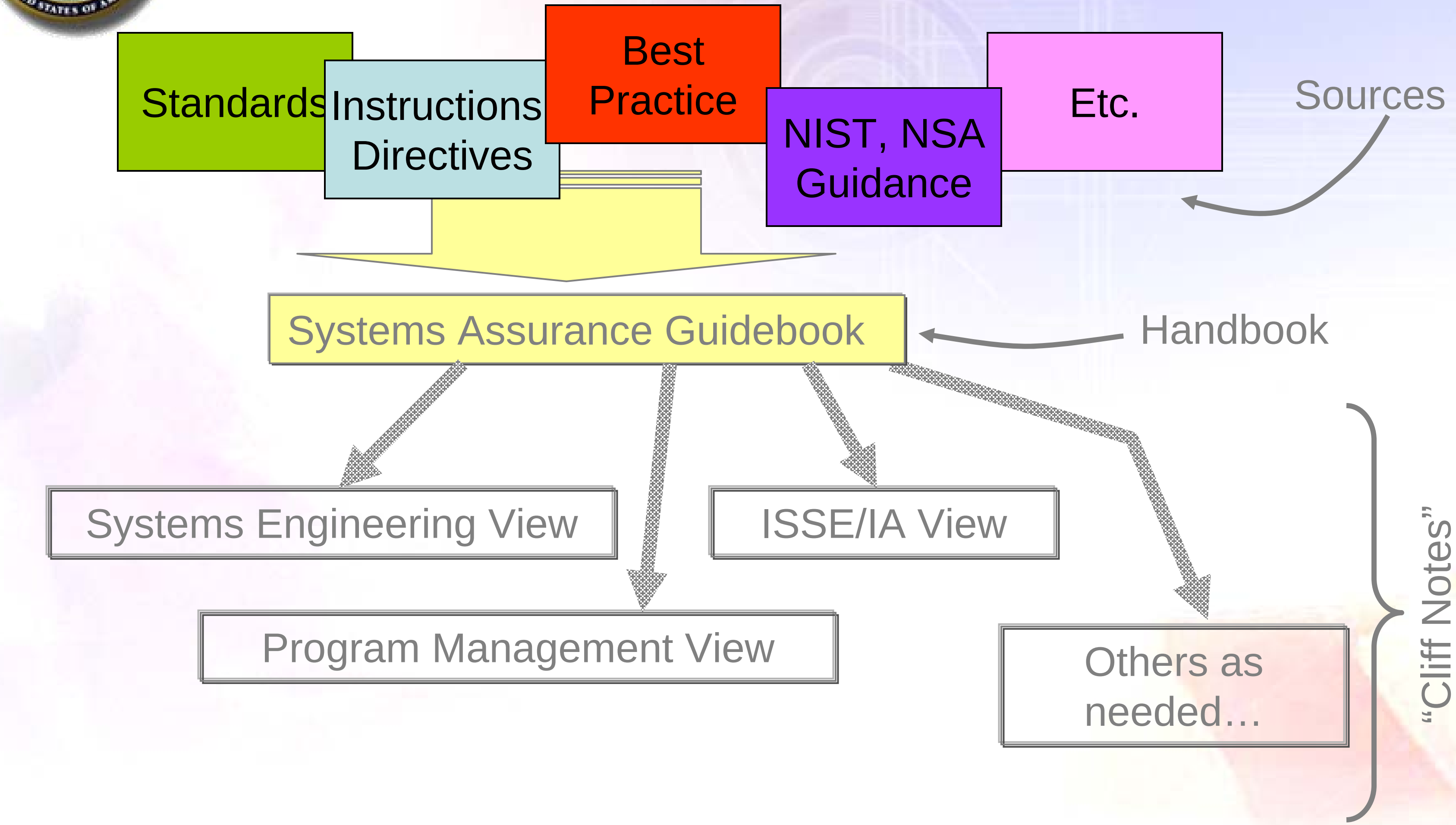
SA Guidebook Intent

- **Intent:**
  - Provide *practical guidance* on augmenting systems engineering practice for system assurance
  - Synthesize existing knowledge from organizations, standards and best practices
  - Recap concepts from standards
- **Implementation:**
  - Iterative releases with updates as new knowledge is gained and applied
  - Multiple Views for information dissemination
    - Technical Project Manager
    - System Engineer
    - Subject Matter Expert Detail

SA Guidebook – Engineering-in-Depth

- **Augments SE 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
    - Test & Evaluation; Center for Assured Software (CAS)
    - Enhanced vulnerability detection techniques
    - SwA Body of Knowledge
- **Intent is to yield assured program / system with demonstrable evidence of assurance**

Guidebook Strategy



Standards

Instructions Directives

Best Practice

NIST, NSA Guidance

Etc.

