SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Inserting SwA Practices into Organizational Policies and Processes

Winter 2011 SwA WG Sessions

Background

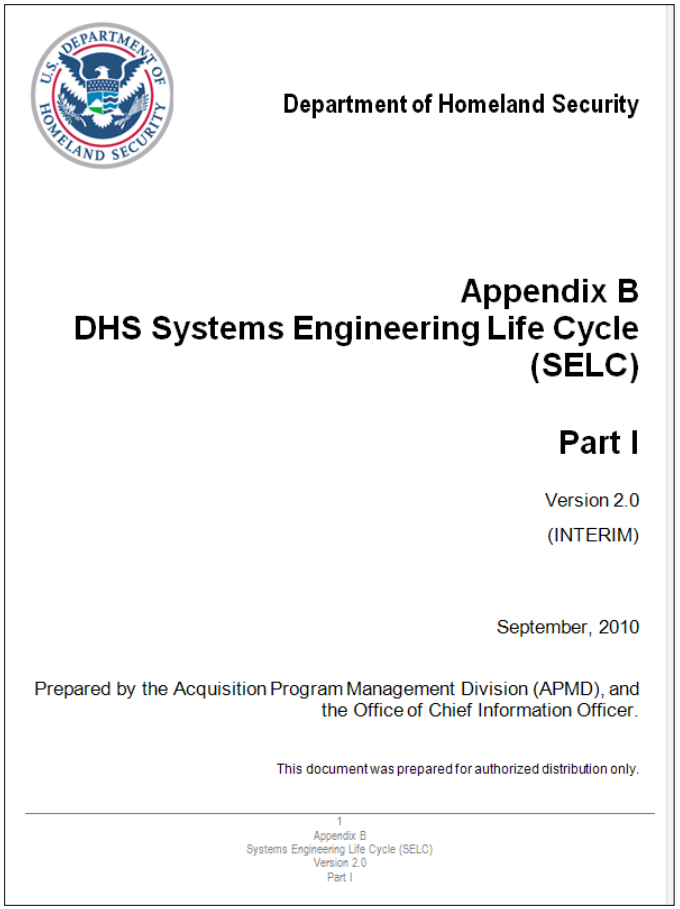
"Who's making me do this?

Where is it stated that this is a requirement?"

"We can help you with that!"

DHS Management Directive / SELC

- Analyzed the DHS Management Directive 102
- Appendix B is the DHS Software Engineering Life Cycle
- All new systems developed throughout the Department must follow the DHS SELC requirements



Department of Homeland Security

Appendix B
DHS Systems Engineering Life Cycle (SELC)

Part I

Version 2.0
(INTERIM)

September, 2010

Prepared by the Acquisition Program Management Division (APMD), and the Office of Chief Information Officer.

This document was prepared for authorized distribution only.

