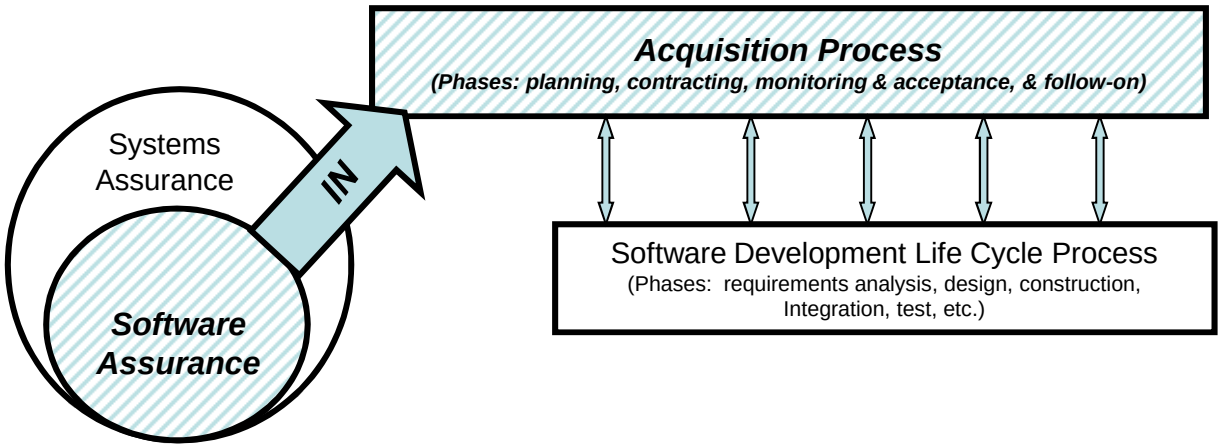
Panel Discussion: Acquisition and Mitigating Software Supply Chain Risk

Facilitator: Stan Wisseman, Co-chair of the Acquisition and Outsourcing Working Group

Mini-keynote: Matt Coose, Federal Network Security, DHS NCSD

Homeland Security



- Stakeholders need justifiable confidence that the software that enables their core mission operations can be trusted to function as expected
- Responsibility for software assurance must be shared by Acquirers in the software supply chain
- Acquirers involved in purchasing software products or services have a responsibility to factor in Software Assurance to minimize software risks
- The Working Group has published information that helps acquirers apply a risk-based approach to software acquisition/outsourcing.
- Currently co-chaired by Don Davidson (OASD/NII) and Stan Wisseman (Booz Allen)

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Participants

- *Matt Coose, DHS – Mini Keynote*
- *Robert Dix, Juniper Networks*
- *Hart Rossman, SAIC*
- *Michael Brown, FAA*
- *E. Kenneth Hong Fong, OUSD (AT&L)*

What's working today?
What else needs to be done?
How can the Acquisition working group help?

Homeland Security

Matt Coose

- Director, Federal Network Security, DHS NCSD
- Over 18 years of leadership and management experience in both the federal and private sectors and has held a variety of positions in both business and information technology, including CIO of the NPDD
- As FNS Director, works across the federal government to improve its cybersecurity posture
- Earned a B.S. in Mechanical Engineering Management, an MBA, a Masters in IT Systems, a PMP, and a Six Sigma

Homeland Security

Federal Network Security (FNS) Software Assurance Forum "An Enterprise Approach" Panel Briefing

Matt Coose, Director, Federal Network Security

Homeland Security

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Problem Statement

- ***Challenge:*** Insecure software entering the Federal IT environment through the global supply chain and system development lifecycle introduces vulnerabilities that may be easily exploited in both hardware and software.
- ***Solution:*** Obtain greater visibility into the global supply chain, employing methods to identify and close gaps among critical players (i.e. suppliers, acquisitions specialists, integrators, end users)
- This presentation will highlight the FNS Branch's mission, goals and priorities in helping agencies to "close the gaps" as it relates to software assurance

Homeland Security

- Addresses the need for a single, accountable focal point for achieving a federal enterprise security model.

