DoD Software Assurance (SwA) Overview

Thomas Hurt

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

17th Annual NDIA Systems Engineering Conference
Springfield, VA | October 29, 2014

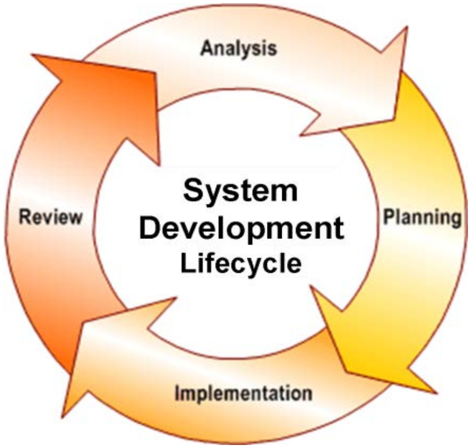
Distribution Statement A – Approved for public release by DOPSR on 10/20/14; SR Case# 15-S-0122 applies. Distribution is unlimited.

Overview

- Plan — Where are we going?
- Progress — Where are we now?
- Challenges — What do we need?
- Industry input — How can DoD and industry optimize the relationship?

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.

NDAA 2013 Section 933



Our objective is to establish software assurance as a mature SE discipline across DoD

Distribution Statement A – Approved for public release by DOPSR on 10/20/14; SR Case# 15-S-0122 applies. Distribution is unlimited.

Motivation: 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 (e.g., malicious code insertion)
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile software)
- ***Traditional Consequences***: **Loss of critical data and technology**
- ***Emerging Consequences***: **Software vulnerabilities that are targeted or surface in sustainment, and exploitation of development and manufacturing supply chain**
  - Either can damage National Security or critical warfighting capability

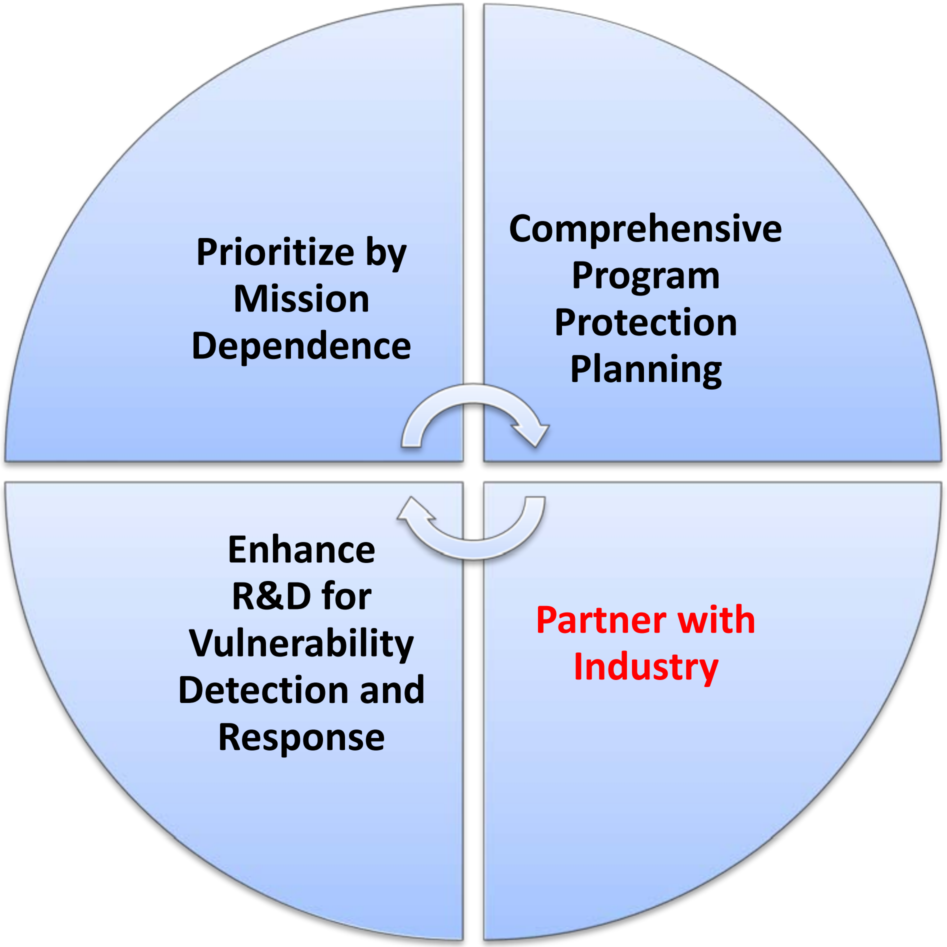
Today's acquisition environment drives the increased emphasis:

Then		Now
Stand-alone systems	>>>	Networked systems
Some software functions	>>>	Software-intensive and critical functions in software
Known supply base	>>>	Prime Integrator, multiple opaque tiers 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
- SW-based critical functions
- Intellectual Property Protection



Prioritize by Mission Dependence

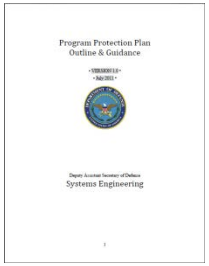
Comprehensive Program Protection Planning

Enhance R&D for Vulnerability Detection and Response

Partner with Industry

Delivering Trusted Systems

Program Protection Plan



Program Protection Plan
Outline & Guidance

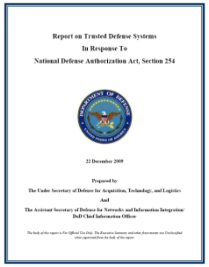
• VERSION 1.0 •
• July 2011 •

Deputy Assistant Secretary of Defense
Systems Engineering

1

USD(AT&L)
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 frontmatter 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 DOPSR on 10/20/14; SR Case# 15-S-0122 applies. Distribution is unlimited.

Public Law Driving SwA Evolution

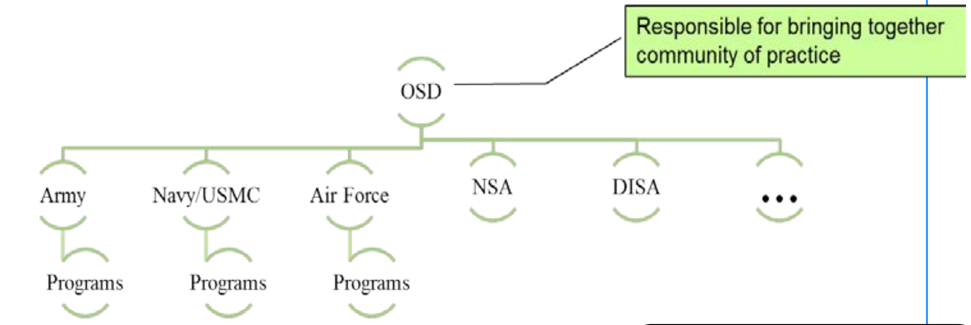
- **Public Law 111-383, Ike Skelton National Defense Authorization Act (NDAA) for Fiscal Year 2011, section 932, Strategy on Computer Software Assurance**
  – Required section 932 Report delivered to the Committees
- **Public Law 112-239-January 2, 2013, NDAA for Fiscal Year 2013, Section 933, Improvements in Assurance of Computer Software Procured by the Department of Defense:**
  – A research and development strategy to advance capabilities in software assurance and vulnerability detection
  – The state-of-the-art of software assurance analysis and test
  – How the Department might hold contractors liable for software defects or vulnerabilities
- **Public Law 113-66, NDAA for Fiscal Year 2014, Section 937, Joint Federated Centers for Trusted Defense Systems for the Department of Defense**
  – JFAC Charter in signature process with DEPSECDEF
  – Section 937 Report to the Committees due for final draft 15 Oct 2014
  – Activities to initiate JFAC operation in-process

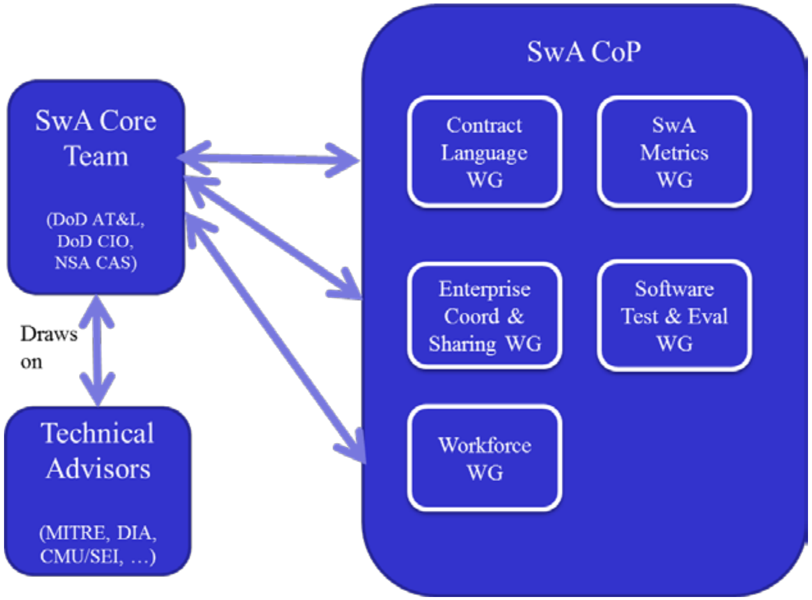
Distribution Statement A – Approved for public release by DOPSR on 10/20/14; SR Case# 15-S-0122 applies. Distribution is unlimited.

