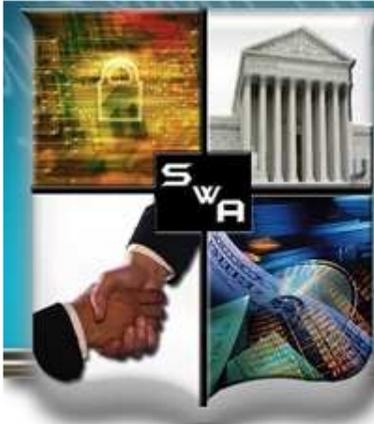




DoD-DHS-NIST  
Software Assurance Forum  
***SwA Community Collaboration  
Strategy: Forward to June SwA WGs***



Homeland  
Security

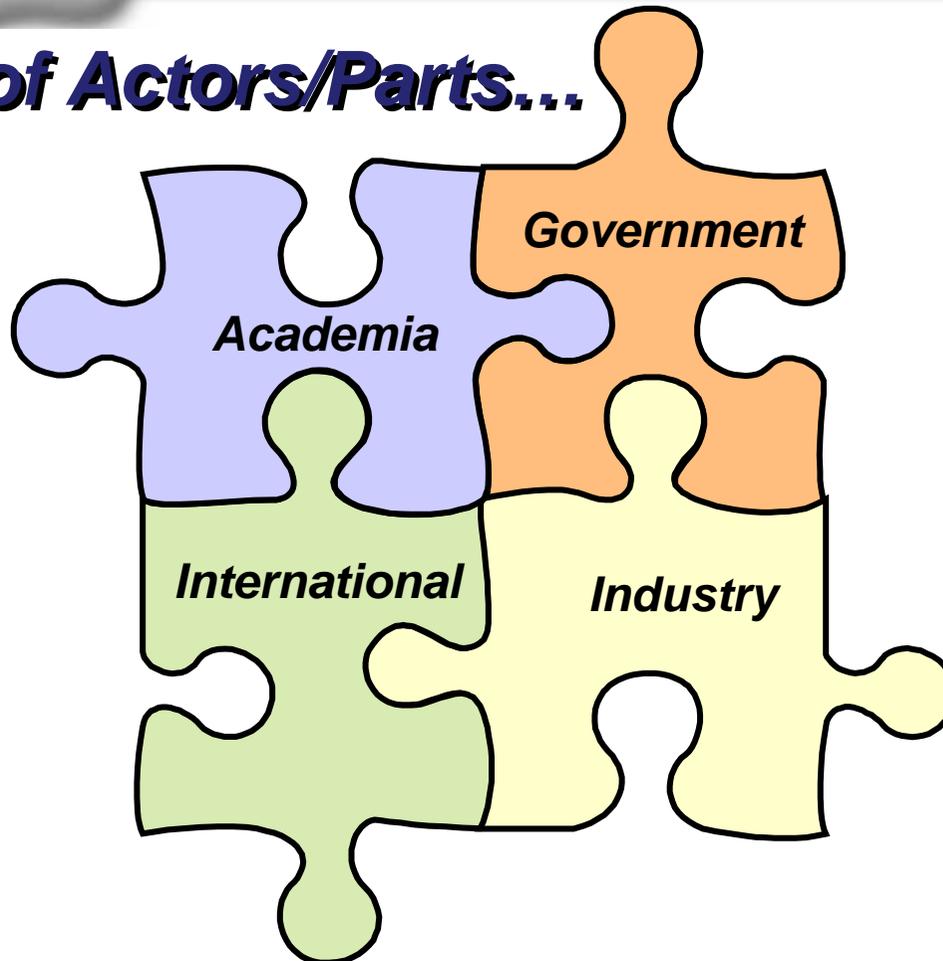


# SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

To Be Successful We Must Work  
Together

***Lot's of Actors/Parts...***



***Are there common  
Work-products /  
Solutions ?***

***...all with  
different  
Challenges.***



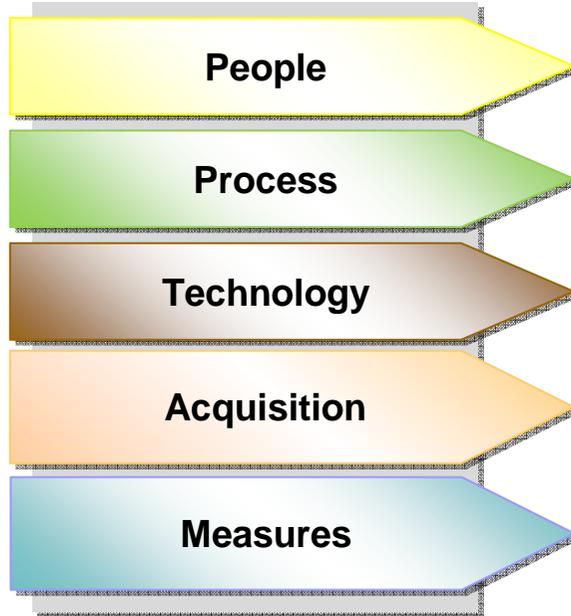
# SOFTWARE ASSURANCE FORUM

## BUILDING SECURITY IN

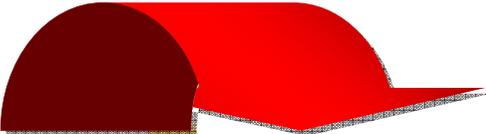
### December 2009 Working Groups

#### Key Areas identified for Working Group Collaboration

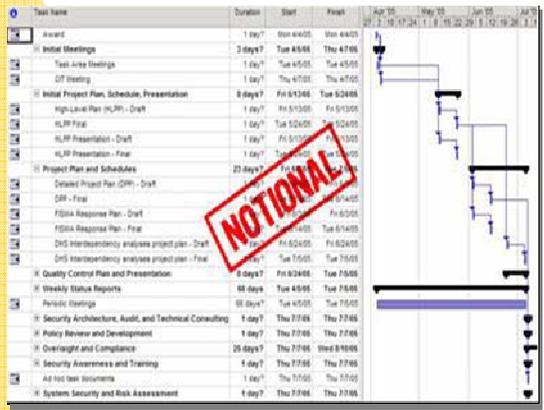
Working Groups



- ✓ Challenge of Adopting SwA through Education and Training
- ✓ Benchmarking Development Practices
- ✓ Understanding Product Characteristics throughout the SDLC
  - ▶ Enhancing Communication Between the Supplier and Acquirer
  - ▶ Making the Business case