- Focuses on providing the means to enable long-term strategic prevention of attacks against federal government networks by addressing common challenges faced by all agencies.

- Collaborates with the federal agency community and other National Cyber Security Division program areas in designing, implementing, and maintaining evolving security solutions that address the aggregate needs of the federal enterprise.

Homeland Security

*To be the recognized leader for **driving change** that enhances the **Cybersecurity posture** of the Federal Government*

Homeland Security

Assess Enterprise Needs and Required Capabilities

- Through interagency collaboration identify and prioritize actions required to mitigate risks and improve Cybersecurity posture across the Enterprise

Influence Policy and Strategies to Implement

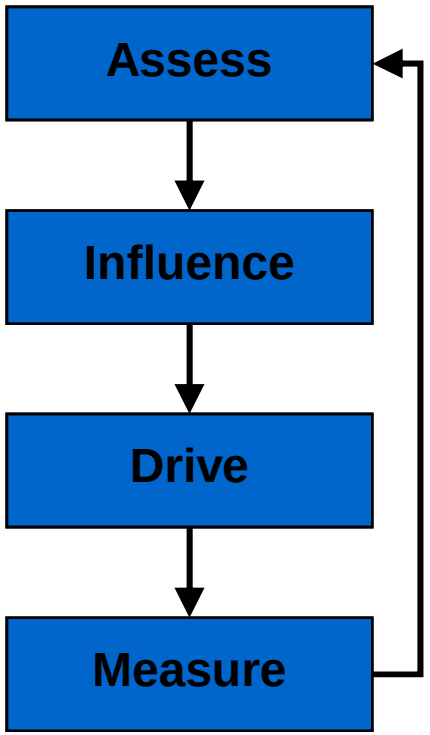
- Promote actionable Cybersecurity policies, initiatives, standards, and guidelines for implementation

Drive Implementation of Capabilities

- Enable and drive the effective implementation of Cybersecurity risk mitigation activities and capabilities

Measure and Monitor Implementation and Security Posture

- Measure and monitor agency implementation strategies and compliance with published Cybersecurity policies, initiatives, standards, guidelines and directives



Homeland Security

- Assess Enterprise Needs and Required Capabilities
  - Review the security and resilience of the currently installed base
    - Develop Red Team/Blue Team armed with static and dynamic analysis tools
      - Composition of teams
      - Identify exploitable weaknesses in the current networks
      - Use SCAP plus CWE and CAPEC to determine security and resilience of the installed base (Federal Enterprise)
    - Determine the feasibility of identifying a Shared Service Center or Industry acquisition as a Center of Excellence for Software security and resiliency

Homeland Security

- Influence Policy and Strategies to Implement
  - Advocate use and evolution of Security Control Automation Protocol SCAP (Policy)
  - Advocate use and evolution of Common Weakness Enumeration (CWE)
  - Advocate use and evolution of Common Attack Pattern Enumeration and Classification (CAPEC)
  - Influence the content of the NIST Inter Agency report 7622 (Draft 1 30 Sept. 09) Supply Chain Risk Management Practices for Federal Information Systems

Homeland Security

- Drive Implementation of Capabilities
  - Mitigate Enterprise Security Risk through Acquisitions/Procurements
  - Work with GSA to include on the GSA Schedule additional vendor supplied data on the vetting of the suppliers process and products
  - Include security provisions/language in Information Systems Security Line of Business (ISSLOB) acquisitions for Situational Awareness and Incident Response (SAIR/SmartBuy) tools and services
  - Leverage NCSD Programs (Supply Chain Risk Mgmt, SW Assurance) to provide community collaboration and increased awareness for advancing this effort.

Homeland Security

- Measure and Monitor Implementation Strategies and Security Posture
  - Measure and Monitor implementation of cyber security initiatives
    - Security Control Automation Protocol SCAP
    - Common Weakness Enumeration (CWE)
    - Common Attack Pattern Enumeration and Classification (CAPEC)
  - Identify relevant standards and reference models to address security process and practices (eg, ISO, NIST)
    - Guide process improvement
    - Benchmark organizational capabilities
    - Assert claims about product security and resiliency

Homeland Security

Robert B. Dix, Jr.