Adding SwA Content

Appendix B

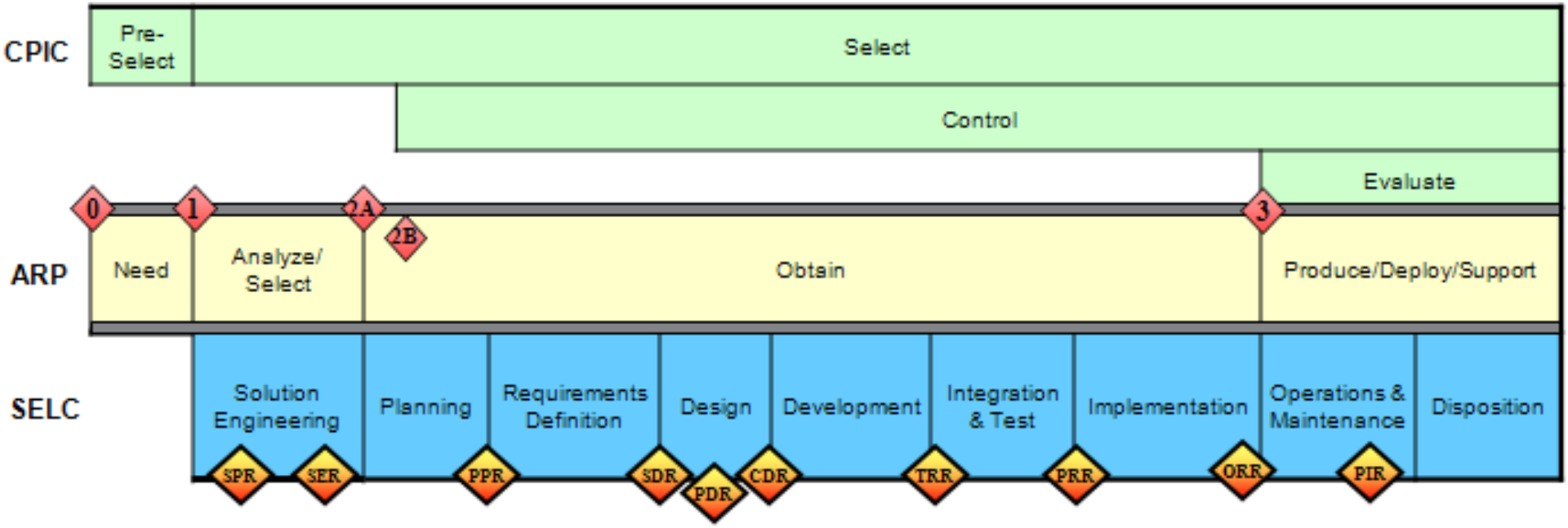
Systems Engineering Life Cycle

Part I

SELC Overview & Framework

Capital Planning and Investment Control (CPIC) and the Acquisition Review Process (ARP)

including Systems Engineering Life Cycle (SELC)



*NOTE: The waterfall model is depicted for illustrative purposes only; some development models have iterative phases

ARP Acquisition Decision Events

- 0: Collect Needs
- 1: Validate Needs
- 2A: Approve Acquisition
- 2B: Approve Acquisition Types
- 3: Approve Produce/Deploy/Support

SELC Stage Reviews

- SPR: Study Plan Review
- SER: Solution Engineering Review
- PPR: Project Planning Review
- SDR: System Definition Review
- PDR: Preliminary Design Review
- CDR: Critical Design Review
- TRR: Test Readiness Review
- PRR: Production Readiness Review
- ORR: Operational Readiness Review
- PIR: Post Implementation Review

Existing Available SwA Resources

- Leverage the SwA Pocket Guides
  - Software Supply Chain Risk Management Due-Diligence
  - Software Assurance in Acquisition and Contract Language
- Due-Diligence Questionnaires provide a host of checks for SwA best practices to ask of suppliers and in-house developers throughout the SDLC.

