NDIA Software Assurance Summit
S&T Outbrief

Industry insights and ongoing assurance S&T efforts

- What are Industry strategies and best practices?
  - Evaluation capability is needed
  - Ensure programs of record are going to require evaluations as part of doing business
    - Establish the market
  - STSC as a model for the EA/CAS
  - Vendors engage academia for research, new ideas
  - Emerging tools are being incorporated into curricula – graduates are increasing familiar with new development techniques, tools
  - Vendor base for SwA tools exists although current tools don't yet address all SwA needs
  - Critical systems may need to live without the latest/greatest to avoid or reduce vulnerability risks

- What lessons have been learned?
  - Make sure the need is there otherwise we won't get the necessary resources
    - ROI on the cost of having a vendor get their product certified
  - Allow vendors and suppliers to conduct most of the cert as centralized cert will be too expensive, take too long

Industry Thoughts Regarding DoD Strategy Elements

- Identify barriers to successful S&T
  - Getting funding for research, transition, implementation
  - Getting consensus on the direction of the research
  - Limited amount of competent resources
  - Chain for incorporating new SW technologies is too long
  - Hard fuzzy problem

- Flesh out the detailed strategy plans and products
  - Establish a research agenda
  - Process eval (CMMI) vs product evaluation
    - Don't ignore the process side for S&T
  - Tools and techniques exist or are emerging, catalog existing/emerging ideas and exploit those first
  - Ensure new approaches are timely, relevant – don't take too long for certs/evals
  - Line between security/safety/quality isn't clear – center may sell better if we increase scope

- Identify Industry Enablers, e.g., IR&D, Methodologies, Processes
  - ROI, Market
  - Pay per vulnerability?
  - Clarity of requirements
  - Establish a culture of 'due diligence' in SW industry
  - Embedded r-t system processes could carry over to increase discipline on non-r/t SW

Recommended actions for continued collaboration

- Contact Open Group regarding industry collaboration on generation of a UL-like process and activity
  - Test suites
- Get SwA on SSTC agenda
- Contact the Trusted Computing Group (Intel)
- Collaborate/coordinate research with Microsoft
- West Coast SW Development forum participation
- NPS/CMU/UTulsa COE?
- Consider holding our own workshop with Academia
- Upcoming HCSS workshop – get word out via industry forums
- Vendor forums? – RSA in Feb San Jose