- Vice President of Government Affairs & Critical Infrastructure Protection for Juniper Networks
- Has served in senior leadership roles in industry and government, including serving as Staff Director for the House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census during the 108th Congress
- Represents Juniper on the Industry Executive Subcommittee for the President's National Security Telecommunications Advisory Committee and currently serves as Chair of the IT Sector Coordinating Council. Mr. Dix serves on the National Security Task Force for the U. S. Chamber of Commerce and the Executive Committee for the Partnership for Critical Infrastructure Protection.

Homeland Security

DoD-DHS-NIST Software Assurance Forum

Acquisition & Mitigating Software Supply Chain Risk

November 5, 2009

Robert B. Dix, Jr.

Juniper Networks

Homeland Security

Global supply chain risk management is key to brand integrity

Global supply chain risk management is critical to national, homeland, and economic security

Homeland Security

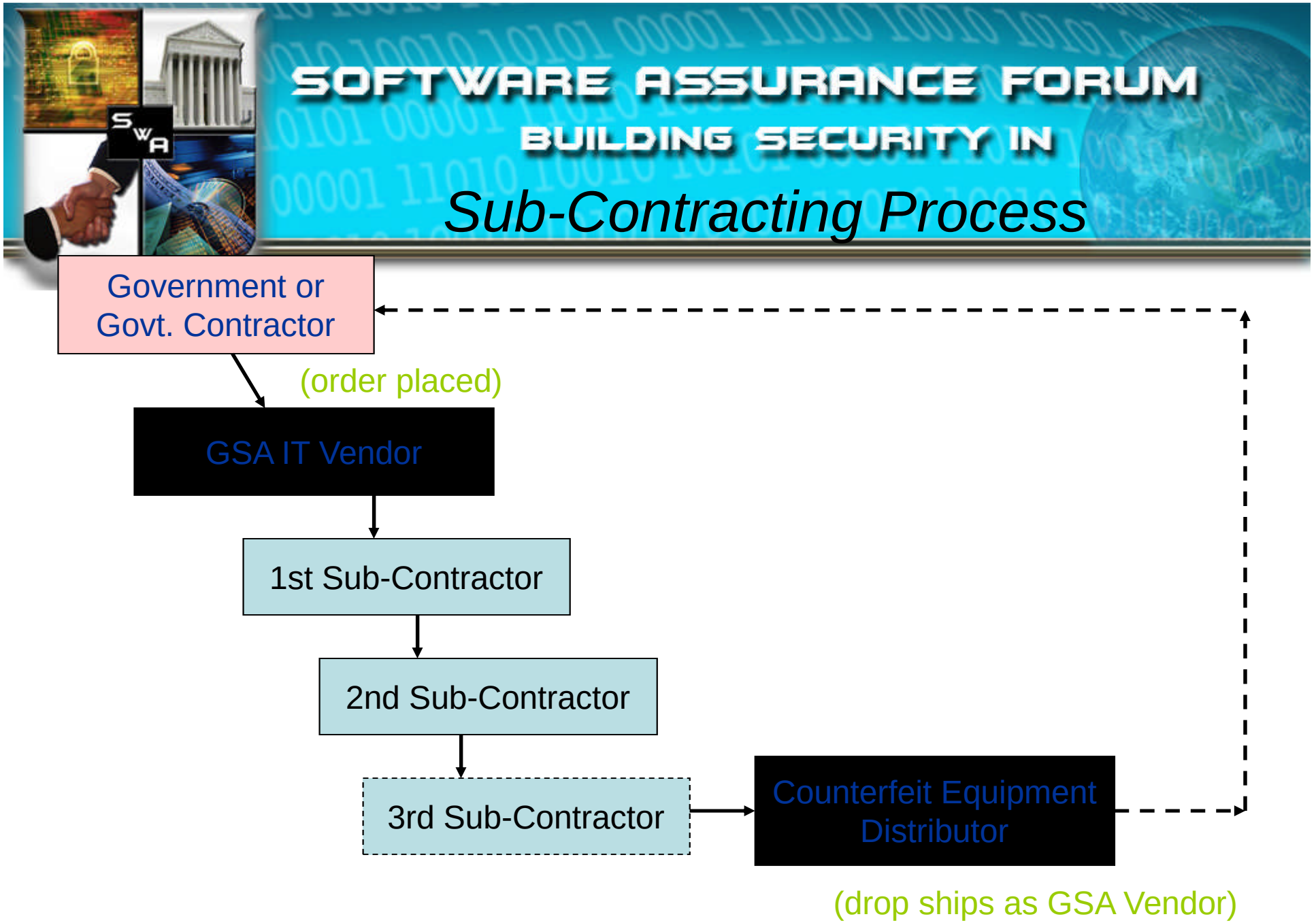
- Profit
- Extortion
- Theft of IP
- Espionage
- National Security
- Economic Disruption

