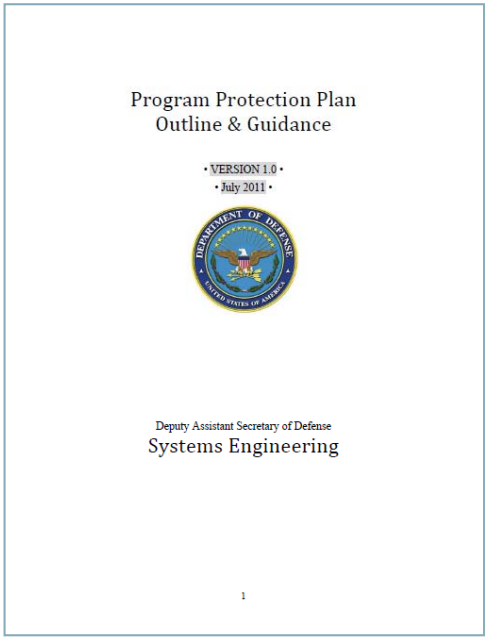
NDIA Systems Security Engineering Committee
Welcome and Update

Holly Coulter Dunlap, Chair
Beth Wilson, Alternate Chair

October 2013

Systems Security Engineering Committee

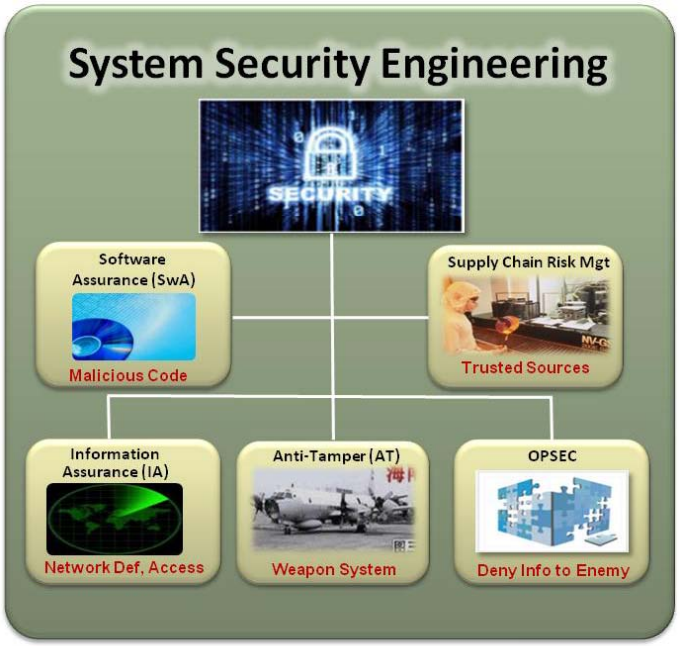
- **Restart Former Systems Assurance Committee**
- **New Systems Security Engineering Committee**
  - Kick-off held June 18, 2013
  - Track at SE Symposium and Joint track with SoS
  - Planning follow-on workshop in 2014 on Program Protection Plan


Program Protection Plan
Outline & Guidance

• VERSION 1.0 •
• July 2011 •

Deputy Assistant Secretary of Defense
Systems Engineering

1



Program Protection Plan
May 2012 Workshop Results

Rank	Issue	Status
1	Taxonomy	NDIA/INCOSE SSE to work
2	Limited Security Performance Metrics are available	NDIA SSE to work
3	Satisfying PPP Objectives through Improved Contract / Acquisition Strategy	Government has revised RFP language, still looking for examples from industry where RFP language makes it difficult to respond
4	Lack of well defined threat and attack vectors for SE community in Acquisition and Industry	Mitre working
5	Lack of education across the acquisition and industry communities with respect to SSE	DAU/Academia to work WPI online PPP certificate program announced at INOCSE IS13