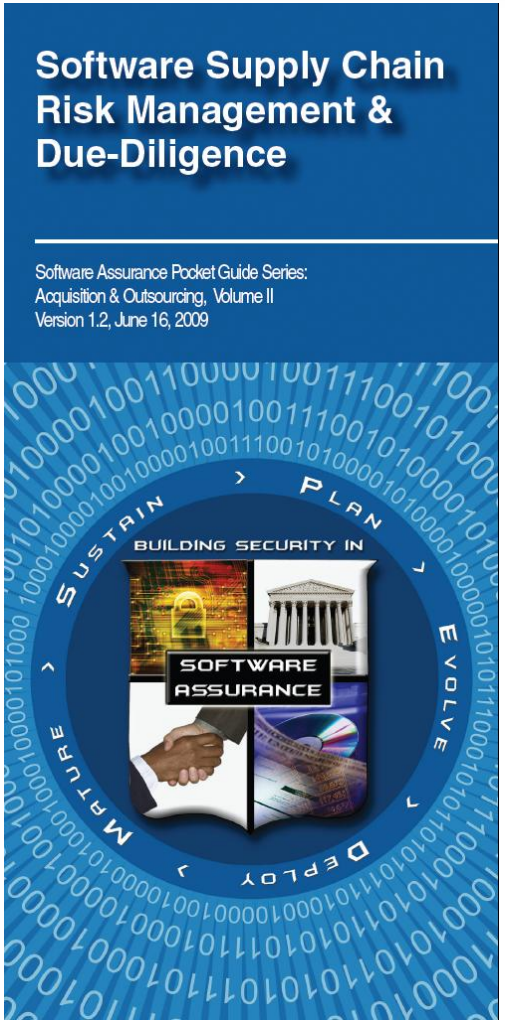


Table 1 – SwA Concern Categories

SwA Concern Categories	Risks	Purpose for Questions
Software History and Licensing	The software supplier's development practice in using code of unknown origin may be unable to produce trustworthy software.	To address supply chain concerns and identify specific risks pertaining to the history/pedigree of the software during any and all phases of its life cycle that should have been considered by the supplier. This point addresses supply chain concerns.
Development Process Management	If supplier project management does not perceive the value of SwA and enforce best practices, they will not be consistently implemented.	To determine whether project management enforces software assurance–related best practices.
Software Security Training and Awareness	Developers unaware of software assurance best practices are likely to implement software with security flaws (making it more susceptible to attack).	To determine whether training of developers in SwA best practices is a supplier policy and practice.
Planning and Requirements	If nonfunctional requirements (security, quality, safety) are not specified, developers will not implement them.	To determine whether the supplier's requirements analysis process explicitly addresses SwA requirements.
Architecture and Design	The software may be designed without considering security or minimization of exploitable defects.	To determine how security is considered during the design phase.
Software Development	If developers lack qualified tools or if personnel are allowed to inappropriately access or change configuration items in the development environment, then delivered software might have unspecified features. The supplier might lack sufficient process capability to deliver secure products, systems or services.	To ascertain that the supplier has and enforces policies and SwA practices in the development of software that use secure software development environments to minimize risk exposures.
Built-in Software Defenses	The software may lack preventive measures to help it resist attack effectively and proactively.	To ensure that capabilities are designed to minimize the exposure of the software's vulnerabilities to external threats and to keep the software in a secure state regardless of the input and parameters it receives from its users or environment.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

						A - Solution Engineering		1 - Planning	2 - Requirements Definition	3 - Design		4 - Development	5 - Integration and Test	6 - Implementation		7 - Operations & Maintenance
No.	Question	COTS Proprietary	COTS Open-Source	GOTS	Custom	SPR	SER	PPR	SDR	PDR	CDR	IRR	PRR	OTRR	ORR	PIR
1	Can the pedigree of the software be established? Briefly explain what is known of the people and processes that created the software.	✓	✓	✓	✓		X					X				
2	Explain the change management procedure that identifies the type and extent of changes conducted on the software throughout its life cycle.	✓		✓	✓		X					X				
3	What type of license(s) are available for the open source software? Is it compatible with other software components in use? Is indemnification provided, and will the supplier indemnify the purchasing organization from any issues in the license agreement? Explain.	✓	✓		✓		X									
4	Is there a clear chain of licensing from original author to latest modifier? Describe the chain of licensing.	✓					X									
5	What assurances are provided that the licensed software does not infringe upon any copyright or patent? Explain.	✓		✓	✓		X									
6	Does the company have corporate policies and management controls in place to ensure that only corporate-approved (licensed and vetted) software components are used during the development process? Explain.	✓			✓		X									
7	Are licensed software components still valid for the intended use?	✓		✓			X					X				
8	Is the software in question original source or a modified version?		✓				X					X				
9	Has the software been reviewed to confirm that it does not infringe upon any copyright or patent?	✓	✓		✓		X					X				
10	How long has the software source been available? Is there an active user community providing peer review and actively evolving the software?	✓	✓				X			X						
11	Does the license/contract restrict the licensee from discovering flaws or disclosing details about software defects or weaknesses with others (e.g., is there a "gag rule" or limits on sharing information about discovered flaws)?	✓			✓	X	X									
12	Does the license/contract restrict communications or limit the licensee in any potential communication with third-party advisors about provisions for support (e.g., is there a "gag rule" or limits placed on the licensee that affect ability to discuss contractual terms or breaches) regarding the licensed or contracted product or service?	✓			✓	X	X									
13	Does software have a positive reputation? Does software have a positive reputation relative to security? Are there reviews that recommend it?	✓	✓				X									
14	Is the level of security where the software was developed the same as where the software will operate?			✓	✓		X					X	X			
	Development Process Management															
15	What are the processes (e.g., ISO 9000, CMMI, etc.), methods, tools (e.g., IDEs, compilers), techniques, etc. used to produce and transform the software (brief summary response)?	✓		✓	✓		X									
16	What security measurement practices and data does the company use to assist product planning?	✓			✓		X									
17	Is software assurance considered in all phases of development? Explain.	✓		✓	✓		X									
18	How is software risk managed? Are anticipated threats identified, assessed, and prioritized?	✓		✓	✓		X									
	Software Security Training and Awareness															
19	Describe the training the company offers related to defining security requirements, secure architecture and design, secure coding practices, and security testing.	✓			✓		X									
20	Does the company have developers that possess software security related certifications (e.g., the ISC2 CSSLP, SANS SSI secure coding certifications, etc.)?	✓			✓		X									
21	Describe the company's policy and process for professional certifications and ensuring certifications are valid and up-to-date.	✓			✓		X									
	Planning and Requirements															
22	Are there some requirements for security that are "structured" as part of general releasability of a product and others that are "as needed" or "custom" for a particular release?	✓			✓		X									

