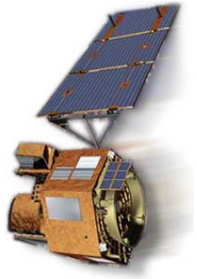
CSC
NORTH AMERICAN
PUBLIC SECTOR

Strategies for Program Protection – Identifying Risks and Setting Requirements






Paul R. Croll
Fellow
CSC
pcroll@csc.com

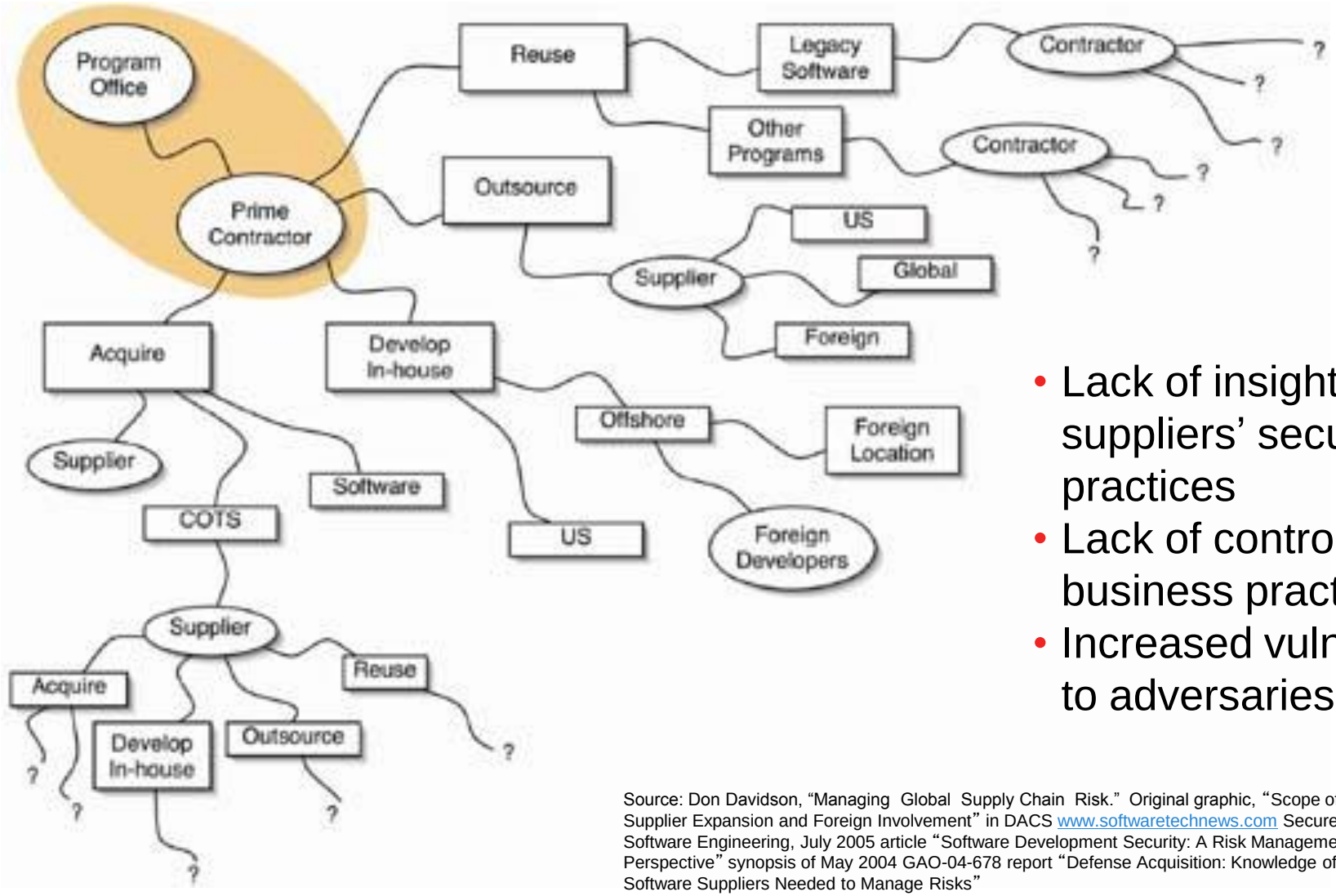
Outline

- Scope of the Problem
- Program Protection in the DoD Context
- Results of the NDIA Program Protection Workshop
- Next Steps

