DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

NDIA Software Assurance Summit
September 7-8, 2005

Industry Best Practices Breakout
Outbrief

Industry insights and ongoing assurance efforts

- ❑ How has industry defined the problem?
  - » General agreement with the intentional and unintentional problem scope

- ❑ What are Industry strategies and best practices?
  - » Identified 4 sheets of them…

- ❑ What lessons have been learned? (Motivators/Disincentives)
  - » Commercial Software Industry doesn't really want to know who develops the software – increase their arms length
  - » Contract SoWs, specific language would put practices on contract
  - » Knowledge of the threat
  - » Unrealistic tool expectations
  - » Policy requiring software assurance

Industry Thoughts Regarding Best Practices

- Barriers
  - » Lack of software assurance knowledge (e.g. by contract personnel)
  - » Lack of disciplined application of good software development practices that can reduce unintentional vulnerabilities
  - » Insider threats (ie. Malicious developers) are hard to counter
  - » Ability of best practices to support rapid development
  - » Cost of practice vs. benefit
  - » Software reuse implications – some practices might hinder ability to reuse other software or services
  - » Ability to reverse engineer and impact legacy products (identifying historical sources, countering momentum, etc)
  - » “too many standards”
  - » Attack speed is increasing; improved targeting approaches
  - » Economic model incentivizes poor software assurance (users will buy poor quality software; first to market is rewarded)
  - » Lack of awareness of the problem – ability to quantify the impacts
  - » Perceived lack of alternatives (products, processes)
  - » “shelf life” of a threat assessment, indicators, and who is responsible for discerning them

Recommended actions for continued collaboration

- ❑ Reach out to a broader community to capture ongoing best practices
- ❑ “Catalog” the practices
  - » Maturity
  - » Who are the experts/who is doing them
  - » Organize them (domain, etc.)
  - » Costs/benefits of each
  - » Where they are applicable
  - » Identify existing processes where these practices might apply
- ❑ Share the threat data with the practitioners to increase awareness
  - » Knowledge of bad actors
  - » Methods, and how to counter
- ❑ Provide a mechanism for interested practitioners to subscribe to this community of interest