Acquisition and Intelligence Community Collaboration

Kristen Baldwin

Deputy Director, Software Engineering and System Assurance
Office of the Deputy Under Secretary of Defense
(Acquisition and Technology)

Outline

- **Discuss two examples of the growing collaboration between Acquisition and Intelligence communities:**
  - **DoD Systems Engineering Research University Affiliated Research Center**
  - **DoD Acquisition Cyber Security and Program Protection**
- **Describe opportunities to engage**

Systems Engineering Research

University Affiliated Research Center

The Need

- **Current SE methods, processes, tools do not address the breadth, complexity, and tempo of today's development environment.**

- **Although systems engineering is recognized as key to delivering weapon systems, there is no single body leading the effort to advance SE methods, processes, and tools (MPTs) to support DoD challenges…nor funding line.**

- **There is an inadequate supply of systems engineers experienced with the breadth and complexity of DoD's current development environment.**

The Solution

- **Provide funding for a center to lead, coordinate, and harmonize research focused on delivering improved SE MPTs that support DoD challenges**

  - **Establishes and maintains essential systems engineering research and analysis capabilities**

  - **Nurtures and grows graduate-level systems engineering academic and research programs that support DoD acquisition program needs**
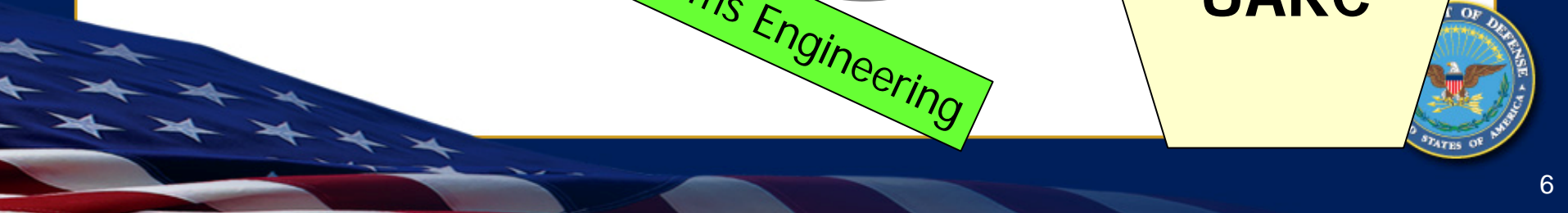
Advancing SE Practice

Acquisition Community (DoD and Industry)

Provide Lessons Learned and Challenges

- Tasking Activities
- Industry
- Associations
- Academia

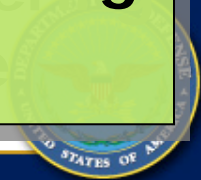Advance State of Systems Engineering

SER UARC

SER UARC Mission

To research and analyze advanced and emerging systems engineering practices and relevant technologies to address the full spectrum of DoD and Intelligence systems across the Department

Goal: Ensuring consistency and systems engineering excellence throughout the acquisition cycle

SER UARC Team

UARC Lead Organizations

STEVENS Institute of Technology

USC UNIVERSITY OF SOUTHERN CALIFORNIA

Members

- Auburn University
- Air Force Institute of Technology
- Carnegie Mellon University
- Fraunhofer Center at UMD
- Massachusetts Institute of Technology
- Missouri University of Science and Technology (S&T)
- Pennsylvania State University

- Southern Methodist University
- Texas A&M University
- Texas Tech University
- University of Alabama in Huntsville
- University of California at San Diego
- University of Maryland
- University of Massachusetts
- University of Virginia
- Wayne State University

Summary

- **UARC will address SE research challenges across DoD and the Federal Government**

- **Research results (new/improved MPTs) will be shared across Government and industry to improve SE practice.**

- **Opportunity for DoD and Industry investment**
  - **Advance the state of Systems Engineering**
  - **Nurture and grow graduate-level systems engineering academic and research programs**

UARC Program Manager
Dennis Barnabe
drbarnab@nsa.gov

UARC Deputy PM
Sharon Vannucci
sharon.vannucci@osd.mil

DoD
Cyber Security
And
Program Protection

Increased Priority for Program Protection

- ★ *Threats*: Nation-state, terrorist, criminal, rogue developer who:
  - ✴ Gain control of IT/NSS/Weapons through supply chain opportunities
  - ✴ Exploit vulnerabilities remotely
- ★ *Vulnerabilities*: All IT/NSS/Weapons (incl. systems, networks, applications)
  - ✴ Intentionally implanted logic (e.g., back doors, logic bombs, spyware)
  - ✴ Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- ★ *Consequences*: Stolen critical data & technology; corruption, denial of critical warfighting functionality

