DoD Software Assurance (SwA) Overview

Tom Hurt
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

NDIA Program Protection Summit / Workshop
McLean, VA | May 19, 2014

Outline

- Current Assurance Outlook
- DoD Trusted Defense Systems & Networks Strategy
- What is Software Assurance?
- SwA integrated into the DoD System Lifecycle
- SwA as a Systems Engineering Discipline
- SwA Analysis and Test Resources
- DoD SwA R&D Strategy
- Proposed DoD Enterprise Assurance Approach
- Challenge to Industry

Current Assurance Outlook

- ***Threat*: Nation-state, terrorist, criminal, or rogue developer who:**
  - Exploits vulnerabilities remotely
  - Gains control of systems through supply chain opportunities
- ***Vulnerabilities***
  - All systems, networks, and applications (Hardware & Software)
  - Intentionally implanted (i.e. malicious code insertion)
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile software)
- ***Traditional Consequences*: Loss of critical data and technology**
- ***Emerging Consequences*: Exploitation of manufacturing and supply chain, and of software vulnerabilities in sustainment**
  - Either can result in corruption; loss of confidence in critical warfighting capability

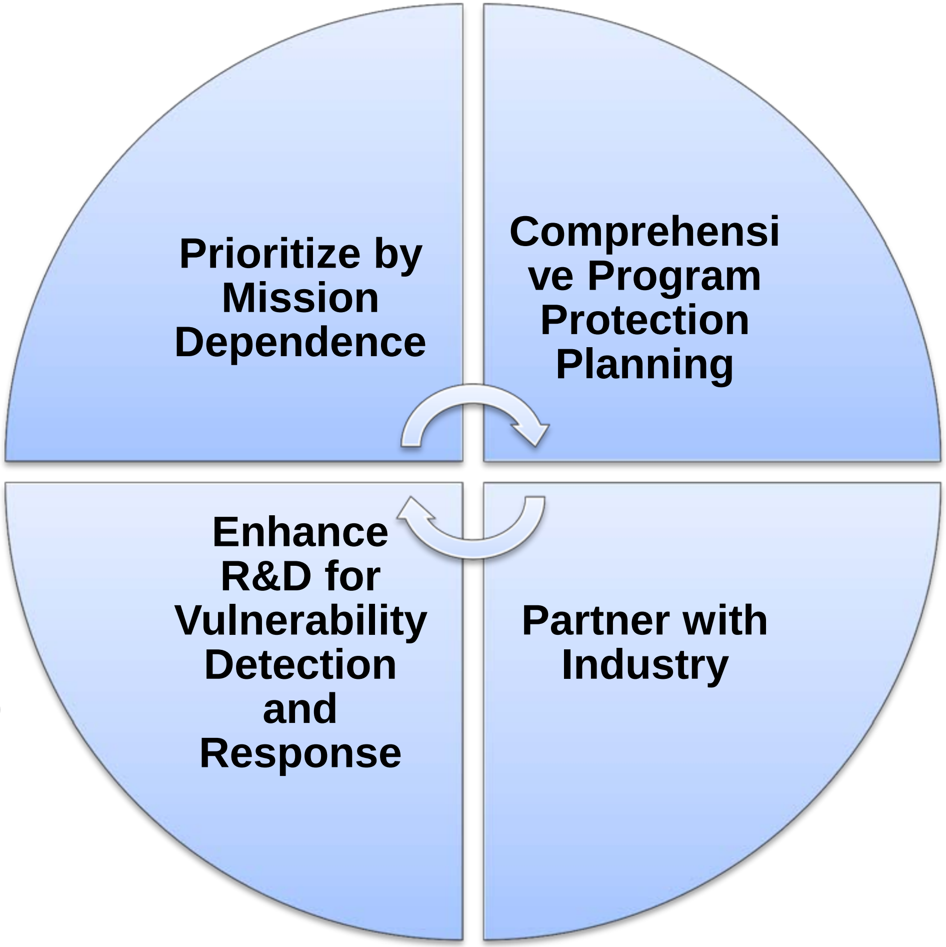
Today's acquisition environment drives the increased emphasis:

Then		Now
Stand-alone systems	>>>	Networked systems
Some software functions	>>>	Software-intensive and critical functions in Software
Known supply base	>>>	Prime Integrator, hundreds of suppliers
CPI (technologies)	>>>	CPI and critical components

Trusted Defense Systems and Networks Strategy

Drivers/Enablers

- National Cybersecurity Strategies
- Globalization Challenges
- Increasing System Complexity
- Pervasive Networks & SW-intensive Systems
- Intellectual Property Protection