NORTH AMERICAN
PUBLIC SECTOR

Scope of the Problem

Globalization Brings Program Protection Challenges



- Lack of insight into suppliers' security practices
- Lack of control over business practices
- Increased vulnerability to adversaries

Source: Don Davidson, "Managing Global Supply Chain Risk." Original graphic, "Scope of Supplier Expansion and Foreign Involvement" in DACS www.softwaretechnews.com Secure Software Engineering, July 2005 article "Software Development Security: A Risk Management Perspective" synopsis of May 2004 GAO-04-678 report "Defense Acquisition: Knowledge of Software Suppliers Needed to Manage Risks"

Scope of The Cybersecurity Problem

Size in FP	Civilian Government Projects	Military Projects	*Average*
1	1	1	*1*
10	5	4	*5*
100	29	14	*24*
1,000	155	55	*120*
10,000	832	209	*600*
100,000	4,467	794	*3,031*
1,000,000	23,988	3,020	*15,412*
Average	*4,211*	*585*	*2,742*

Figure 1. Estimated Number of Security Vulnerabilities in Software Applications. Source: Capers Jones © 2008

Size in FP	Civilian Government Projects	Military Projects	*Average*
1	25.00%	5.00%	*11.29%*
10	35.00%	15.00%	*26.00%*
100	45.00%	20.00%	*33.57%*
1,000	62.00%	30.00%	*54.57%*
10,000	80.00%	35.00%	*74.00%*
100,000	87.00%	40.00%	*80.14%*
1,000,000	92.00%	45.00%	*86.29%*
Average	*60.86%*	*27.14%*	*52.27%*

Figure 2. Probability of Serious Security Vulnerabilities in Software Applications. Source: Capers Jones © 2008

- For military projects, as one approaches systems the size of typical large combat systems (expressed as function points), the estimated number of security vulnerabilities rises to above 3000 and the probability of serious vulnerabilities rises to over 45%
- The statistics are much worse for civilian systems. As we move more and more into COTS and open source software for our combat systems, one might expect that the true extent of vulnerabilities in our systems would lie somewhere between those of military and civilian systems.

COTS and Open Source Exacerbate the Problem

- Reifer and Bryant studied 100 packages were selected at random from 50 public Open-Source, COTS, and GOTS libraries
  - Spanned a full range of applications and sites like SourceForge
  - Over 30% of Open Source and GOTS (Government Off the Shelf) packages analyzed had dead code
  - Over 20% of the Open Source, COTS, and GOTS packages had suspected malware
  - Over 30% of the COTS packages analyzed had behavioral problems
- Reifer and Bryant conclude that the potential for malicious code in applications software is large as more and more packages are used in developing a system.

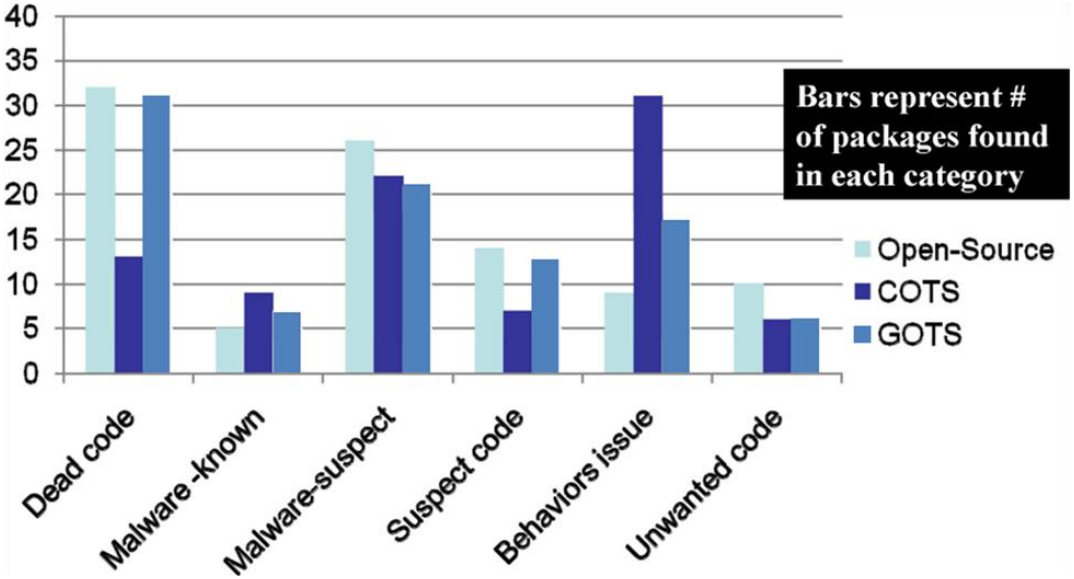


Figure 5. COTS Study Findings. *Source: D. Reifer and E. Bryant, Software Assurance in COTS and Open Source Packages, DHS Software Assurance Forum, October 2008*