System Assurance is the confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted during the lifecycle
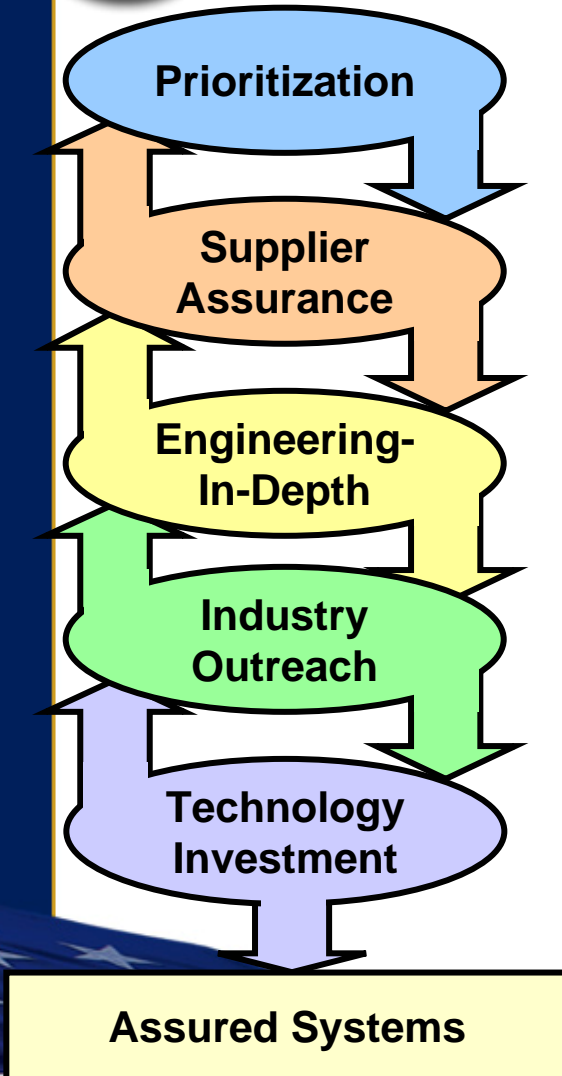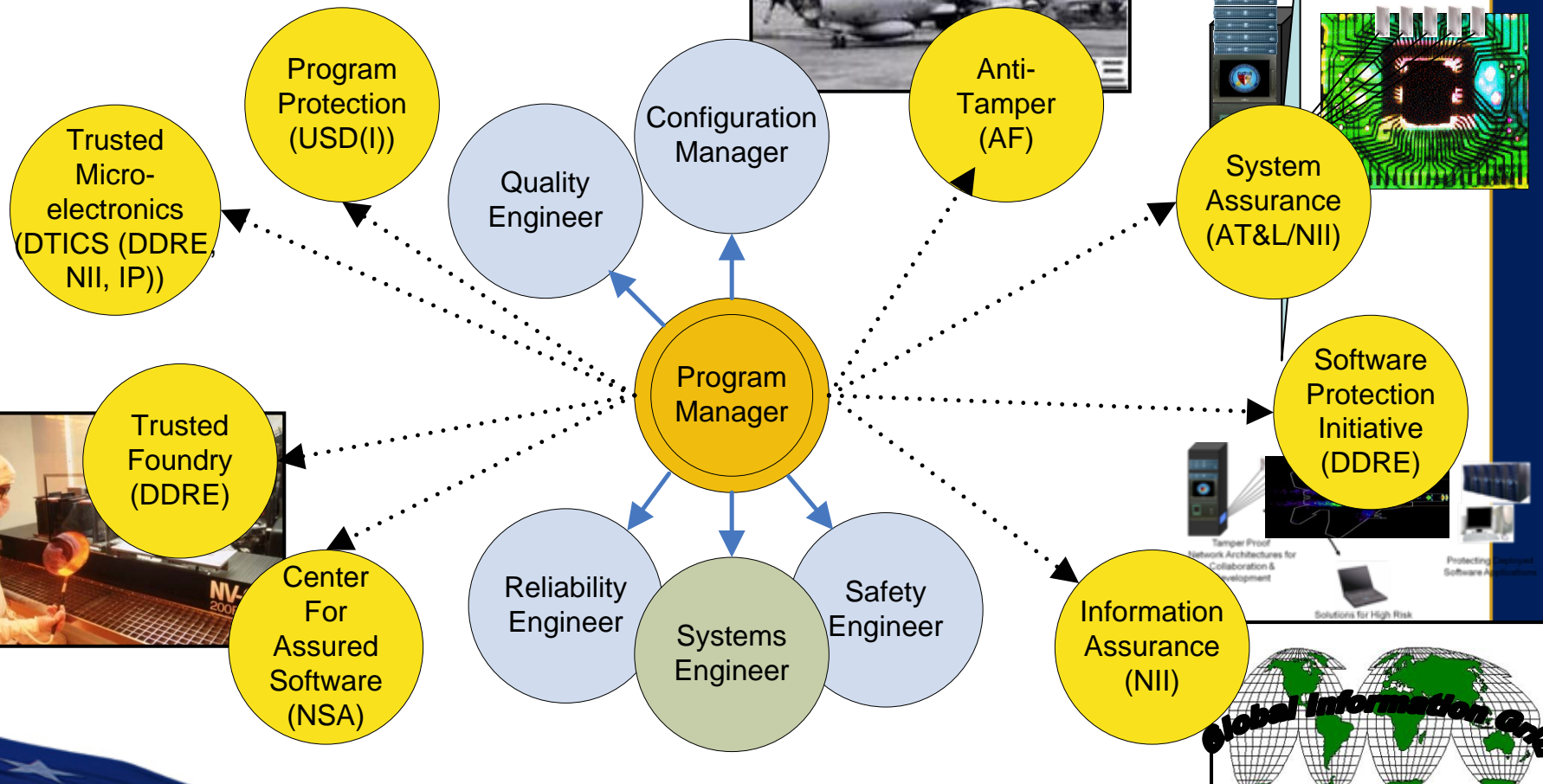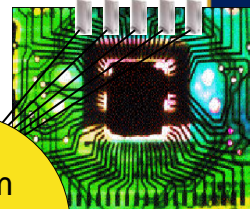
The Solution Components