Table 3- 2 Study Plan Review Exit Criteria

Study Plan Review Exit Criteria
• Does the study plan address the needs in the approved Mission Need? • Is the basis and justification for an AoA or AA adequate? (and linked to CDP?) • Is the scope of AoA or AA clearly defined? (what is included and what is not) • Is the study team director and co-chairs identified? • Do the participating organizations have documented roles and responsibilities? • Are the assumptions and constraints reasonable and adequate? • Is the schedule realistic given the required resources, including SMEs? • Are the deliverables identified? • What level of engagement of users/operators is planned? • Describe how the AoA/AA team will interface with the CONOPS team and the ORD effort? • What are the criteria for the selection of alternatives? • How many alternatives will be examined? (minimum of three) • What are the analysis methodology (ies) including Modeling and Simulation and Technology Demonstrators? • Is the review and approval process identified for the AoA/AA, including an AoA/AA report and brief to seniors?

Table 3- 3 Software Assurance Due Diligence Questions:

Question	COTS Propri-etary	COTS Open-Source	GOTS	Custo m
Does the license/contract restrict the licensee from discovering flaws or disclosing details about software defects or weaknesses with others (e.g., is there a "gag rule" or limits on sharing information about discovered flaws)?	✓			✓
Does the license/contract restrict communications or limit the licensee in any potential communication with third-party advisors about provisions for support (e.g., is there a "gag rule" or limits placed on the licensee that affect ability to discuss contractual terms or breaches) regarding the licensed or contracted product or service?	✓			✓
Is delivery of demonstrably secure software a contractual requirement for third-party developed software? If yes, what criteria are used to operationally define "secure software"?				✓
Are the version control and configuration management policies and procedures the same throughout the entire organization and for all products? How are they enforced? Are	✓			✓

Inserting SwA Requirements

- Weave SwA requirements into the exit criteria for each SDLC stage review.
- It is easier to insert extra requirements into the existing processes and reviews than to change the process.
- Require a review by a SwA SME during each phase of the SDLC.

Software Weaknesses

- Require use of SwA automation for remediation of software weaknesses throughout phases:
  - Require use of CWE compatible tools
  - Require analysis of tools that have coverage for CWE Top-N list (i.e., CWRAF, CWSS)

Code Analysis

- Require use of manual code reviews, and static and dynamic analysis tools throughout development.
- Require legacy code to be analyzed using static analysis tools.
- Evaluate whether any reused code is **fit for use** in the new environment.

Lifecycle Cost Estimation

- SDLC policy typically requires lifecycle cost estimations.
- This is your opportunity to make the business case for building security into the software.
- Show lifecycle cost analyses of resilient software versus insecure software (Rugged software versus playing Patching Whack-A-Mole)

Supplier Management

- Leverage the questionnaires and contract language in the pocket guides.
- For non-COTS development, establish supplier agreements per assurance requirements.
- Evaluate solicitation responses per SwA requirements.
- Monitor and correct supplier processes and performance per assurance requirements.
- Evaluate and accept supplier work products per assurance requirements.

Follow Up Work

- Completed work:
  - Met with the office of the DHS CIO
  - Submitted our input for DHS MD 102/SELC
- Future work:
  - Plan to tackle other acquisition guidance
  - Identify other policy and guidance in which to insert SwA best practices including DHS Security Handbook

Feedback & Questions

- Feedback / questions / suggestions?
- What worked at your organization?