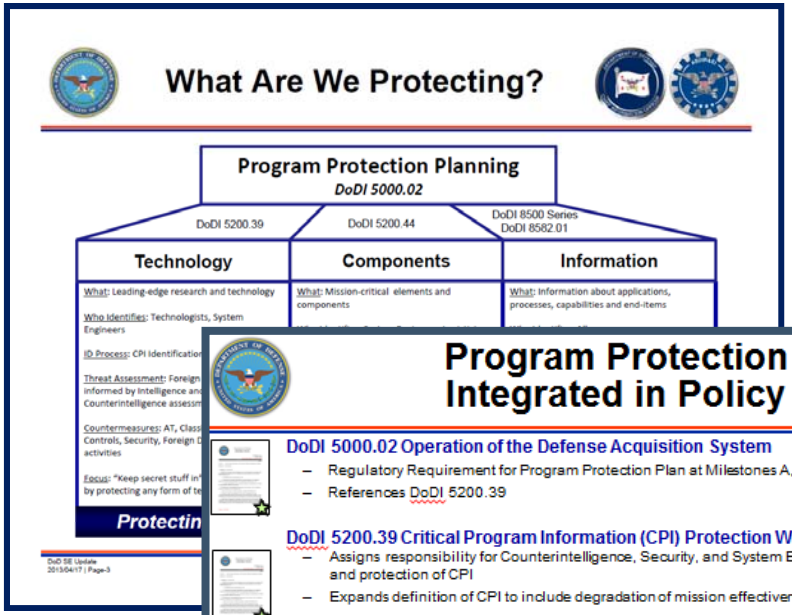
Mission Analysis Committee Project → SSE Committee

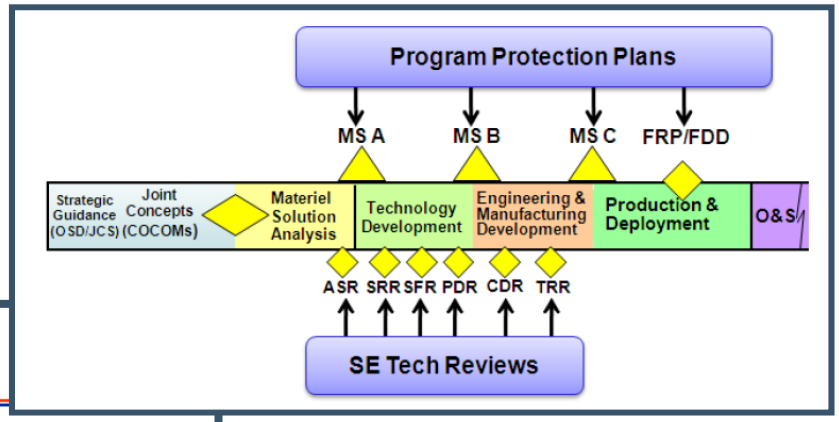
Identify PPP Enablers, Analytics, and Activities

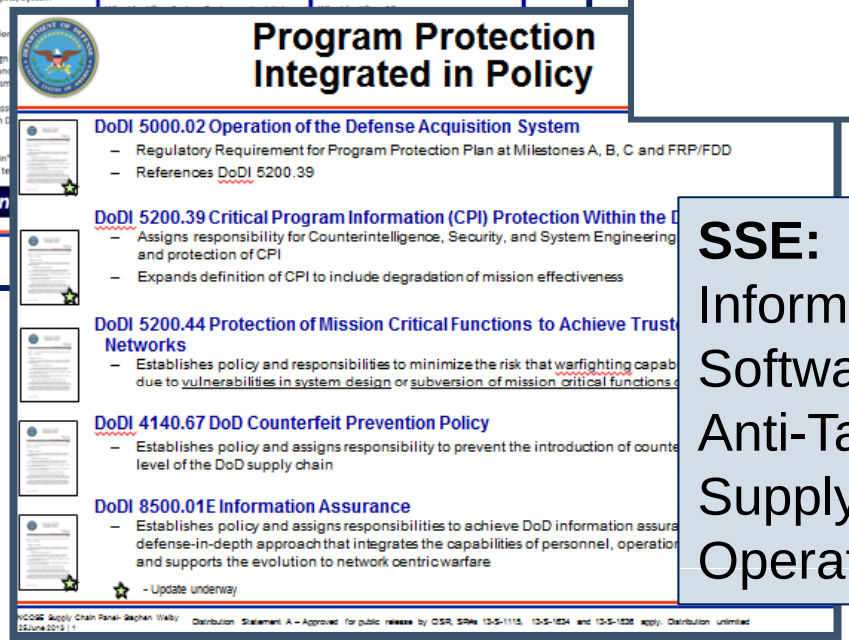
Defense Acquisition Guidebook 13.14.2. Systems Security Engineering (SSE) Process (page 1150)