Prioritization

Supplier Assurance

Engineering-In-Depth

Industry Outreach

Technology Investment

Assured Systems

Vision of Success

★ **The requirement for assurance is allocated among the right systems and their critical components**

★ **DoD understands its supply chain risks**

★ **DoD systems are designed and sustained at a known level of assurance**

★ **Commercial sector shares ownership and builds assured products**

★ **Technology investment transforms the ability to detect and mitigate system vulnerabilities**

Numerous Defensive Protection Strategies and Related Engineering Disciplines

Trusted Micro-electronics (DTICS (DDRE, NII, IP))

Program Protection (USD(I))

Quality Engineer

Configuration Manager

Anti-Tamper (AF)

System Assurance (AT&L/NII)

Program Manager

Software Protection Initiative (DDRE)

Trusted Foundry (DDRE)

Center For Assured Software (NSA)

Reliability Engineer

Systems Engineer

Safety Engineer

Information Assurance (NII)

Protection implemented via multiple initiatives with multiple owners

Several Assurance Efforts in Acquisition

★ **Defense Industrial Base Cyber Security**

  ✪ **DIB Information Sharing**

  ✪ **Implementing Cyber Security on Contracts**

  ✪ **Interim Policy and Near Term Pilots with Programs and Industry**

★ **Program Protection Planning**

  ✪ **Policy requiring all programs identify Critical Program Information (CPI) at MS A and submit PPP at MS B**

  ✪ **Guidance and Procedures in development**

★ **Engineering for System Assurance Guidebook**

  ✪ **Systems Engineering and Acquisition Life-Cycle Overlay for Assurance**

  ✪ **Joint Industry and Government effort, released 1 Oct 08**

Critical Program Information

- ⭐ **"CPI. Elements or components of an RDA program that, if compromised, could cause significant degradation in mission effectiveness;**

  - ✩ **Includes information about applications, capabilities, processes, and end-items.**

  - ✩ **Includes elements or components critical to a military system or network mission effectiveness.**

  - ✩ **Includes technology that would reduce the US technological advantage if it came under foreign control…"**

  DoDI 5200.39

Program Protection Envisioned Benefit

Program Benefit

- Coherent direction and integrated policy framework to respond to security requirements
- Risk-based approach to implementing security
- Provision of expert engineering and intelligence support to our programs
- Streamline process to remove redundancy; focus on protection countermeasures

DoD Benefit

- Reduced risk exposure to gaps/seams in policy and protection activity
- Improved oversight and focus on system assurance throughout the lifecycle
- Ability to capitalize on common methods, instruction and technology transition opportunities
- Cost effective approach to "building security in" where most appropriate

Expanding DoD Industry Partnership

- ★ **Acquisition Cyber Security is a long term interest for DoD**
  - ✭ **Fully anticipating Cyber Security is expected to be a ongoing priority for the new administration**

- ★ **DoD will continue to take advantage of the global marketplace and COTS solutions**
  - ✭ **Engineering for System Assurance seeks to identify and fortify critical components allowing incorporation of COTS**
  - ✭ **Industry outreach must explore strategy for commercially reasonable assurance for globally sourced products**

- ★ **Industry is part of the solution**
  - ✭ **NDIA System Assurance Committee will continue to focus on the solution strategy**
  - ✭ **ITAA, GEIA, INCOSE, others all participate on this committee**