Getting the Workforce to
Factor Enterprise Risk into Outsourcing Decisions

What is Supply Chain Risk Management?

- Supply chain risk management (SCRM) ensures that the enterprise's sourced products (HW&SW) and services are functionally correct

- SCRM encompasses five different categories of risk*

  1. Installation of **malicious logic** in hardware or software
  2. Installation of **counterfeit** hardware or software
  3. Failure or **disruption** in the production or distribution of a critical product or service
  4. Reliance upon a **malicious or unqualified** supplier
  5. Installation of **unintentional vulnerabilities**

* US General Accounting Office (GAO) March 23, 2012 p. 12

What is Supply Chain Risk Management?

- The key outcome of -SCRM is that it guarantees that an organization's sourced products do what they are intended to do **and only that**
- SCRM is enforced through a system-of-systems Enterprise Security Framework (ESF) of controls
- Mitigations are designed and deployed through a formal criticality analysis and prioritization scheme (defense in depth)
- The aim of SCRM is to ensure that **we fully understand all meaningful risks (to the enterprise)** when arriving at a make-buy decision?

Building a Unified Body Practice for SCRM

- Practices from a ange of conventional fields could conceivably be part of a unified body of practice for ICT supply chain risk management
  - hardware and software engineering
  - systems engineering
  - information systems security engineering
  - Safety
  - Reliability
  - Testing
  - information assurance
  - project management
  - Intelligence
  - Legal
  - International relations

A Short Conclusion

- The problem addressed by our initiative is, how to manage enterprise-risk from globally sourced ICT sub-components- that may **not function as anticipated and may in fact have undesired functionality"**

- It is critical to get enterprise risk under control since most of of society's functionality/capability is dependent on ICT sub-components

- **We hope that we can enlist your help and support in developing and finalizing a correct and relevant unified concept**

THANK YOU FOR YOUR ATTENTION

Dan Shoemaker, PhD, Director and Senior Research Scientist

Global EdICT - Supporting Don Davidson, Chief of Outreach Globalization Task Force (GTF) OASD-NII / DoD CIO

dan.shoemaker@att.net