DoD SwA
Community of Practice (COP)

DoD SwA CoP Objectives

- Create a DoD community of Software Assurance practice
- Develop a system for recovering and spreading emerging best practices across the DoD
- Establish communication and coordination within DoD SwA community
- Mature software assurance practice within the PPP


Responsible for bringing together community of practice

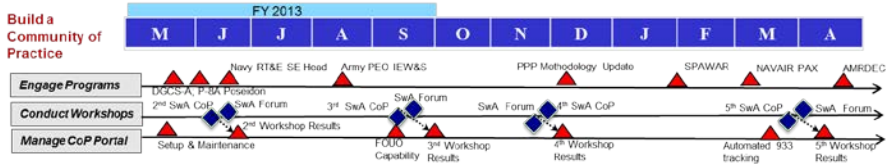


NDAA 2013 Section 933

- *SwA across life cycle*
- *Use automated tools*

informs

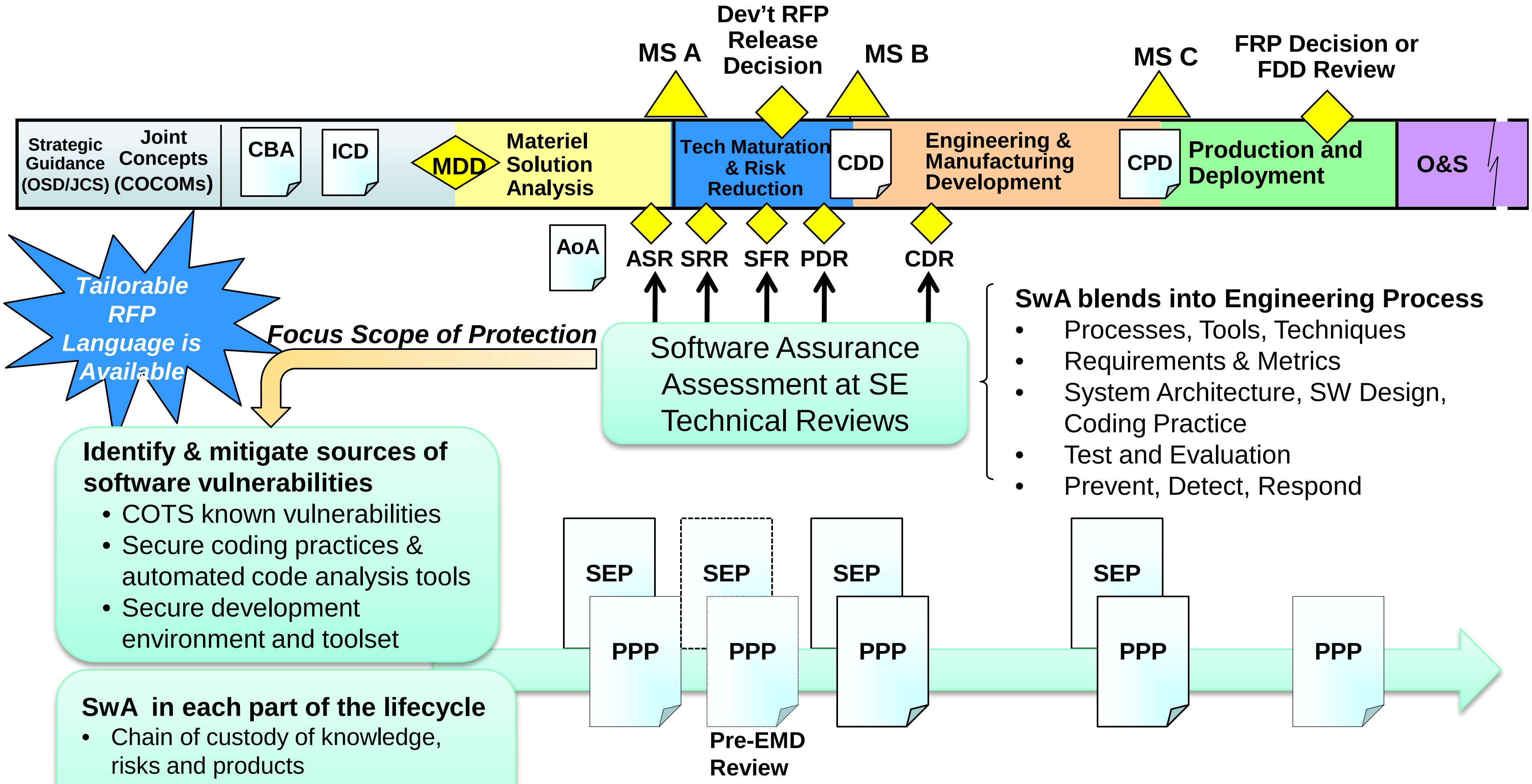
- Plan of Action & Milestones



Key Activities

- Engage Programs
- Conduct Workshops
- Provide tutorials
- Manage CoP Portal

Software Assurance: As 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

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

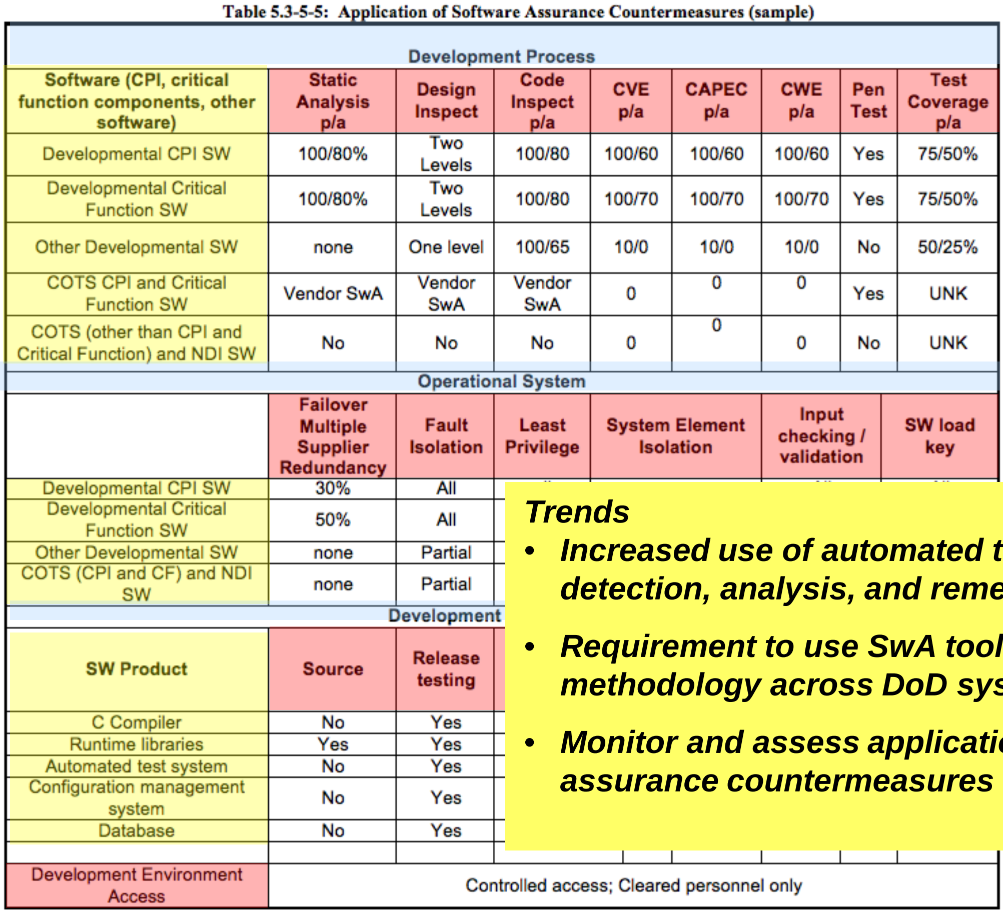


Table 5.3-5-5: Application of Software Assurance Countermeasures (sample)