Homeland Security

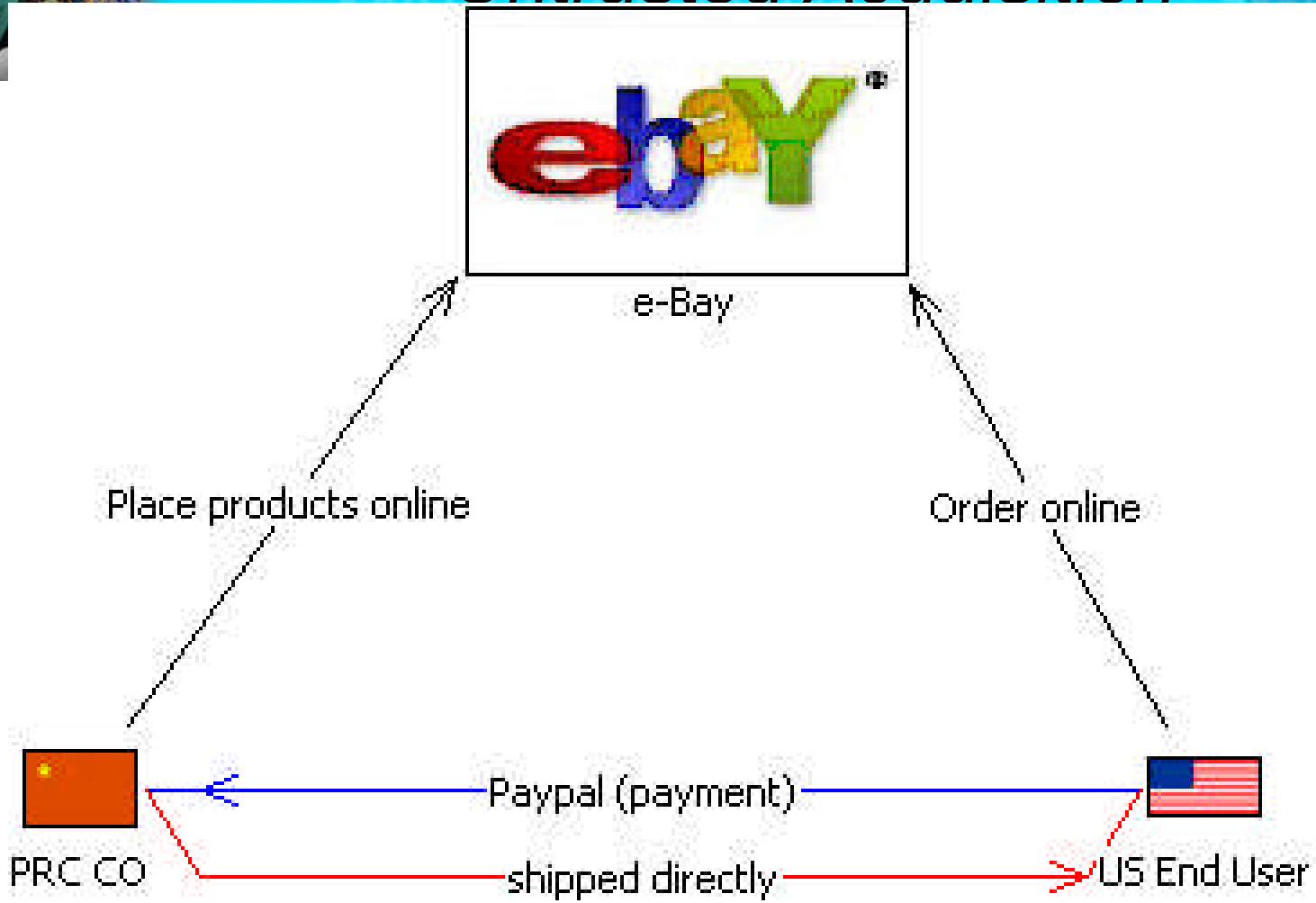
Government *MUST* buy from trusted sources