	SYSTEM DEVELOPMENT LIFE CYCLE					
	MDD / MSA	A / TECH DEV	B / EMD	C / PRODUCTION	O&S	
SSE						
SwA						
SCRM						
IA						
AT						
OPSEC						

SSE Committee for Industry Perspective







SSE:
Information Assurance
Software Assurance
Anti-Tamper
Supply Chain Risk Mitigation
Operational Security

Summary

- **SSE Presence at SE Conference**
  - Tutorials
  - SSE Track
  - Joint SSE and SoS Track
  - Net-Centric Operations/Interoperability Track

- **Participation Welcome!**
  - Follow-on PPP Workshop
  - Lifecycle Activity Matrix

Backup

NDIA Program Protection Workshop

Refinement of Combined Breakout Group Top 5 Issues & Recommended Actions Summary

August 8, 2012

Combined Top 5 Issues

Rank	Group	Issue
1	3	Taxonomy
2	2	Limited Security Performance Metrics are available
3	1	Satisfying PPP Objectives through Improved Contract / Acquisition Strategy
4	2	Lack of well defined threat and attack vectors for SE community in Acquisition and Industry
5	2, 3	Lack of education across the acquisition and industry communities wrt SSE

Recommended Next Steps

Rank	Group	Issue	Next Step
1	3	Taxonomy	NDIA WG Follow-up
2	2	Limited Security Performance Metrics are available	NDIA WG Follow-up
3	1	Satisfying PPP Objectives through Improved Contract / Acquisition Strategy	Continue DASD/SE and DOD CIO piloting; Consider and where possible incorporate industry recommendations
4	2	Lack of well defined threat and attack vectors for SE community in Acquisition and Industry	• Make available attack vector study results and catalog(Mitre) • Encourage industry use of IR&D funds to address. • Consider BAA to further engage industry •Link to SERC Design Pattern countermeasures
5	2, 3	Lack of education across the acquisition and industry communities wrt SSE	DASD/SE and DOD CIO lead incorporation of SSE into Icollege, NDU, DAU ACQ 101, SE and PM Web classroom based courses, standards groups (OSG, GMU), industry associations (NDIA, INCOSE, … and University SE Curriculums

1. Group 3 Issue 2: Taxonomy

Discussion Points:

- Integration of the DoD security disciplines is hampered by terms of reference that have different meanings depending on the discipline or the context.

- The scope of each discipline is not well defined. Some threats and attacks overlap the disciplines, while other vulnerabilities to threats and attacks seem to fall outside the scope of the PPP as well as each of the enumerated security disciplines.

Recommendations:

1.Hold classified information sharing workshop to categorize attacks and threats, and determine how they apply to each security discipline. Rescope PPP and disciplines as necessary. Action: DASD/SE, DoD CIO

2.Review, consolidate, deconflict, and establish common terms of reference across disciplines. Define AT terms in the DAG, DoDI 5200.39, and the 8500 series. Once established, publish each of the security discipline terms in DoD issuances, such as DoDI 5200.39, DAG, and CNSSI 4009. Action: DASD/SE, NSA/I8, Anti-Tamper Executive Agent (ATEA, SAF/AQLS).

2. Group 2 Issue 5: Limited security performance metrics are available

Discussion Points:

- Lack of performance metrics to ensure program protection requirements.