It Is Difficult to Verify the Security of COTS Products

- Miller describes COTS products as black boxes to their customers
  - No means to review the code or the architecture
  - Veracity of security claims relies on the developers reputation, published security reports, and security forums
  - Vendors coding practices are largely unknown
  - COTS software is generic and does not typically address your specific operating environment, requiring careful configuration for secure operation
- Miller also points out that COTS software is generally a more attractive target than custom code

Source: Miller, C. *Security Considerations in Managing COTS Software*, Cigital, Inc. 2006, Department of Homeland Security, Build Security In

CSC

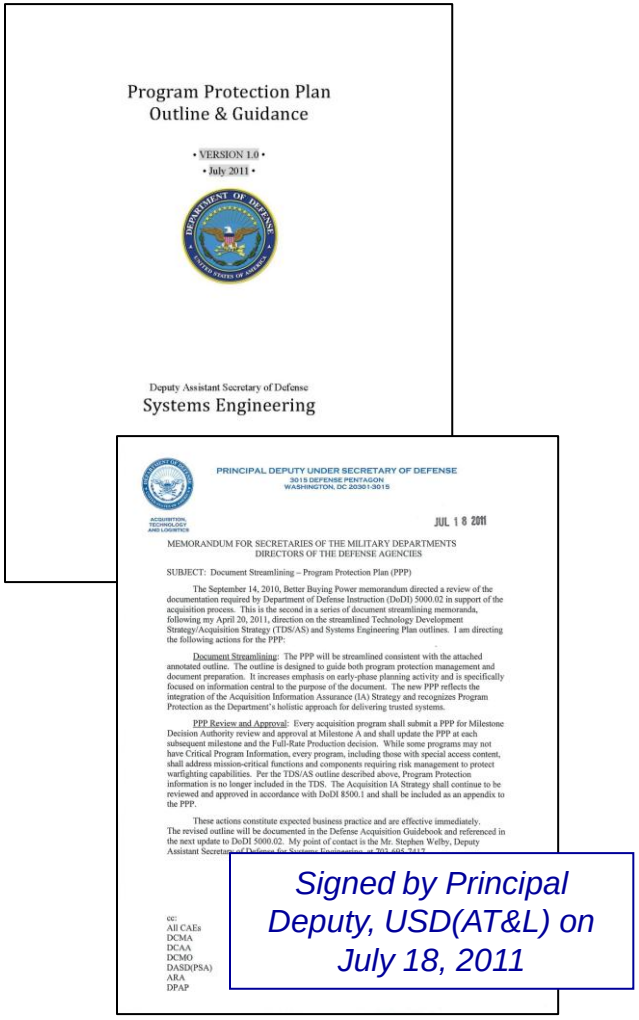
NORTH AMERICAN
PUBLIC SECTOR

Program Protection in the DoD Context

Program Protection

The integrating process for managing risks to advanced technology and mission-critical system functionality, from foreign collection, design vulnerability or supply chain exploit/insertion, and battlefield loss throughout the acquisition lifecycle.

Program Protection Plan (PPP) Outline and Guidance as "Expected Business Practice"



Signed by Principal Deputy, USD(AT&L) on July 18, 2011

What's in the Policy Memo?

– *"<u>Every acquisition program</u> shall submit a PPP for Milestone Decision Authority review and approval at Milestone A and shall update the PPP at each subsequent milestone and the Full-Rate Production decision."*