Government must secure inventory after delivery

Government & Industry must work together


SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN
Sub-Contracting Process
Government or Govt. Contractor
(order placed)
GSA IT Vendor
1st Sub-Contractor
2nd Sub-Contractor
3rd Sub-Contractor
Counterfeit Equipment Distributor
(drop ships as GSA Vendor)

Untrusted Acquisition



- Government searches for lowest price
- Contract language allows for
  - Subcontracts
    - 2 to 3 levels of sub-contractors
  - “Blind drop” or “drop ship”
  - Non-OEM purchase
  - Smaller businesses
- Little vetting of vendors by GSA
    - If done by government, usually only background check

- Industry has been dealing with supply chain risk management for quite some time
- Brand integrity life cycle- from concept to delivery
- SAFECode
- AGMA
- CACP
- Many more

THANK YOU!!

Robert B. Dix, Jr.
Vice President
Government Affairs & Critical Infrastructure Protection

571-203-2687
rdix@juniper.net

Hart Rossman

- VP/CTO for Cyber Security Solutions at SAIC
- A Senior Research Fellow with the Supply Chain Management Center at the University of Maryland, is on the IANS faculty, represents SAIC's Incident Response Team in FIRST, and is an advisor to the Corporate Executive Programme.
- Earned an MBA from the University of Maryland, R.H. Smith School of Business, a CISSP, and CSSLP

Homeland Security

Michael Brown

- VP/CTO for Cyber Security Solutions, SAIC
- Retired as an Army Colonel after 32 years of service. As the Director of the Army's IA Office, he formulated the IA Programs for Active Army, the National Guard, and the Army Reserves
- As the FAA CIO, he is responsible for C&A, risks assessments, training, policy development, compliance reviews, access and identify management, and a major SOC
- Has received numerous awards from the FAA, DOT, Dept of Education, the Legion of Merit, and Meritorious Service Medal

Homeland Security

E. Kenneth Hong Fong

- Sr. Systems Engineering Analyst, OUSD (AT&L)
- Has 35 years of experience in leadership positions
- Currently provides systems assurance analysis and engineering support to DoD Programs of Record from an OSD level. The program protection is focused on identification and protection of critical functions and their underlying technologies and components
- Earned BA from Northeastern Illinois University, and MS from DePaul University

Homeland Security

November 2009 Software Assurance Forum
Acquisition and Mitigating Software Supply Chain Risk

~

Kristen Baldwin, Director Systems Analysis
System Engineering Directorate
Office of the Director Defense, Research and Engineering
Office of the Under Secretary of Defense for Acquisition, Technology and Logistics

05 November 2009

Agenda

- New Threats and Vulnerabilities & Public Laws
- Leverage Existing Security Policies
- Policy Implementation Path Forward
  - CPI Protection Designed-in Early & Continued Throughout Lifecycle
  - One System Security Engineering Process
- Recent Activities
- Counterfeits

Identify and Protect

Critical System Information

Washington, D.C. - At a conference in Washington, D.C., this week, a Department of Defense official sounded a startling alarm.

"The defense community is critically reliant on a technology that obsoletes itself every 18 months, is made in unsecure locations and over which we have absolutely no market share influence," said Ted J. Glum, director of the DoD's Defense Microelectronics Activity unit.

"Other than that," he cracked, "we're good."