Recommendations:

1. Have the NDIA SA committee establish a working group to develop metrics which considers the following guidance from the breakout group:

- Establish criteria and evaluation methodologies for validation of program protection requirements.
  - Explore how the AT community has used residual vulnerabilities as performance metrics for security performance and countermeasure tree analysis for validation.
- Gather data to understand the relationship between vulnerabilities at each lifecycle phase and the practices used to avoid or mitigate them; establish performance baseline.
- Actively engage in SE related FISMA metrics development.
- Consider partnering with INCOSE SSE WG

3. Group 1; Issue 1: Program Contracts & Acquisition strategy Does Not Currently Clearly Define PPP Requirements

Discussion Points:

- Robust integrated program protection contracts & acquisition strategy in requests for proposals (RFPs) will reduce variation, increase the likelihood the customer will receive what they expect, drive data based decisions to reduce risk to customers, programs, and contractors, and provide a means to increase accountability.

Recommendations:

Government Action

Recommendation 1:

Consider a Supply Chain risk analysis as a part of a trade study step when the government wants a consistent approach to all responses. A Risk analysis trade space based upon criticality, costs, schedule, and performance to drive the program supply chain acquisition strategy (pre-RFP).

It can also be used to develop original company research for innovative solutions to meet the requirements as part of a response to an RFP.

- Source of Supply
- V&V (including in process) Testing (eg AS5553)
- SCRM Risk Mitigation Methods
- Purchasing Information & Verification
- Material Control
- Reporting Requirements

Government Action

Recommendation 2:

Include the contractors process and approach to SCRM in Sections L&M

- RFP Section L, Requirements, & Section M, Evaluation Criteria, need to address the different stages of acquisition.
- Include the program supply chain acquisition strategy developed in the AoA, as appropriate.
- RFP for the Tech Development Phase should require specific test events of PPP features (AT/IA/SCRM screening) prior to MS(B).

3. Group 1; Issue 1 Continue: Program Contracts & Acquisition Strategy Does Not Currently Clearly Define PPP Requirements

Recommendation 3:

Government Action

Require a government review of PPP contractor solutions

- The proposal development schedule should require government program office to review and approve the proposed PPP contractor solutions (AT / SCRM / SwA) at every major SE review (e.g SRR, SFR, PDR, CDR).

Recommendation 4:

Government Action

Communicate Security, Classification & Safety Guidance with the RFP in the PPP requirements.

- SCRM needs to be addressed in the Program Security Guidance. Within an RFP, any unique SCRM requirements need to be identified.
- Include a paragraph which identifies documents for security and safety compliance.

Government Action

Recommendation 5:

Address Horizontal Protection Requirements in RFP

- Develop a template that would include a paragraph for the contractor to identify requirements of "inherited CPI" and donor program.

4. Group2; Issue 1: Lack of well defined threat and attack vectors for SE community in Acquisition and Industry

Discussion Points:

- At early stages, SE doesn't have good understanding of threat & attack vectors
- How to apply attack vectors to early system concepts
- Probability of occurrence? (developing risk cubes)
- Requirements / counter-measures / mitigation for design development (Sects. 3 & 4 of specs)

Collaborate across the program protection seams

Recommendations:

Recommendation 1'. Encourage government and industry to define and publish threat and attack vectors for supply chain through IR&D, government research and funded activities

- Gather and refine a catalog of attack vectors and associated context information for threat events (i.e., the execution of those attack vectors)
- Gather and refine a catalog of countermeasures mapped to the attack vectors associated. These countermeasures would include:
  - appropriate design-attribute type countermeasures, as well as their translation into system requirements
  - process-activity type countermeasures, as well as their translation into SOW requirements
- Publish the results (with appropriate classification)

5. Group2 Issue 3: Lack of education across the acquisition and industry wrt SSE

Discussion Points:

How to disseminate best practices lessons learned to respond to Program Protection
Difficult to distinguish “CPI” from “Critical Components”

Recommendations:

Recommendation 1. Government and Industry needs to develop training for acquisition and engineering communities.

- Government to work with National Defense University, Icollege, DAU, Universities and Industry Associations to make courses available

Recommendation 2. Increase information sharing of approved countermeasures.

- Government and industry to apply research to develop secure design constructs and security improved acquisition process through government funded research, industry IR&D and other industry investments

Recommendation 3. Better define SSE skills sets which are required.

Recommendation 4: Improve guidance to distinguish CPI from CC.