Sources

Systems Assurance Guidebook

Handbook

Systems Engineering View

ISSE/IA View

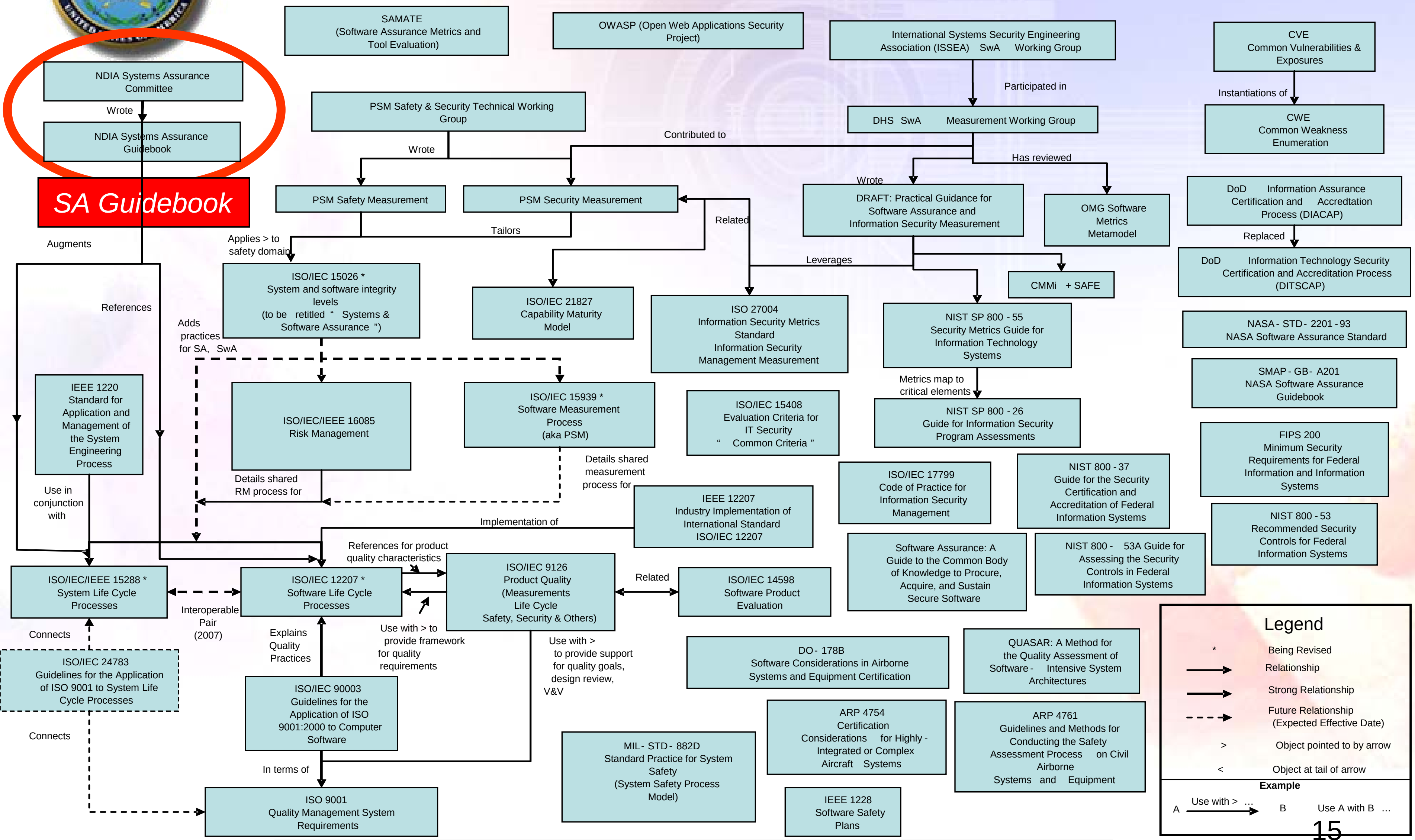
Program Management View

Others as needed…

"Cliff Notes"

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

Why this is hard…



SAMATE (Software Assurance Metrics and Tool Evaluation)

OWASP (Open Web Applications Security Project)

