



***CyberSecurity, US CNCI-SCRM,  
Public-Private STANDARDIZATION ...***

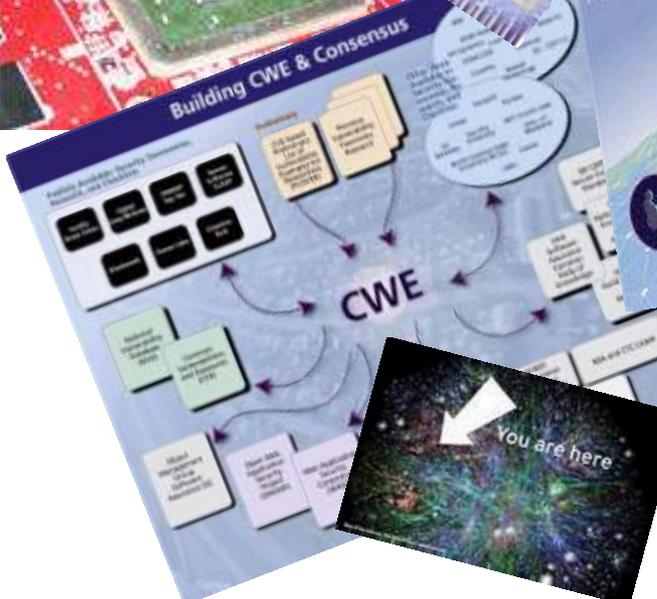
***Supply Chain & SwA***

***@ ITSAC***

***Don.Davidson@osd.mil***  
***Trusted Mission Systems & Networks***  
***OASD-NII / DoD CIO***



# CYBERSECURITY





# Comprehensive National Cybersecurity Initiative (CNCI)



Focus Area 1

- Trusted Internet Connections
- Deploy Passive Sensors Across Federal Systems
- Pursue Deployment of Intrusion Prevention System (Dynamic Defense)
- Coordinate and Redirect R&D Efforts

Establish a front line of defense

Focus Area 2

- Connect Current Centers to Enhance Cyber Situational Awareness
- Develop a Government Wide Cyber Counterintelligence Plan
- Increase the Security of the Classified Networks
- Expand Education

Demonstrate resolve to secure U.S. cyberspace & set conditions for long-term success