Forbes.com

Business In The Beltway
Pentagon Worries About Chinese Chips
Andrew T. Gillies, 09.04.08, 3:09 PM ET

- Software Supply Chain Risk. **The risk that the opportunity to corrupt software poses to the organization. The industrial base increasingly relies on software for components and services that support its critical information and systems. However, the complex, transitory, and global nature of the commercial software marketplace provides opportunities for bad actors to gain unauthorized access to data, alter data, disrupt operations, or interrupt communications by inserting malicious code into or otherwise corrupting components bound for information technology systems.**

- *Threats*: Nation-state**, terrorist**, criminal**, rogue developer** who:
  - Gain control of systems through **supply chain opportunities**
  - **Exploit vulnerabilities remotely**
- *Vulnerabilities*: All 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 technology; corruption, denial of critical warfighting functionality, or loss of information about these areas

Today's acquisition environment drives the increased emphasis:

Then		Now
Standalone systems	>>>	Networked systems
Some software functions	>>>	Software-intensive
Known supply base	>>>	Prime Integrator, hundreds of suppliers

- **Per DoD Instruction 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense*, July 16, 2008, it is DoD policy:**

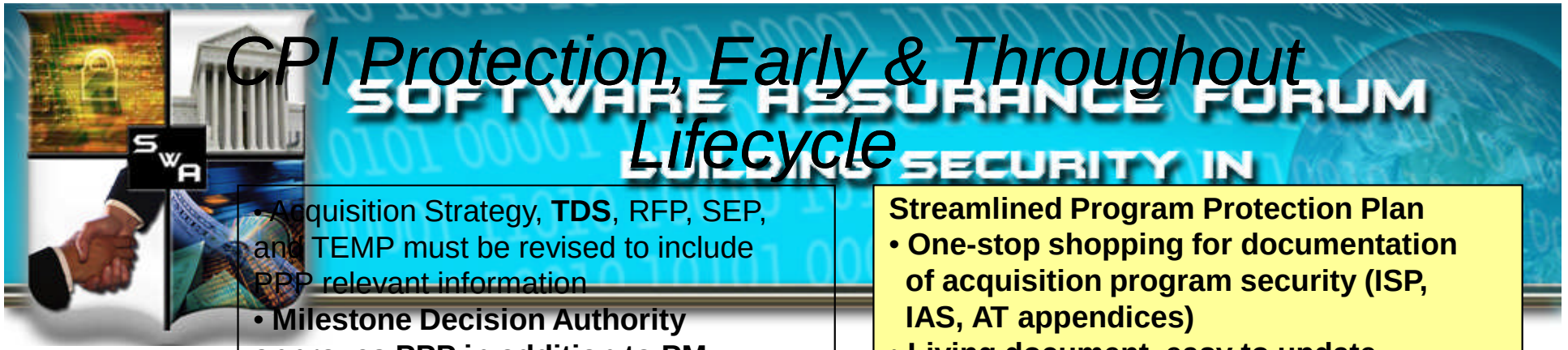
  b. To mitigate the exploitation of CPI, extend the operational effectiveness of military systems through application of appropriate risk management strategies, employ the most effective protection measures, to include system assurance and anti-tamper (AT), and document the measures in a Program Protection Plan (PPP)

  …

  g. To minimize the chance that the Department's warfighting capability will be impaired due to the compromise of elements or components being integrated into DoD systems by foreign intelligence, foreign terrorist, or other hostile elements through the supply chain or system design.

  h. To require that contracts supporting RDA programs where CPI has been identified shall contain contractual terms requiring the contractor to protect the CPI to the standards articulated in this Instruction.