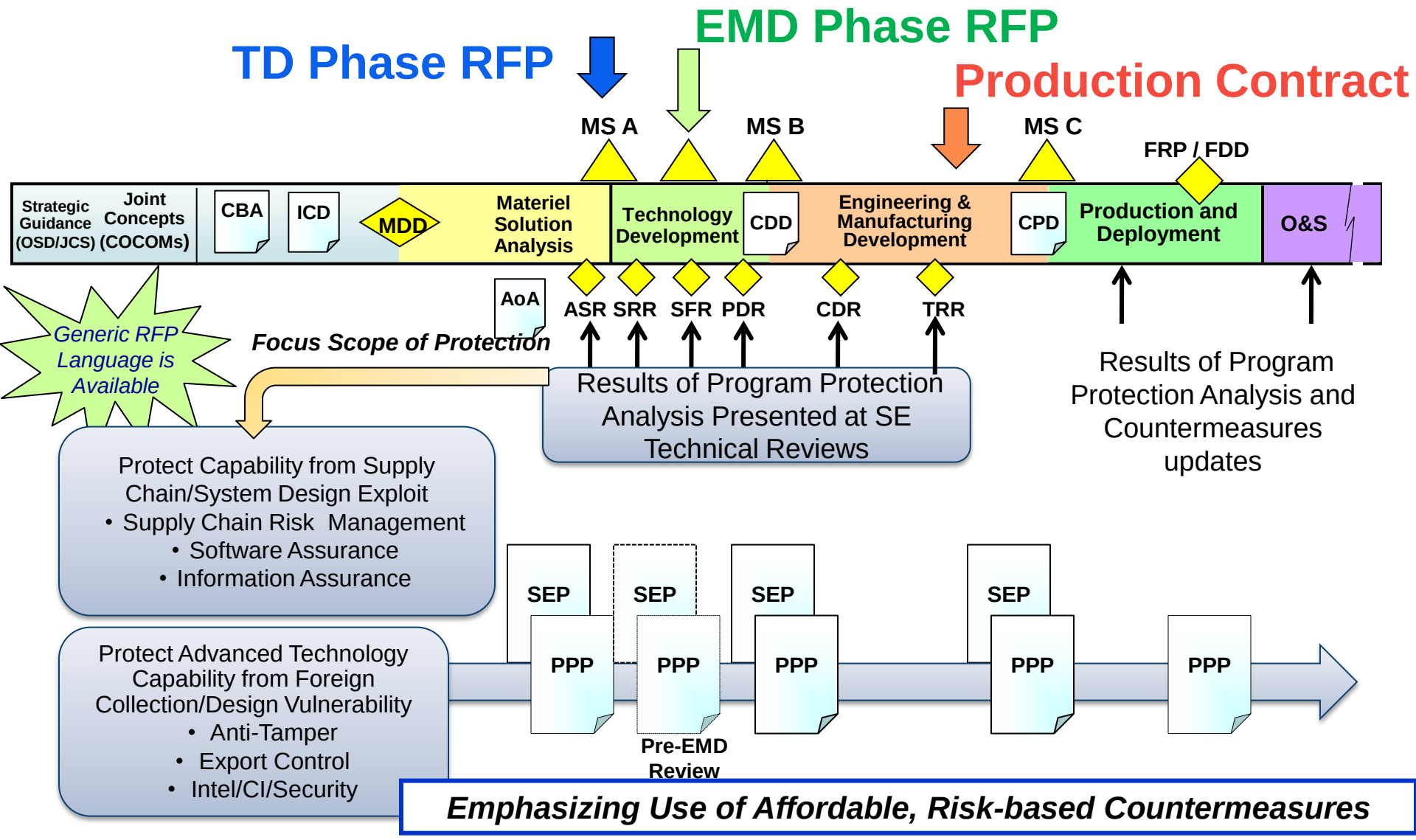
– Expected business practice, effective immediately, and reflected in upcoming DoDI 5000.02 and DAG updates

The PPP is the Single Focal Point for All Security Activities on the Program

http://www.acq.osd.mil/se/pg/index.html#PPP

Source: Kristen Baldwin, Principal Deputy, DASD/Systems Engineering

Program Protection Embedded in SE Technical Reviews



Source: Melinda Reed,, DASD/Systems Engineering

Key Elements of the PPP

Key Sections	Rationale
3.0 CPI and Critical Components (CC) – Documents output of Research & Tech. Protect and Criticality Analysis – Distinguishes between inherited and organic elements	**Focus protection on critical technology, information, and components**
4.0 Horizontal Protection – Assessment of similar CPI on other DoD programs	**Protect technologies across the DoD**
5.0 Threats, Vulnerabilities and Countermeasures – Identifies collection, supply chain, and battlefield threats – Documents assessment of vulnerability to threats and mitigating actions	**Acknowledge advanced, persistent threat** **Assess weaknesses to documented threats and use risk-based mitigations**
6.0 Other Plans – Pointers to related documents (CI Support Plan, TEMP, etc.)	**Reference, not duplicate, key documents**
7.0 Residual Risk Assessment – Document unmitigated risks to CPI and CC compromise	**Document risks program is assuming**
8.0 Foreign Involvement – Identify known and potential foreign military sales, and direct commercial sales	**Drive export realism and prepare for export-specific measures early**
9.0 Processes for PM Oversight & Implementation	**PM Resources and Implementation Reviews**
10.0 Processes for Monitoring & Reporting Loss of CPI and CC	**Assess effectiveness of implemented countermeasures**
11.0 Costs – Estimate of implementation costs for CPI and CC protection	**Support cost/benefit assessment of risk mitigations**