Prioritize by Mission Dependence

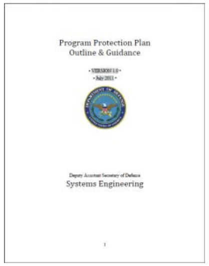
Comprehensive Program Protection Planning

Enhance R&D for Vulnerability Detection and Response

Partner with Industry

Delivering Trusted Systems

Program Protection Plan



Program Protection Plan
Outline & Guidance

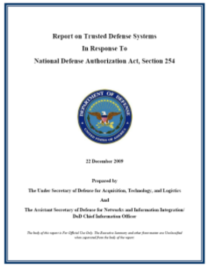
• VERSION 1.0 •
• July 2011 •

Deputy Assistant Secretary of Defense
Systems Engineering

1

USD(AT&L)
Download:
http://www.acq.osd.mil/se/pg/guidance.html

Report on Trusted Defense Systems



Report on Trusted Defense Systems
In Response To
National Defense Authorization Act, Section 254

22 December 2009

Prepared by
The Under Secretary of Defense for Acquisition, Technology, and Logistics
And
The Assistant Secretary of Defense for Networks and Information Integration/
DoD Chief Information Officer

The body of this report is For Official Use Only. The Executive Summary and other front matter are Unclassified when separated from the body of the report.

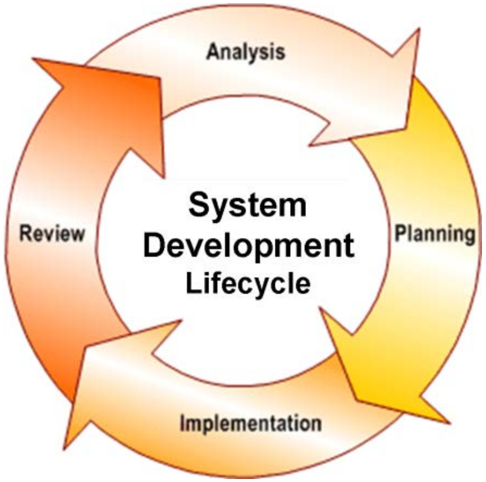
USD(AT&L)
ASD(NII)/DoD CIO
Executive Summary:
http://www.acq.osd.mil/se/pg/spec-studies.html

Distribution Statement A – Approved for public release by OSR on 5/15/14; SR Case# 14-S-1605 applies. Distribution is unlimited.

What is Software Assurance?

Software Assurance. The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle.

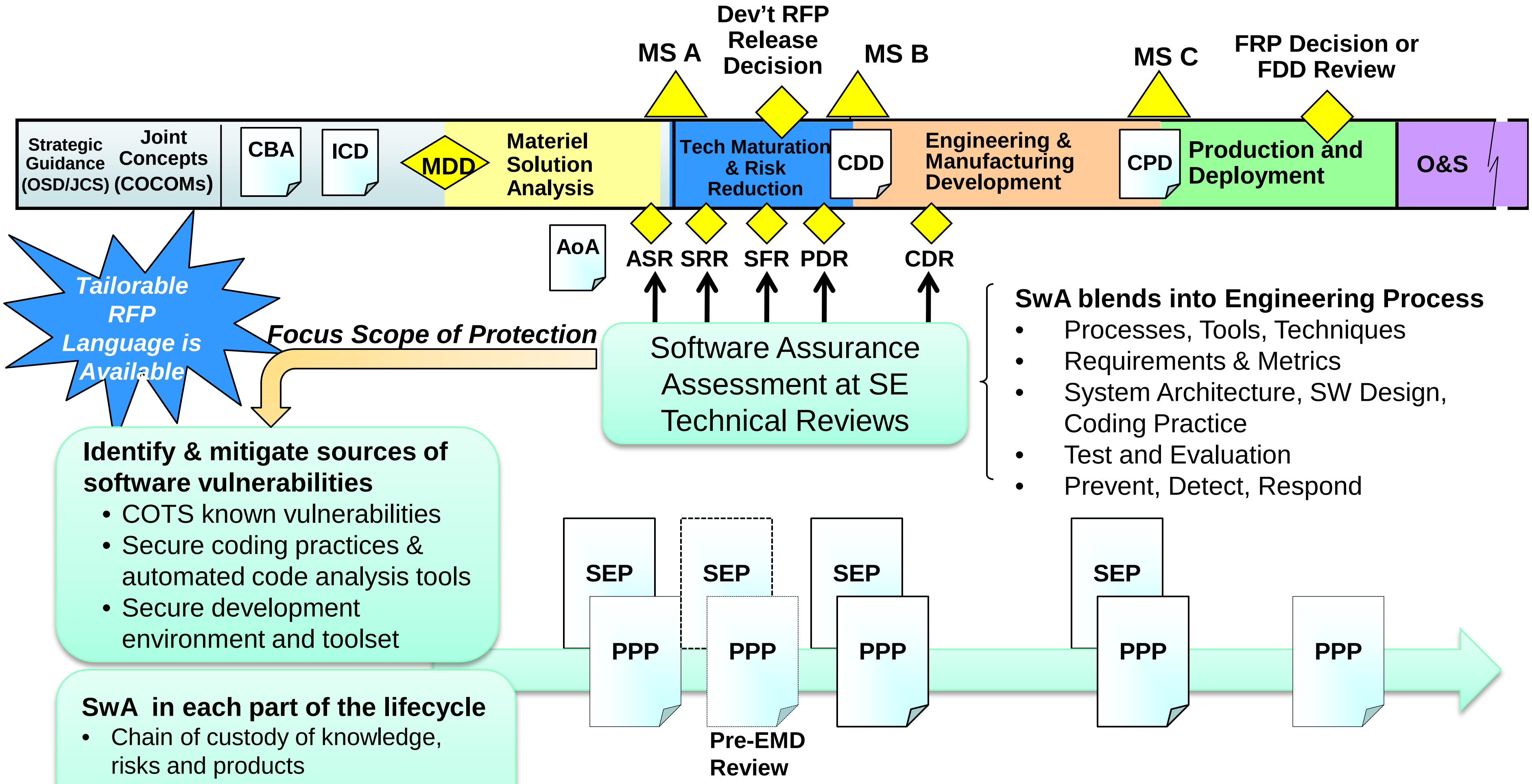
Reference: DoD Instruction 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)



