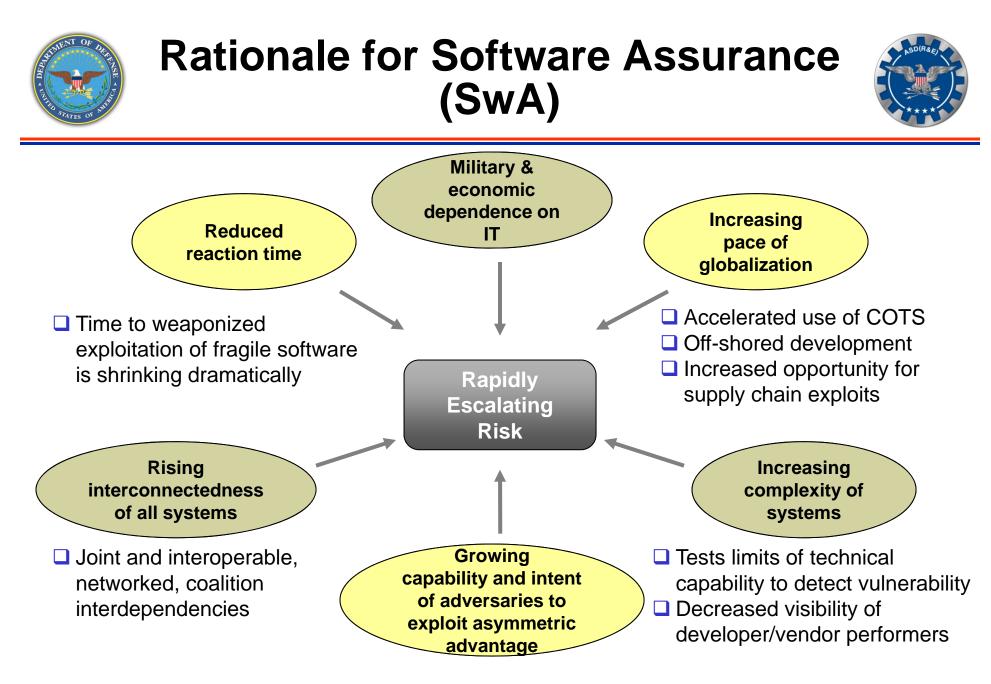


DoD Software Assurance

Kristen Baldwin Principal Deputy Office of the Deputy Assistant Secretary of Defense for Systems Engineering 16th Annual NDIA Systems Engineering Conference Arlington, VA | October 30, 2013

Distribution Statement A – Approved for public release by OSR on 10/28/2013, SR Case # 14-S-0165 applies. Distribution is unlimited.



DoD is dependent on the integrity of supply chain, software/hardware/IT

DoD Software Assurance 10/30/2013 | Page-2

Distribution Statement A – Approved for public release by OSR on 10/28/2013, SR Case # 14-S-0165 applies. Distribution is unlimited.





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

Source: DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), and 2013 NDAA S933



Nov 2012: DoDI 5200.44 Trusted Systems and Networks



Department of Defense INSTRUCTION							
DoD CIO/USD(AT&L)							
SUBJECT: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)							
References: See Enclosure 1							
 <u>PURPOSE</u>. This Instruction, in accordance with the authorities in DoD Directive (DoDD) 5134.01 (Reference (a)) and DoDD 5144.1 (Reference (b)): a. Establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, as defined in this Instruction, by foreign intelligence, terrorists, or other hostile elements. 							
b. Implements the DoD's TSN strategy, described in the Report on Trusted Defense Systems (Reference (c)) as the Strategy for Systems Assurance and Trustworthiness, through Program Protection and information assurance (IA) implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, information assurance, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust.							
c. Incorporates and cancels Directive-Type Memorandum 09-016 (Reference (d)).							
d Directs actions in accordance with the SCRM implementation strategy of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (e)), section 806 of Public Law 111-383 (Reference (f)), DoD Instruction (DoDI) 5200.39 (Reference (g)), DoDD 5000.01 (Reference (h)), DoDI 5000.02 (Reference (i)), DoDD 8500.01E (Reference (j)), and Committee on National Security Systems Directive No. 505 (Reference (k)).							
2. <u>APPLICABILITY</u> . This Instruction applies to:							
a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").							