Source: Kristen Baldwin, Principal Deputy, DASD/Systems Engineering

CSC

NORTH AMERICAN
PUBLIC SECTOR

Results of the NDIA Program Protection Workshop

Background

- The NDIA System Assurance Committee, in conjunction with the Department of Defense OUSD(AT&L)/SE, convened a workshop on Strategies for Program Protection – Identifying Risks and Setting Requirements, May 1 – 2, 2012.
- This workshop was cosponsored by OMG, TechAmerica, and the NDIA Cyber Division.
- Workshop Description
  - The workshop was intended to examine the challenges in implementing an effective Program Protection strategy and produce prioritized recommendations and a timeline for action.
  - Three breakout groups were formed:
    - Group 1 – Industry Contracting Perspectives, Strategies and Recommended Actions, including Supply Chain Risk Management
    - Group 2 – System Security Engineering for Program Protection, including Software Assurance
    - Group 3 – Integrating Security Disciplines to Support Program Protection Objectives, including Consistency of Terminology

Consolidated Issues

	A	B	C
1	NDIA Program Protection Workshop		
2	Consolidated Issues		
3		Votes	Rank
4	Group 1 Issues - Industry Contracting Perspectives		
5	1.Satisfying PPP objectives through improved Contract/Acquisition Strategy	21	3
6	2.Vague/Insufficient Requirements	11	
7	3.Need to improve Risk Identification/Allocation Process	12	
8	4.Lack of IP Control	3	
9	5.Need for Unified PPP Decision Authority/Approval Process	14	
10	6.Lack of Clear/Timely Test and Verification Events	9	
11	7.Need a Unified, Security Centric Assessment/Guideline Process	11	
12	Group 2 Issues - System Security Engineering		
13	1.Lack of well defined threat and attack vectors for SE community in Acquisition and Industry	19	4
14	2.Lack of understanding of PPP tailoring: Industry needs additional info re: what detail is needed at each life cycle phase	10	
15	3.Lack of education across the acquisition and industry communities wrt SSE	18	5
16	4.Lack of specific guidance for software assurance risk assessment	8	
17	5.Limited security performance metrics are available	25	2
18	Group 3 Issues - Integrating Security Disciplines		
19	1.Challenges to Process Integration	11	
20	2.Taxonomy	26	1
21	3.Education/Training	8	
22	4.CPI Reform	10	
23	5.Horizontal Protection	10	
24	6.Metrics	6	

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

Top Issue 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 Anti-Tamper 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).

Top Issue 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

Top Issue 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

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

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).

Top Issue 3 (Group 1 Issue 1: Program Contracts & Acquisition Strategy Does Not Currently Clearly Define PPP Requirements) (Cont.)

Government Action

3. 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).
4. Communicate Security, Classification & Safety Guidance with the RFP in the PPP requirements.

Government Action

   - 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.
5. Address Horizontal Protection Requirements in RFP

Government Action

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

Top Issue 4 (Group 2 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
  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)

Top Issue 5 (Group 2 Issue 3: Lack of education across the acquisition and industry wrt Secure Systems Engineering)

- Discussion Points:
  - How to disseminate best practices lessons learned to respond to Program Protection
  - Difficult to distinguish “Critical Program Information (CPI)” from “Critical Components”
- Recommendations:
  1. Government and Industry need to develop training for acquisition and engineering communities.
     - Government to work with National Defense University, DAU, Universities and Industry Associations to make courses available
  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
     - Better define SSE skills sets which are required.
  3. Improve guidance to distinguish CPI from CC.

CSC

NORTH AMERICAN
PUBLIC SECTOR

Next Steps

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 • 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

For More Information . . .

Paul R. Croll
CSC
10721 Combs Drive
King George, VA 22485-5824

Phone: +1 540.644.6224

Fax: +1 540.663.0276

e-mail: pcroll@csc.com