Our objective is to establish software assurance as an accepted SE discipline within the Department.

Distribution Statement A – Approved for public release by OSR on 5/15/14; SR Case# 14-S-1605 applies. Distribution is unlimited.

Software Assurance Integrated into the DoD System Lifecycle


MS A
Dev't RFP Release Decision
MS B
MS C
FRP Decision or FDD Review
Strategic Guidance (OSD/JCS)
Joint Concepts (COCOMs)
CBA
ICD
MDD
Materiel Solution Analysis
Tech Maturation & Risk Reduction
CDD
Engineering & Manufacturing Development
CPD
Production and Deployment
O&S
AoA
ASR
SRR
SFR
PDR
CDR
Tailorable RFP Language is Available
Focus Scope of Protection
SEP
SEP
SEP
SEP
PPP
PPP
PPP
PPP
PPP
Pre-EMD Review

Software Assurance Assessment at SE Technical Reviews

SwA blends into Engineering Process
- Processes, Tools, Techniques
- Requirements & Metrics
- System Architecture, SW Design, Coding Practice
- Test and Evaluation
- Prevent, Detect, Respond

Identify & mitigate sources of software vulnerabilities
- COTS known vulnerabilities
- Secure coding practices & automated code analysis tools
- Secure development environment and toolset

SwA in each part of the lifecycle
- Chain of custody of knowledge, risks and products
- Engineering level traceability from MDD through disposal

Emphasizing Use of Affordable, Risk-based Countermeasures

Distribution Statement A – Approved for public release by OSR on 5/15/14; SR Case# 14-S-1605 applies. Distribution is unlimited.

Software Assurance as a Systems Engineering Discipline: Countermeasure Selection

Development Process

Apply assurance activities to the procedures and structure imposed on software development

Operational System

Incorporate countermeasures in the requirements, architecture, design, and acquisition of end-item software products and their interfaces

Development Environment

Apply assurance activities to the environment and tools for developing, testing, and integrating software code and interfaces