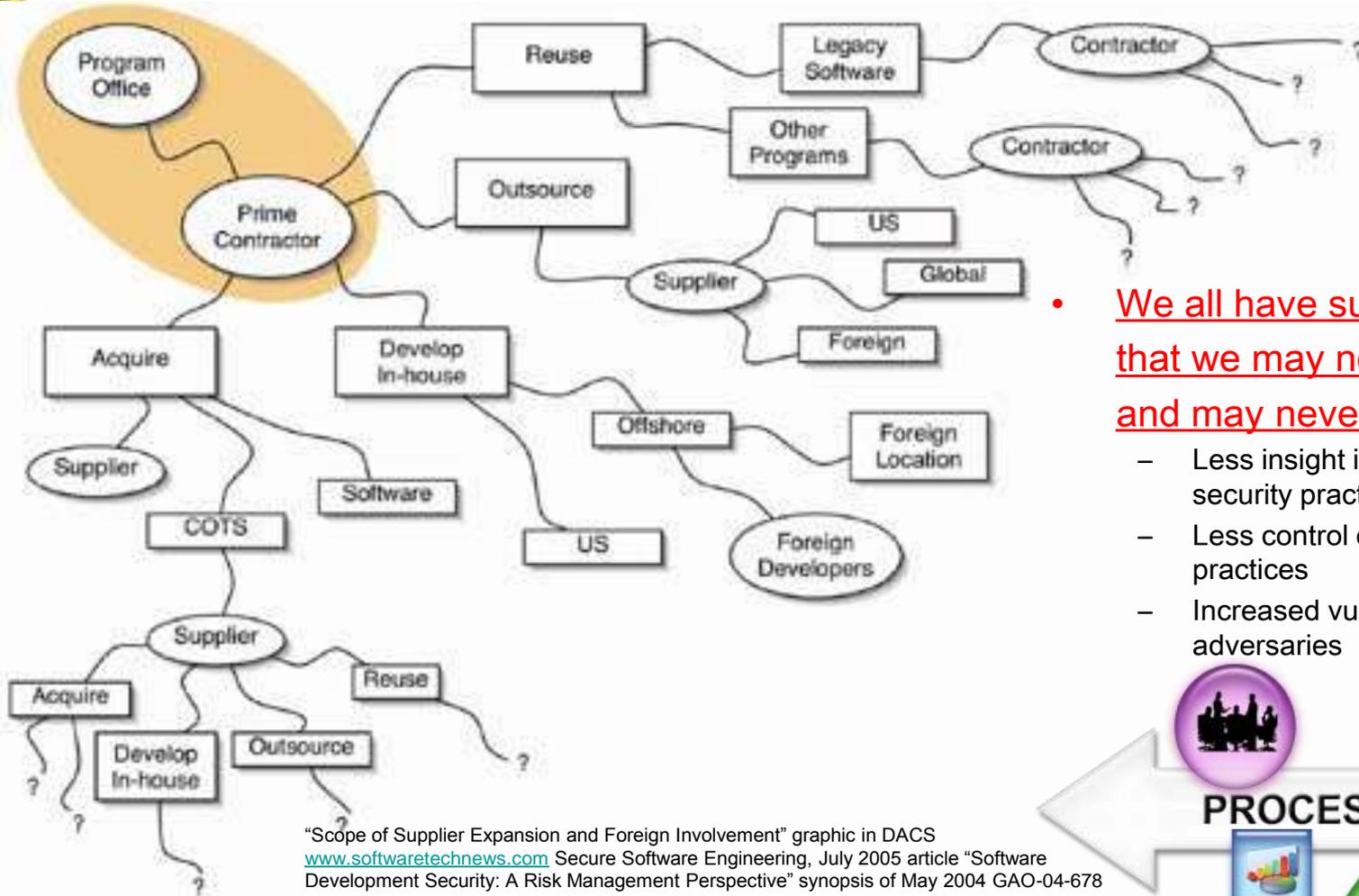
Focus Area 3

- Define and Develop Enduring Leap Ahead Technology, Strategies & Programs
- Define and Develop Enduring Deterrence Strategies & Programs
- Develop Multi-Pronged Approach for Global Supply Chain Risk Management
- Define the Federal Role for Extending Cybersecurity into Critical Infrastructure Domains

Shape the future environment to demonstrate resolve to secure U.S. technological advantage and address new attack and defend vectors



# Globalization brings challenges



- We all have suppliers that we may not know and may never see
  - Less insight into suppliers' security practices
  - Less control over business practices
  - Increased vulnerability to adversaries

"Scope of Supplier Expansion and Foreign Involvement" graphic in DACS  
[www.softwaretechnews.com](http://www.softwaretechnews.com) Secure Software Engineering, July 2005 article "Software Development Security: A Risk Management Perspective" synopsis of May 2004 GAO-04-678 report "Defense Acquisition: Knowledge of Software Suppliers Needed to Manage Risks"





# Today's Reality of our Increased Dependency Requires an Increased Confidence in our ICT



- Dependencies on technology are greater then ever
- Possibility of disruption is greater than ever because software (and overall ICT) is vulnerable
- Loss of confidence alone can lead to stakeholder actions that disrupt critical business activities



Internet users in the world: 1,766,727,004  
 E-mail messages sent today: 215, 674, 475, 422  
 Blog Posts Today: 458, 972  
 Google searches Today: 2,302,204,936

**Critical Infrastructure / Key Resources** Sectors

- Agriculture and Food
- Energy
- Transportation
- Chemical Industry
- Postal and Shipping
- Water
- Public Health
- Telecommunications
- Banking and Finance
- Key Assets

**Physical Infrastructure** Physical Assets

- Railroad Tracks
- Highway Bridges
- Pipelines
- Ports
- Cable
- Fiber
- Reservoirs Treatment plants
- Farms
- Food Processing Plants
- Hospitals
- Power Plants
- Production Sites
- FDIC Institutions
- Chemical Plants
- Delivery Sites
- Nuclear power plants
- Government Facilities
- Dams

**Cyber Infrastructure** Cyber Assets

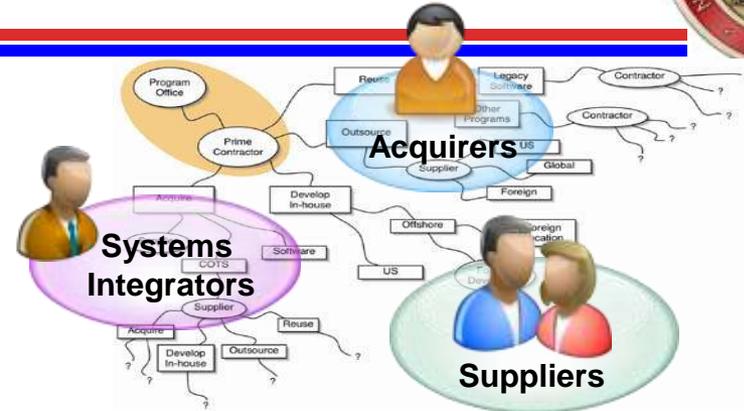
- Control Systems
  - SCADA
  - PCS
  - DCS
- Services
  - Managed Security
  - Information Services
- Software
  - Financial Systems
  - Human Resources
- Hardware
  - Database Servers
  - Networking Equipment
- Internet
  - Domain Name System
  - Web Hosting