International Systems Security Engineering Association (ISSEA) SwA Working Group

CVE Common Vulnerabilities & Exposures

NDIA Systems Assurance Committee

Wrote

NDIA Systems Assurance Guidebook

SA Guidebook

PSM Safety & Security Technical Working Group

Participated in

DHS SwA Measurement Working Group

Instantiations of

CWE Common Weakness Enumeration

Contributed to

Wrote

Has reviewed

PSM Safety Measurement

PSM Security Measurement

Wrote

DRAFT: Practical Guidance for Software Assurance and Information Security Measurement

OMG Software Metrics Metamodel

DoD Information Assurance Certification and Accredtation Process (DIACAP)

Augments

Applies > to safety domain

Tailors

Related

Replaced

Leverages

DoD Information Technology Security Certification and Accreditation Process (DITSCAP)

CMMi + SAFE

ISO/IEC 15026 * System and software integrity levels (to be retitled " Systems & Software Assurance ")

ISO/IEC 21827 Capability Maturity Model

ISO 27004 Information Security Metrics Standard Information Security Management Measurement

NIST SP 800 - 55 Security Metrics Guide for Information Technology Systems

NASA - STD - 2201 - 93 NASA Software Assurance Standard

References

Adds practices for SA, SwA

SMAP - GB - A201 NASA Software Assurance Guidebook

Metrics map to critical elements

IEEE 1220 Standard for Application and Management of the System Engineering Process

ISO/IEC/IEEE 16085 Risk Management

ISO/IEC 15939 * Software Measurement Process (aka PSM)

ISO/IEC 15408 Evaluation Criteria for IT Security " Common Criteria "

NIST SP 800 - 26 Guide for Information Security Program Assessments

FIPS 200 Minimum Security Requirements for Federal Information and Information Systems

Details shared measurement process for

Details shared RM process for

ISO/IEC 17799 Code of Practice for Information Security Management

NIST 800 - 37 Guide for the Security Certification and Accreditation of Federal Information Systems

Use in conjunction with

IEEE 12207 Industry Implementation of International Standard ISO/IEC 12207

NIST 800 - 53 Recommended Security Controls for Federal Information Systems

Implementation of

References for product quality characteristics

Software Assurance: A Guide to the Common Body of Knowledge to Procure, Acquire, and Sustain Secure Software

NIST 800 - 53A Guide for Assessing the Security Controls in Federal Information Systems

ISO/IEC/IEEE 15288 * System Life Cycle Processes

ISO/IEC 12207 * Software Life Cycle Processes

ISO/IEC 9126 Product Quality (Measurements Life Cycle Safety, Security & Others)

Related

ISO/IEC 14598 Software Product Evaluation

Interoperable Pair (2007)

Connects

Explains Quality Practices

Use with > to provide framework for quality requirements

Use with > to provide support for quality goals, design review, V&V

DO - 178B Software Considerations in Airborne Systems and Equipment Certification

QUASAR: A Method for the Quality Assessment of Software - Intensive System Architectures

ISO/IEC 24783 Guidelines for the Application of ISO 9001 to System Life Cycle Processes

ISO/IEC 90003 Guidelines for the Application of ISO 9001:2000 to Computer Software

ARP 4754 Certification Considerations for Highly - Integrated or Complex Aircraft Systems

ARP 4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

Connects

MIL - STD - 882D Standard Practice for System Safety (System Safety Process Model)

In terms of

ISO 9001 Quality Management System Requirements

IEEE 1228 Software Safety Plans

Legend

* Being Revised

Relationship

Strong Relationship

Future Relationship (Expected Effective Date)

> Object pointed to by arrow

< Object at tail of arrow

Example

A Use with > … B Use A with B …

Related Standards, Efforts, and Working Groups…

Contributors

- **NDIA**
- **INCOSE**
- **MITRE**
- **IDA**
- **SEI**
- **OSD, Joint Staff, Services**
- **Contractor community**
- **Academe**