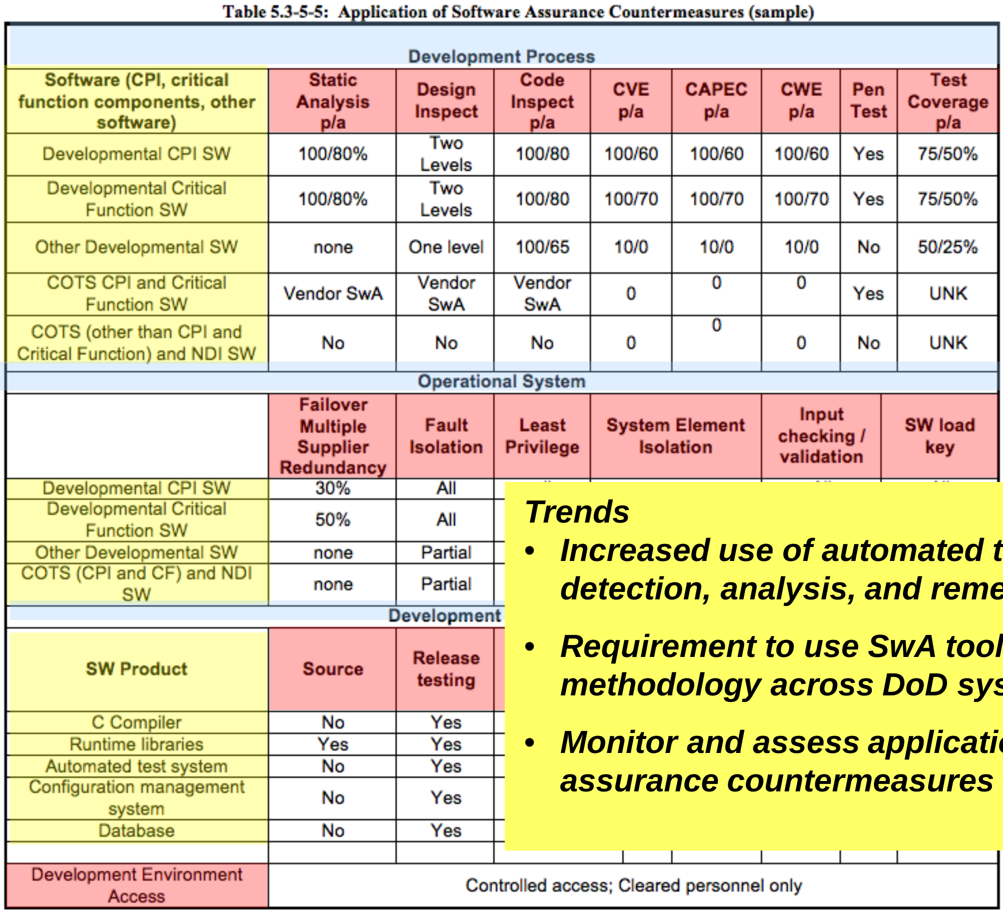


Table 5.3-5-5: Application of Software Assurance Countermeasures (sample)

Development Process								
Software (CPI, critical function components, other software)	Static Analysis p/a	Design Inspect	Code Inspect p/a	CVE p/a	CAPEC p/a	CWE p/a	Pen Test	Test Coverage p/a
Developmental CPI SW	100/80%	Two Levels	100/80	100/60	100/60	100/60	Yes	75/50%
Developmental Critical Function SW	100/80%	Two Levels	100/80	100/70	100/70	100/70	Yes	75/50%
Other Developmental SW	none	One level	100/65	10/0	10/0	10/0	No	50/25%
COTS CPI and Critical Function SW	Vendor SwA	Vendor SwA	Vendor SwA	0	0	0	Yes	UNK
COTS (other than CPI and Critical Function) and NDI SW	No	No	No	0	0	0	No	UNK

Operational System						
	Failover Multiple Supplier Redundancy	Fault Isolation	Least Privilege	System Element Isolation	Input checking / validation	SW load key
Developmental CPI SW	30%	All				
Developmental Critical Function SW	50%	All				
Other Developmental SW	none	Partial				
COTS (CPI and CF) and NDI SW	none	Partial				

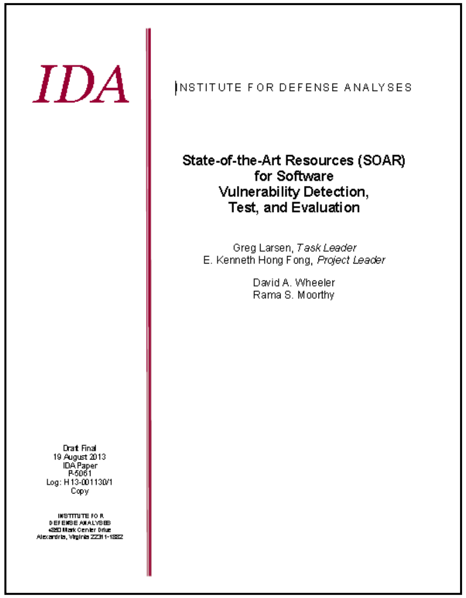
Development		
SW Product	Source	Release testing
C Compiler	No	Yes
Runtime libraries	Yes	Yes
Automated test system	No	Yes
Configuration management system	No	Yes
Database	No	Yes
Development Environment Access	Controlled access; Cleared personnel only	