- Implements the DoD's Trusted Systems and Networks (TSN) strategy
- Manage risk of mission-critical function and component compromise throughout lifecycle of key systems by utilizing
 - Criticality Analysis as the systems engineering process for risk identification
 - Countermeasures: Supply chain risk management, software assurance, secure design patterns
 - Intelligence analysis to inform program management
- Codify trusted supplier requirement for DoD-unique application-specific integrated circuits (ASICs)



FY13 NDAA Section 933



14	SEC. 933. IMPROVEMENTS IN ASSURANCE OF COMPUTER
15	SOFTWARE PROCURED BY THE DEPARTMENT
16	OF DEFENSE.
17	(a) BASELINE SOFTWARE ASSURANCE POLICY.—The
18	Under Secretary of Defense for Acquisition, Technology,
19	and Logistics, in coordination with the Chief Information
20	Officer of the Department of Defense, shall develop and
21	implement a baseline software assurance policy for the en-
22	tire lifecycle of covered systems. Such policy shall be in-
23	cluded as part of the strategy for trusted defense systems
24	of the Department of Defense.
	631
1	(b) POLICY ELEMENTS.—The baseline software as-
2	surance policy under subsection (a) shall
3	(1) require use of appropriate automated vul-
4	nerability analysis tools in computer software code
5	during the entire lifecycle of a covered system, in-
6	eluding during development, operational testing, op-
7	erations and sustainment phases, and retirement;
8	(2) require covered systems to identify and
9	prioritize security vulnerabilities and, based on risk,
10	determine appropriate remediation strategies for
11	such security vulnerabilities;
12	(3) ensure such remediation strategies are
13	translated into contract requirements and evaluated
14	during source selection;
15	(4) promote best practices and standards to
16	achieve software security, assurance, and quality;
17	and

FY13 NDAA SEC. 933: IMPROVEMENTS IN ASSURANCE OF COMPUTER SOFTWARE PROCURED BY THE DEPARTMENT OF DEFENSE

- USD(AT&L), in coordination with the DoD CIO... "shall develop and implement a baseline software assurance policy for the entire lifecycle of covered systems. Such policy shall be included as part of the strategy for trusted defense systems of the Department of Defense."
- "(1) require use of automated vulnerability analysis tools during the entire life cycle of a covered system..."
- …"(2) require covered systems to identify and prioritize security vulnerabilities and, based on risk, determine appropriate remediation strategies for such security vulnerabilities;"

NDAA: National Defense Authorization Act http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310enr/pdf/BILLS-112hr4310enr.pdf



DoD SwA Actions



Compliance

- NDAA Compliance (2011: S932, 2013: S933)

Policy and guidance

- Implemented DoDI 5200.44 SwA language
- Updating DAG Ch. 13 Program Protection Planning Guide
- Crafting DoDI 5000.02 updates for SwA

Implementation

- Engaging Programs of Record through Program Protection Planning
- Tutorials for programs, engineering centers, industry

• DoD SwA Community of Practice (CoP)

- Government SwA Core Group (AT&L, CIO, NSA, Services, Agencies) provides operational direction
- SwA CoP established. Quarterly meetings and ongoing working groups.





Implementation Mechanisms

- Support to programs
 - Provide SwA tutorials to the community
 - Program mentoring for SwA as part of Program Protection Plan (PPP) reviews

• PPP review and approval

- All PPPs reviewed in accordance with PPP Outline & Guidance (est. July 2011)
- 22 PPPs approved FY12 and FY13
- Upward trend in SwA content

PPP					Total
Reviews	MS A	MS B	MS C	FRP	Approved
FY12	0	2	0	3	5
FY13	1	4	4	8	17
Totals	1	6	4	11	22



DoD Software Assurance Community of Practice (CoP)



- Membership
 - OSD, NSA, Services, Agencies, COCOMs
- 3 Ongoing Workgroups
 - Contract Language, including contractor liability for SW defects and vulnerabilities
 - Enterprise Coordination and Collaboration (SwA Security Classification Guide, Intelink portal)
 - Workforce Education & Training; ongoing survey and availability of needed and emerging SwA-related skills

• Workgroups being organized

- SwA Metrics
 - $\circ~$ How to assess implementation of DoD SwA policy
 - How to assess program implementation of DoD SwA policy over life cycle
- SwA in Testing
 - o DT&E, OT&E
 - o Facilities, tools, methodologies





Operationalize SwA-related policy

- Engage programs, software centers
- Measure progress and effectiveness define metrics
- Adaptive to threats, attack patterns

• Promulgate tools, practices

- Promote best practice, tools, standards
- Establish software assurance analysis support capability

• Workforce, training and education

- SwA course content updates, new SwA courses
- SwA competencies
- Explore business model to capitalize on commercial interests, capabilities