Update to NII/CIO Leadership

SwA Forum

2-6 Nov 2009

As of 22 Oct 2009

Don Davidson
GTF / ODASD-CI&IA

Unclassified

Agenda

- Who- Govt – Industry – Academia - International
  - » Govt stakeholders = DHS, DoD, NSA, DoC (NIST)
- What- Software Assurance (SwA) Forum
- When- 2-6 Nov 2009
- Where- Crystal Gateway Marriott
- Why- DHS asked; DoD turn?; SwA is critical to us
- How- Existing GTF contracts & funding

- Background-
- Forum Focus-
- Agenda-

Background

- **Software Assurance (SwA)** is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner (from CNSS 4009 IA Glossary - see Wikipedia for more definitions and descriptions).

- As part of DHS risk mitigation efforts to enable greater resilience of cyber assets, the **Software Assurance Program** seeks to reduce software vulnerabilities, minimize exploitation, and address ways to routinely acquire, develop and deploy reliable and trustworthy software products with predictable execution, and to improve diagnostic capabilities to analyze systems for exploitable weaknesses.

- The Software Assurance Program of the Department of Homeland Security's National Cyber Security Division co-sponsors **SwA Forums** semi-annually with organizations in the Department of Defense and the National Institute for Standards and Technology. The purpose of the forums is to bring together members of government, industry, and academia with vested interests in software assurance to discuss and promote integrity, security, and reliability in software.

Forum Focus

"Achieving Software Assurance (SwA) in a Global Marketplace"

As Is

To Be ?

"Roadmapping" (POAM)

Stakeholders

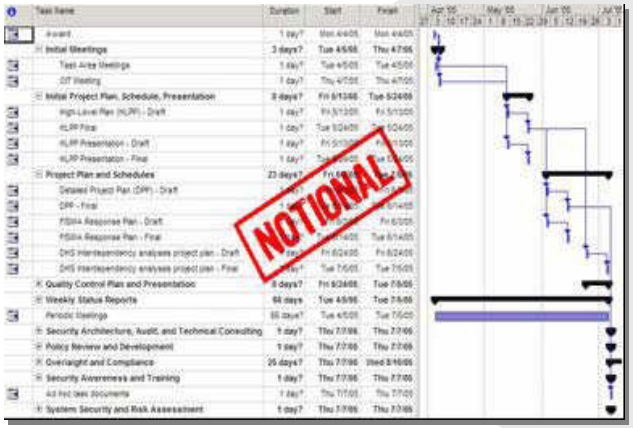
- Government
- Industry
- Academia
- (International)

Working Groups

Measures

- People
- Process
- Technology
- Acquisition

What is your Organization's view of the future?
How can SwA Forum help you get there?



What does your WG's "pathway" look like?
Who participates to develop what?

- Trustworthy systems
- w/ Managed Risk from SW we develop, acquire, use / "rely on"…
- Enabled by
  - "Built in Security"
  - Informed acquisition
  - Transparent supply chains
  - Real Life Cycle Mgt

Our goal is to develop a high level <u>Implementation Road Map</u> for use of our WGs during their Dec'09 Work Sessions.

Agenda

Where have we been?... Where are we going?

Mon	Tue	Wed	Thu	Fri
DoD / DHS Led **Cyber / SwA Education**	***Stakeholders*** *KeyNote* *Govt* *Industry* *Academia* *(international)* ***(Ends)***	***WGs*** *Processes* *Technology* *People* *Measures* *Acquistion* ***(ways/means)***	***Discussion*** *Govt* *Industry* *Academia* *(international)* *& WGs* ***(Planning)***	**NIST-led** **SwA Tools** **(SATE= Static Analysis & Tools Exposition)**

Strategic Planning
SwA Forum- Gap Analysis

Software Security Pavillion

See Detailed Handout

Unclassified

Discussion

- **DHS web-link on SwA Program**

  https://buildsecurityin.us-cert.gov/swa/

- **SwA Forum information & registration**

  (Use conference code SOF96945)

  https://www.enstg.com/Invitation/default.cfm?ems31e=0.663183387027

- **Software Security Pavilion**

  https://www.enstg.com/Invitation/Index.cfm?CFID=131047&CFTOKEN=93711092