Trends

- ***Increased use of automated tools for detection, analysis, and remediation***
- ***Requirement to use SwA tools and methodology across DoD system life cycle***
- ***Monitor and assess application of software assurance countermeasures***

Additional Guidance: http://www.acq.osd.mil/se/docs/SwA-CM-in-PPP.pdf

SwA Analysis and Test Resources



IDA

INSTITUTE FOR DEFENSE ANALYSES

State-of-the-Art Resources (SOAR)
for Software
Vulnerability Detection,
Test, and Evaluation

Greg Larsen, *Task Leader*
E. Kenneth Hong Fong, *Project Leader*

David A. Wheeler
Rama S. Moorthy

Draft Final
19 August 2013
IDA Paper
P-5061
Log: H 13-001130/1
Copy

INSTITUTE FOR
DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

State-of-the-Art Resources (SOAR) for Software Vulnerability Detection, Test, and Evaluation, August 2013

- Approach
  - SwA objectives (e.g., countering weaknesses) were organized and consolidated into categories that the DoD acquisition community can use
  - State-of-the-art of SW analysis and test tools and techniques were organized into families
  - SwA objectives were mapped to tools and techniques, providing a sound basis for a tool selection and use methodology by DoD programs
- Findings
  - There is utility in grouping SwA tools and techniques into families
  - Some tools are costly, and use of any tool or technique incurs program cost
  - Policy, guidance and resources must evolve at pace with constantly changing threats

No “silver bullet” tool or technique exists

DoD SwA R&D Strategy:
Focus Areas – Near and Long Term Goals

	Malicious Code Detection	Measures of Effectiveness	Designed-in Security
Near Term Technical Goals	*Existing and evolutionary:*	*Method and Baseline:*	*Advance security in design as early as possible:*
	Advanced passive monitoring	Effectiveness and cost	Reduction of costs and risk for development and sustainment
	Data collection across all system layers	Across the DoD lifecycle	Automated processes, data-intensive design and development
	Near real-time detection and isolation of “zero days”	Across Government agencies and industry	Assurance result composability
	Workforce education and training		
Long Term Technical Goals	*Revolutionary:*	*Automated MoE Assessment and Reporting System:*	*Co-develop System and Evidence for Assurance:*
	Automated enterprise-wide detection coordination and correlation	Automated trend analysis	Simultaneous development of systems and attestation evidence
	Threat vector prediction from behaviors, signatures and information external to code	Community acceptance and standards that drive contracts	Fully integrated supply chain considerations
			Verification and Assurance scalable across system size, complexity and criticality
			Feedback across entire lifecycle

Distribution Statement A – Approved for public release by OSR on 5/15/14; SR Case# 14-S-1605 applies. Distribution is unlimited.

Proposed DoD Enterprise Assurance Approach

- **Identify participating parties**
  - AT&L, CIO, Services, Agencies, …
- **Parties agree to:**
  - Establish a federation of SW and HW assurance capabilities to support DoD programs
  - Bring to bear SW and HW assurance expertise, and capabilities in support of DoD needs
  - Identify capability needs for SwA and HwA R&D program
  - Identify needed improvements in SW and HW assurance tools and methodoligies
  - Procure, manage, and distribute enterprise licenses for SW and HW assurance tools

Enhance DoD SW and HW Assurance Infrastructure

Distribution Statement A – Approved for public release by OSR on 5/15/14; SR Case# 14-S-1605 applies. Distribution is unlimited.

System Security Engineering (SSE); Software Assurance

- **Is a cross-cutting, multi-disciplinary area of interest**
- **Impacts not only security, but SW development, test, deployment, and operation techniques and practices**
- **Has tools and techniques that support cyber security, software design, software development techniques and practices, software test, and supply chain risk management**
- **Is a growing area of importance in industry**
- **Requires cooperative research, participation, innovation, and engagement**
- **Challenges are:**
  - Translating systems engineering requirements into SwA contract language
  - Identifying effective contract language and verifying results
  - Specifying metrics for security risks, vulnerability detection, and validated mitigation
  - Training and educating the workforce
  - Building efficacy/scalability of tools and techniques
  - Integrating SwA capability into engineering disciplines

Distribution Statement A – Approved for public release by OSR on 5/15/14; SR Case# 14-S-1605 applies. Distribution is unlimited.