#### “Roadmapping”





- Academia is developing curriculum models and content
- Training courses are available for security

Are students motivated to pursue these studies?

Do professionals see value in this training?



- What CAN WE DO to improve adoption of SwA Education and Training?
  - Develop the “short” list that every graduate should know (all students as digital natives create code eventually)
  - Create a game that requires player to have done good planning to win – learn by doing opportunity (another version of the “prioritize the items you have available to take on a space trip” – students could build this game and win something based on having the most fellow students play the game.
  - Schools that are considered centers of excellence will agree to turn on the security flags as evidence that their students know how to work with these restrictions (other requirements that could be used as evidence that their students are better at security)
  - Identify measures of success that can be used by education to provide evidence that students know and understand security issues.
  - Identify for each level of student (K-12, community college, undergrad, masters) the critical set of knowledge they need for security to be considered educated; build modules so this minimum set can be easily taught by instructors who are also in the learning mode



- People
  - Identify and communicate what we have already accomplished
  - Leverage what we have done and recommendations from the BoF to Develop a plan of action to BALANCE Supply/Demand for education and training
    - a. Identify target audience(s)
    - b. Identify speakers/messenger(s) to deliver to the target audience(s)
    - c. Identify the message(s) for each audience
    - d. What do we want the audience(s) to do? → our measure of success is what action they take



- Industry has documented developed frameworks, models, and standards for SwA
- Examples of successful implementation approaches are available

Are acquirers motivated to understand their risk exposure associated with the SwA practices of their suppliers?

Are suppliers motivated to understand the existence and effective implementation of SwA practices within their organization?



- What can we do to increase the understanding and communication of what SwA Practices are and are not being done?
- Recommendations:
  - Simply define the key PRINCIPLES/GOALS that are common
  - Simply articulate the “Why” (MOTIVATION) for the principles
  - Map the Principles and Why’s to the various “Hows” being used by used by different stakeholder communities
  - Translate the Principles and Motivation to reach a broader set of our stakeholders (AUDIENCE)



- Process
  - Identify high-level key principles of “Rugged” software
    - a. Must be above existing models (and not exclude them) – harmonizing strength and weaknesses
    - b. Can we measure any of the principles
    - c. Who needs to adopt the principles (target audience)
    - d. Leverage BoF input to develop a Plan (including message and messengers) for reaching the target audience



- There are robust SwA Practices
- There are robust SwA Technologies

We don't have a robust understanding of how they work together through the SDLC



- What CAN WE DO to better understand the product characteristics throughout the SDLC?
  - Identify Groups of technologies and technical standards
  - Identify 3-5 stakeholder groups
  - Identify the economic, mission, or other value of the technology groups for each stakeholder
  - Leverage measures and existing standards and processes to help communicate to the appropriate stakeholders



- Technology
  - Identify Groups of technologies and technical standards
  - Identify 3-5 stakeholder groups
  - Identify the economic, mission, or other value of the technology groups for each stakeholder
    - a. How do SwA Tools fit in the SDLC
    - b. Who controls the enterprise testing processes\How do we influence enterprise (.mil, .gov, .com) testing processes (what data feeds milestone decisions)
  - Identify speakers/messenger(s) to deliver to the target audience(s)



- Creating Deliverables To Reach New Stakeholders (Executives, First Responder, Stakeholder Communities, CIP)
- Contributing to International Standards
- Understanding Hot Topics
- Planning Ahead

### Next Steps

- Co-Chair's Collaborate to
- Act on BoF input
  - Address Public/Private Leadership Contributions
  - Create a SwA "sound-byte" to US Cyber Advisor

<u>Mon</u>	<u>Tues</u>	<u>Wed</u>
<ul style="list-style-type: none"> <li>✓ <b>Challenge of Adopting SwA through Education and Training</b></li> <li>✓ <b>Benchmarking Development Practices</b></li> <li>✓ <b>Understanding Product Characteristics throughout the SDLC</b> <ul style="list-style-type: none"> <li>▶ SwA Automation Protocol (CWE, CAPEC, MAEC)</li> <li>▶ Making the Business Case for SwA</li> </ul> </li> </ul>		

### Working Group Deliverables

- Communicate Business Enablers
- Recommend Governance Actions to Senior Leadership
- Define and Implement Strategy for Reaching New Stakeholders



- ▶ Enhancing Communication Between the Supplier and Acquirer
- ▶ How do we match supply and demand of resources to address SwA?
- ▶ Legal Aspects of Due Diligence/ Due Care and application of SwA Standards



- How do we more proactively collaborate with Industry Organizations that ARE advancing SwA?
- How do we collaboratively reach the stakeholder community outside of our current audience?

<u>Mon</u>	<u>Tue</u>	<u>Wed</u>	<u>Thu</u>	<u>Fri</u>
Cyber / SwA Education	<u>Stakeholders</u> SAFEcode, OWASP, EC Council (ISC)2, FS-ISAC, OMG, Others		<u>Planning</u>	NIST Static Analysis & Tools Exposition