Milestones & Plan

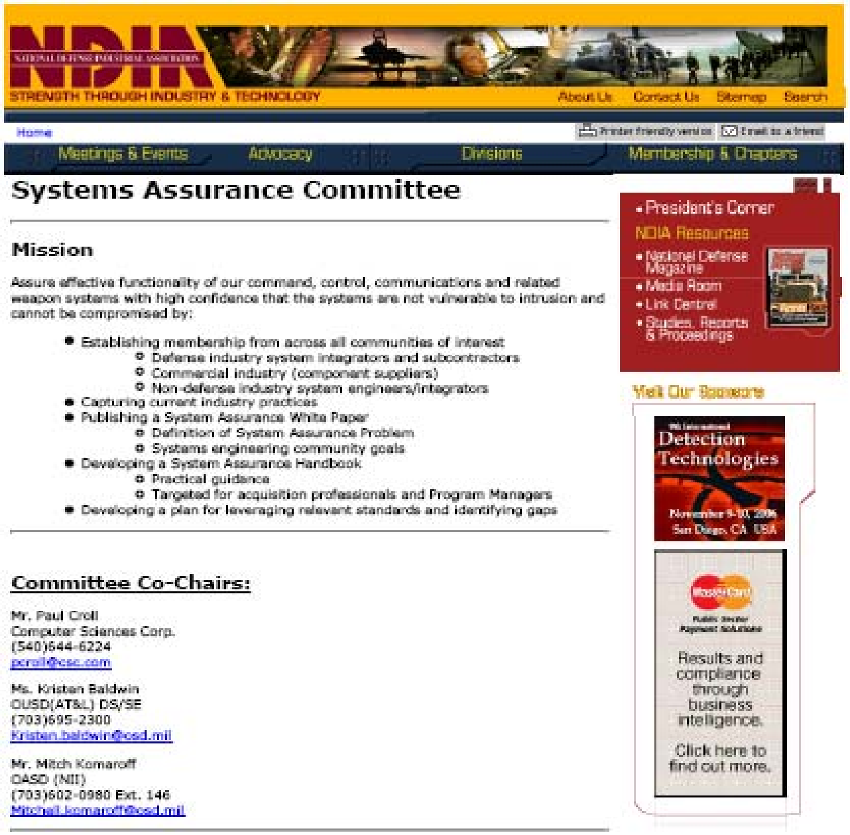
- **Stakeholder Review**
  - From the larger community, different perspectives
- **Pilots**
  - Systems Assurance innovators and areas where comprehensive expertise in one or more relevant domains exists
  - Starting FY09
- **Complete the Guidebook**
  - Release version 0.9 by 30 September 08
  - Version 1.0 in FY09

Contact Wayne Young to participate in stakeholder review

Community Site

http://www.ndia.org/Content/ContentGroups/Divisions1/Systems_Engineering/Systems_Assurance_Committee.htm

http://tinyurl.com/222hvq



Systems Assurance Committee

Mission

Assure effective functionality of our command, control, communications and related weapon systems with high confidence that the systems are not vulnerable to intrusion and cannot be compromised by:

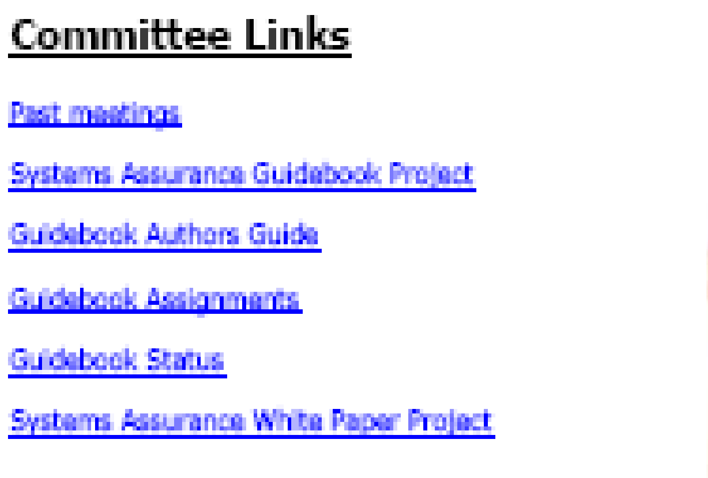
- Establishing membership from across all communities of interest
  - Defense industry system integrators and subcontractors
  - Commercial industry (component suppliers)
  - Non-defense industry system engineers/integrators
- Capturing current industry practices
- Publishing a System Assurance White Paper
  - Definition of System Assurance Problem
  - Systems engineering community goals
- Developing a System Assurance Handbook
  - Practical guidance
  - Targeted for acquisition professionals and Program Managers
- Developing a plan for leveraging relevant standards and identifying gaps

Committee Co-Chairs:

Mr. Paul Croll
Computer Sciences Corp.
(540)644-6224
pcroll@csc.com

Ms. Kristen Baldwin
OUSD(AT&L) DS/SE
(703)695-2300
Kristen.baldwin@osd.mil

Mr. Mitch Komaroff
OASD (NII)
(703)602-0980 Ext. 146
Mitchell.komaroff@osd.mil



Committee Links

Past meetings

Systems Assurance Guidebook Project

Guidebook Authors Guide

Guidebook Assignments

Guidebook Status

Systems Assurance White Paper Project

Backup Detail on Policies

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