DHS-DoD Software Assurance Forum Acquisition Status Briefing

Mary L. Polydys
National Defense University
Information Resources Management College

Stan Wisseman

Booz Allen Hamilton

October 3, 2007

Homeland Security

Two years in the making

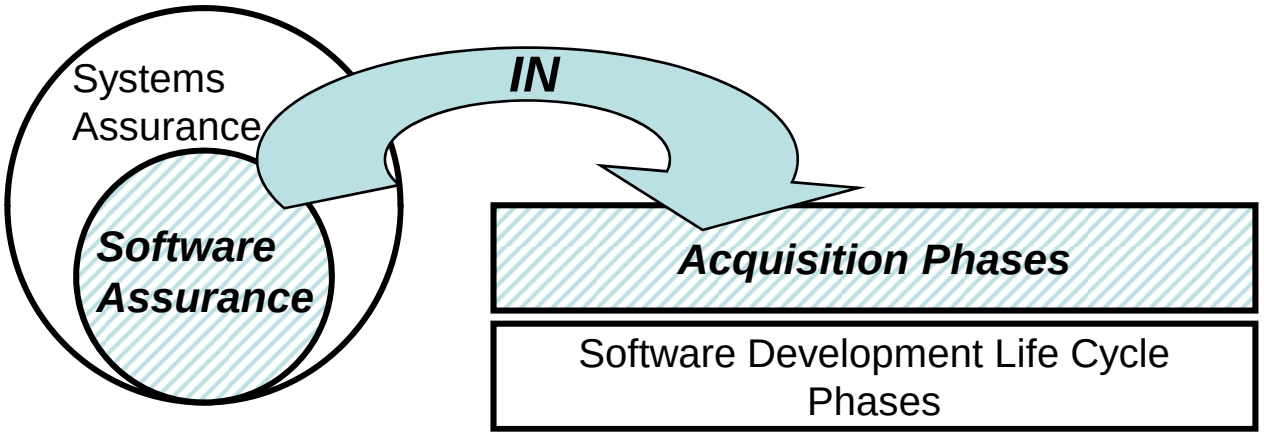
Elephants are inside their mother's womb for 22 months

The same amount of time we've been working on this Guide!

Homeland Security

Acquisition Working Group Goals

- To provide guidance on how to incorporate SwA considerations in key decisions of the acquisition process.



Homeland Security

Acquisition
Working Group Action Items

- Address comments on draft guide received from NIST and industry
- Put revised draft through NCSD review cycle in preparation for a broader public comment period

Homeland Security

Acquisition Guide Revisions

- Diagram to clarify the scope of the document
- Notional comparison of acquisition processes (IEEE 1062; NIST SP 88-84; DoDI 8000.2; ISO 12207)

IEEE 1062	Planning		Contracting		Implementation & Acceptance		Follow-on
NIST SP 800-64	Mission & Business Planning	Acquisition Planning	Acquisition		Contract Performance		Disposal & Contract Closeout
DoDI 8000.2	Pre-Systems Acquisition (Acquisition Strategy, e.g., concept & technology development; contracting, and other strategies)		Systems Acquisition (Contracting for system development & production/deployment)				Sustainment (Operations & Support)
ISO 12207 "Customer"	Initiation		Request for Proposal	Contract Preparation & Update	Supplier Monitoring	Acceptance & Completion	

Homeland Security

Acquisition Guide Revisions (con't)

- Clarification of the risk discussion in the planning phase
- Clarification of alternative software approaches
- Clarification of the discussion of SwA requirements in part 2
- Clarification of several parts of the "SwA Concern Categories"
- Major enhancement of the definitions section
- Includes the new policy on securely configuring commercial software
- References the new state of the art report on software security assurance
- Revision of questions in Appendix D

Homeland Security

Acquisition Working Group Plans

- Guide is available on the BSI site
- Guide should be release for public review in Federal Register following Forum – will collect comments for WG review in December
- Development of outreach package to enable WG members to communicate Guide's purpose and methods of use
- Identification of organizations to pilot use of Guide
- Content for acquisition WG portion of Web site needs to be developed

Homeland Security

We want to thank all that participated

- Authors:
  - Mary Linda Polydys, NDU IRMC
  - Stan Wisseman, Booz Allen Hamilton (contract with DHS National Cyber Security Division)
- Additional contributors included:
  - Nadya Bartol, Booz Allen Hamilton
  - Brad Doohan, Australian Defence Materiel Organisation (working with SEI and DCMA)
  - Greg Gogates, Fasor (in support of FDA)
  - Karen Goertzel, Booz Allen Hamilton
  - Joe Jarzombek, DHS NCSD
  - Steven Lavenhar, Booz Allen Hamilton
  - Michael Leichtman, Booz Allen Hamilton
  - Tom O'Flaherty, INPUT
  - Jeff Williams, Aspect Security

Homeland Security

Thanks (con't)

- Detailed reviews of the guide were provided by:
  - Mary Ann Davidson, Oracle
  - Lauren Eisenberg Davis, Johns Hopkins University Applied Physics Laboratory
  - Annabelle Lee, NIST
  - Sandra Ludwig, Booz Allen Hamilton
  - Paul Nicholas, Microsoft
- During most working group meetings, participants provided feedback on draft materials for the guide. Working Group participants are too numerous to list here but are listed in the guide

Homeland Security