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

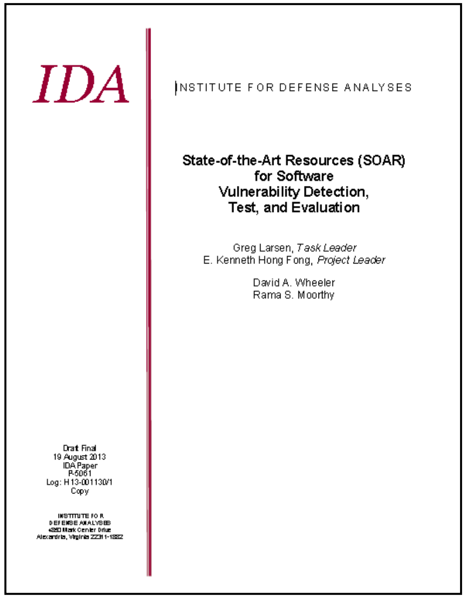
SW Product	Source	Release testing
C Compiler	No	Yes
Runtime libraries	Yes	Yes
Automated test system	No	Yes
Configuration management system	No	Yes
Database	No	Yes
Development Environment Access	Controlled access; Cleared personnel only	

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

State-of-the-Art Resources for SwA



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

- **Technical 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
- **Assessment Results**
  - 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

Available at http://www.acq.osd.mil/se/initiatives/init_pp-sse.html

Distribution Statement A – Approved for public release by DOPSR on 10/20/14; SR Case# 15-S-0122 applies. Distribution is unlimited.

SwA Analysis and Test SOAR: Key Findings

- **There is utility in grouping SwA tools and techniques into families**
  - Aids DoD SwA community in understanding available tools or techniques to use for each identified software weakness
  - Enables comparison of potential suppliers within a family
- **No “silver bullet” tool or technique exists**
  - No single tool meets all weaknesses; multiple tool or technique types must be combined
  - In most cases, a tool or technique does not completely address a weakness (doesn’t find all vulnerabilities associated with a SW weakness)
  - There are a few cases for which no tool was found effective
- **Some tools are costly, and use of any tool or technique incurs program cost**
  - Select tools in general use require significant expertise to use in SW defect and vulnerability remediation
  - Licensing and training are additional cost-drivers
- **Policy and guidance must evolve at pace with constantly changing threats**
  - SwA is best integrated in engineering and test activities across the system and product development lifecycle
  - While SwA-related policy needs to be broad, guidance and implementation for SwA tools and techniques must be agile

Distribution Statement A – Approved for public release by DOPSR on 10/20/14; SR Case# 15-S-0122 applies. Distribution is unlimited.

SwA Analysis and Test SOAR: Representative Tool Matrix

Tool and technique selection methodology:

1. Select technical objectives based on context (e.g., criticality).
2. Select tool/technique families to address those technical objectives.
3. Select tools/techniques within family based on effectiveness, cost, etc.
4. Summarize selection and rationale in SwA part of PPP
5. Apply, assess, report, remediate, iterate

For some given characteristics of SW:

Technical Objective	Tool/Technique Type								
	Static				Dynamic			Hybrid	
	1	2	3	…	21	22	…	31	…
…	—	✓	—	—	—	—	—	◗	—
Counter known vulnerabilities	✓	—	✓	—	✓	◗	—	—	—
Authentication & Access Control	—	—	✓	✓	—	✓	—	◗	◗
…	—	—	—	✅	—	—	◗	—	—

Legend

✅	Completely addresses this objective. This indicator is, unfortunately, rarely used
✓	Can be highly cost-effective measure to address this objective; investigate further
◗	Can be cost-effective for partial coverage of this objective
—	Not identified as being typically applied for this objective

Distribution Statement A – Approved for public release by DOPSR on 10/20/14; SR Case# 15-S-0122 applies. Distribution is unlimited.

Summary and Plans

- **Continue DoD SwA implementation actions**
  - Evolve policy and guidance; continue program engagement
  - Promulgate SwA Analysis and Test SOAR, update the framework over time
  - Continue coordination and development activities using the DoD SwA Community of Practice
  - Work toward implementation of federated SwA (and HwA) capability
- **Align Department software assurance activities as part of the Joint Federated Assurance Center (JFAC)**

Distribution Statement A – Approved for public release by DOPSR on 10/20/14; SR Case# 15-S-0122 applies. Distribution is unlimited.

For Additional Information

Thomas Hurt

Deputy Director, Software Assurance, DASD(SE)

571-372-6129 | thomas.d.hurt.civ@mail.mil

Distribution Statement A – Approved for public release by DOPSR on 10/20/14; SR Case# 15-S-0122 applies. Distribution is unlimited.

Systems Engineering: Critical to Defense Acquisition

Defense Innovation Marketplace

http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering

http://www.acq.osd.mil/se