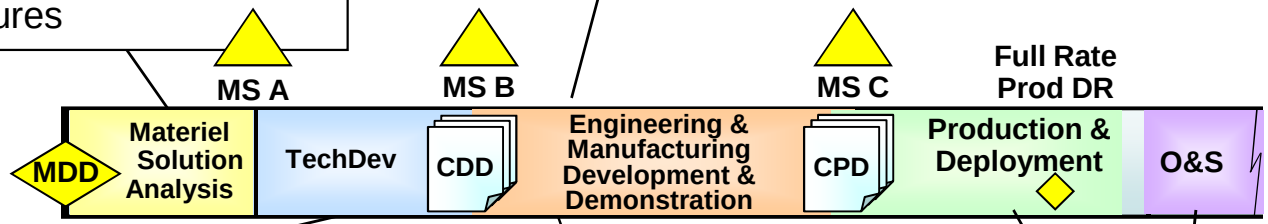
CPI Protection, Early & Throughout Lifecycle



- Acquisition Strategy, **TDS**, RFP, SEP, and TEMP must be revised to include PPP relevant information
- **Milestone Decision Authority approves PPP in addition to PM**

Streamlined Program Protection Plan
- **One-stop shopping for documentation of acquisition program security (ISP, IAS, AT appendices)**
- **Living document, easy to update, maintain**
- **OSD, Service & Security SMEs Working Towards Horizontal Protection**

- Identify draft CPI, estimated protection duration and S&T Lab countermeasures



- Obtain threat assessments from Intel/CI, **assess supplier risks**
- Develop design strategy for CPI protection
- Submit PPP to Acquisition Security Database (ASDB)

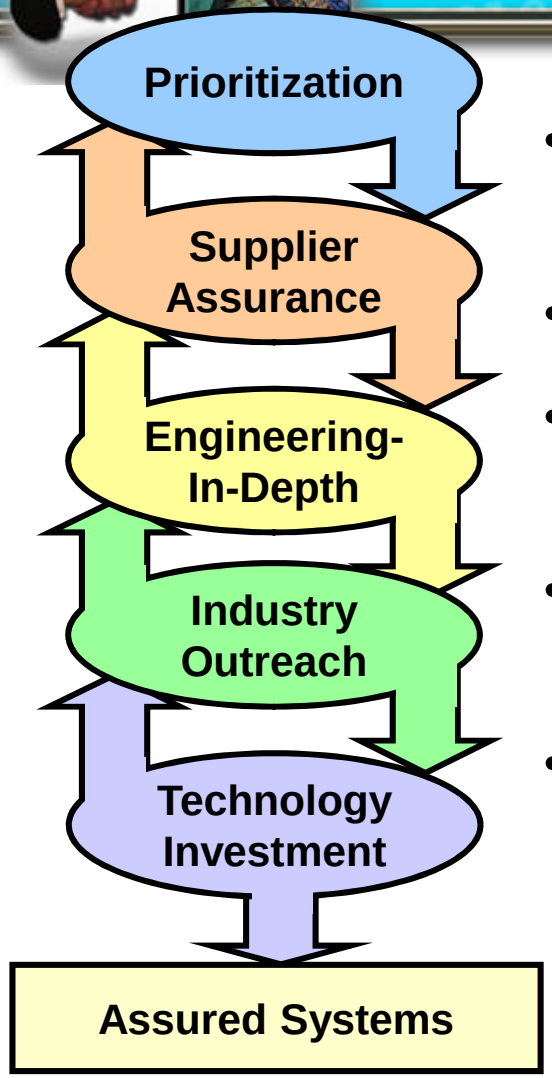
- Contractor designs in CPI Protection Plan through System and **Software Security Engineering**
- Preliminary verification and validation that design meets assurance plans

- Enhance countermeasure information in Program Protection Plan (PPP)
- Evaluate that CPI Protection RFP requirements have been met

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Acquisition and Mitigating Software Supply Chain Risk



- The requirement for assurance is allocated among the right systems and their critical components
- Awareness of supply chain risks
- 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

- **Deputy Secretary of Defense Directive-Type Memorandum (DTM) 08-048, "Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems":**

  Purpose. This DTM establishes policy and a defense-in-breadth strategy for managing supply chain risk to information and communications technology (ICT) within DoD critical information systems and weapons systems in accordance with National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (Reference (a)). The DTM also assigns responsibilities to meet the assessment and reporting requirements of section 254 of Public Law 110-417 (the Fiscal Year 2009 National Defense Authorization Act) (Reference (b)). Furthermore, the DTM directs actions in accordance with DoD Instruction 5200.39 (Reference (c)).

DoD Direction (cont)

FY 2009 National Defense Authorization Act, SEC. 254. TRUSTED DEFENSE SYSTEMS.

(a) VULNERABILITY ASSESSMENT REQUIRED.—The Secretary of Defense shall conduct an assessment of selected covered acquisition programs to identify vulnerabilities in the supply chain of each program's electronics and information processing systems that potentially compromise the level of trust in the systems. Such assessment shall—

(1) identify vulnerabilities at multiple levels of the electronics and information processing systems of the selected programs, including microcircuits, software, and firmware;

(2) prioritize the potential vulnerabilities and effects of the various elements and stages of the system supply chain to identify the most effective balance of investments to minimize the effects of compromise;

(3) provide recommendations regarding ways of managing supply chain risk for covered acquisition programs; and

(4) identify the appropriate lead person, and supporting elements, within the Department of Defense for the development of an integrated strategy for managing risk in the supply chain for covered acquisition programs.

DoD Direction (cont)

- **Under Secretary of Defense Acquisition, Technology, and Logistics and Assistant Secretary of Defense Networks and Information Integration Interim Guidance on Trusted Suppliers for Application Specific Integrated Circuits (ASICs)**

  The Department of Defense is implementing a "Defense Trusted Integrated Circuits Strategy (DTICS)," as approved by the Deputy Secretary of Defense on October 10,2003. Trust is the confidence in one's ability to secure national security systems by assessing the integrity of the people and processes used to design, generate, manufacture, and distribute national security critical components (i.e., microelectronics). …

  As a first element of this strategy, policy is being developed that shall require all trusted systems of category I (Attachment 1) to employ only trusted foundry service(s) to fabricate their custom designed ICs.

- **Trusted Foundry Program** - The OUSD/AT&L, through TAPO and DMEA, is implementing an accreditation plan for design, aggregator/broker, mask and wafer fabrication, packaging and test services across a broad technology range for specialized governmental applications both classified and unclassified. The Defense MicroElectronics Activity (DMEA) has been designated by the Department of Defense through the Trusted Access Program Office (TAPO) as the accrediting authority for this program.

  Trust is defined as "the confidence in one's ability to secure national security systems by assessing the integrity of the people and processes used to design, generate, manufacture, and distribute national security critical components." -- *Michael Wynne Acting USD AT&L (27 January 2004)*

  Currently, there are 29 accredited suppliers

  http://www.dmea.osd.mil/otherdocs/AccreditedSuppliers.pdf

- What is in your system?
- Where did it come from?

Counterfeits
U. S. Government Definition

- **The following definition* was developed by the U.S. Department of Energy, Office of Environment, Safety and Health (Office of Corporate Performance Assessment)**
  - A counterfeit item is a suspect item that is a copy or substitute without legal right or authority to do so or one whose material, performance, or characteristics are knowingly misrepresented by the vendor, supplier, distributor, or manufacturer.
  - A suspect item is one in which there is an indication by visual inspection, testing, or other information that it may not conform to established Government- or industry-accepted specifications or national consensus standards.
    - Suspect items must be further investigated to determine whether they are counterfeit. When an item contains indications, but insufficient evidence, of irregularities such as noncompliance with agreed-upon specifications in the manufacturing process, it may be declared suspect.

DOE HS-32 Suspect/Counterfeit-Defective Items website (http://www.eh.doe.gov/sci) ..
S/CI-DI Process Guide (November 2004)S/CI Awareness Training Manual (October 2006)
NASA Quality Leadership Forum, March 28 & 29, 2007
Counterfeit EEE Parts Panel
Henry Livingston, BAE Systems

- Protect the Supply Chain - Implement safeguards based on industry wide anti-counterfeiting best practices such as:
  - Creating an awareness program
  - Instituting detection methodology
  - Practicing prevention
  - Developing a response strategy

Source SAE International

The Acquisition and Outsourcing Working Group is re-starting and needs your participation

https://buildsecurityin.us-cert.gov/swa/acqwg.html

Homeland Security


SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN
S
W
A

Questions?




Homeland
Security