<b>Who is behind data breaches?</b>	<p>74% resulted from external sources (+1%).          20% were caused by insiders (+2%).  <b>32% implicated business partners (-7%).</b>          39% involved multiple parties (+9%).</p>
<b>How do breaches occur?</b>	<p>7% were aided by significant errors (&lt;&gt;).          64% resulted from hacking (+5%).  <b>38% utilized malware (+7%).</b>          22% involved privilege misuse (+7%).          9% occurred via physical attacks (+7%).</p>

\* Source – 2009 Verizon Data Breach Investigations Report



# Systems Assurance TRADESPACE



Unique Requirements



Higher COST can buy Risk Reduction



**SCRM Standardization** and Levels of Assurance will enable **Acquirers** to better communicate requirements to **Systems Integrators** & **Suppliers**, so that the “supply chain” can demonstrate good/best practices and enable better overall risk measurement and management.

COTS products



Slippery Slope / Unmeasurable Reqt's

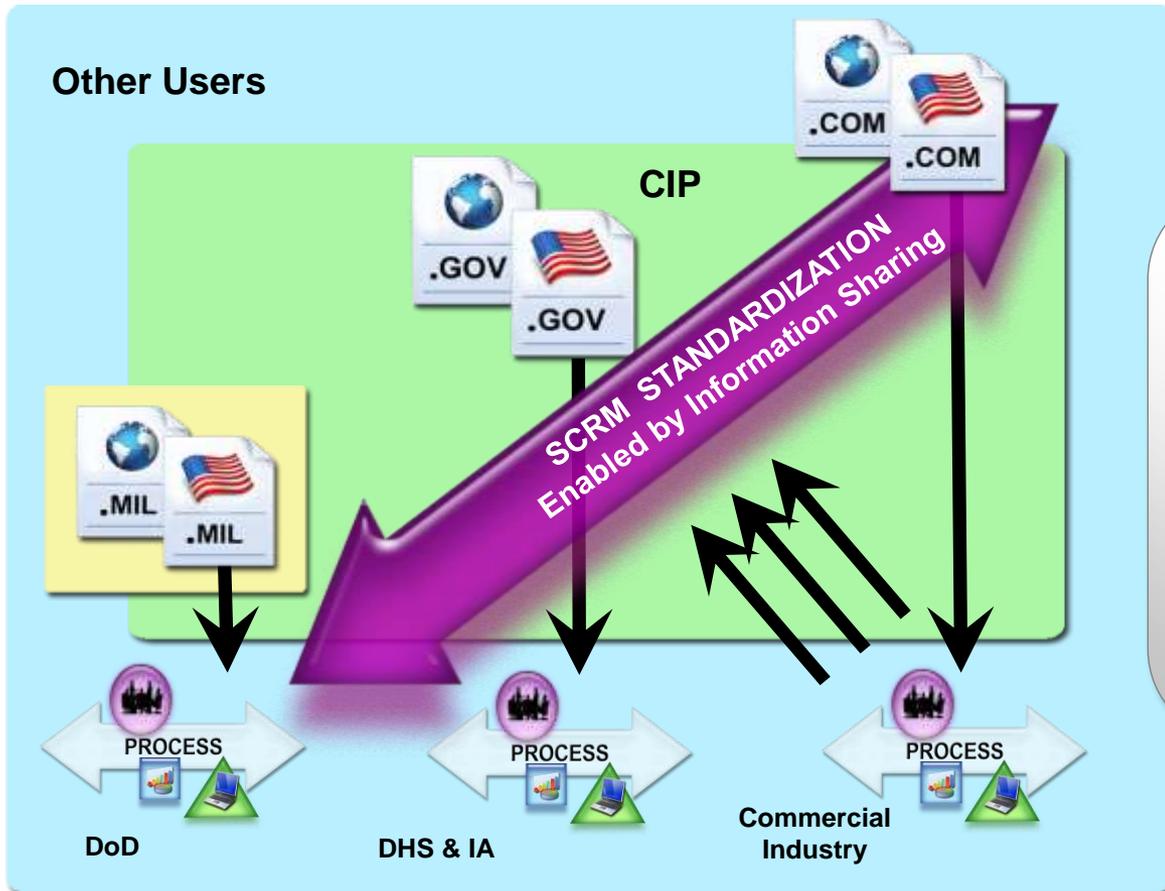
Lower Cost usually means Higher RISK



# SCRM Stakeholders



*US (CNCI) has vital interest in the global supply chain.*



***SCRM “commercially acceptable global standard(s)” must be derived from Commercial Industry Best Practices.***

***SCRM Standardization Requires Public-Private Collaborative Effort***

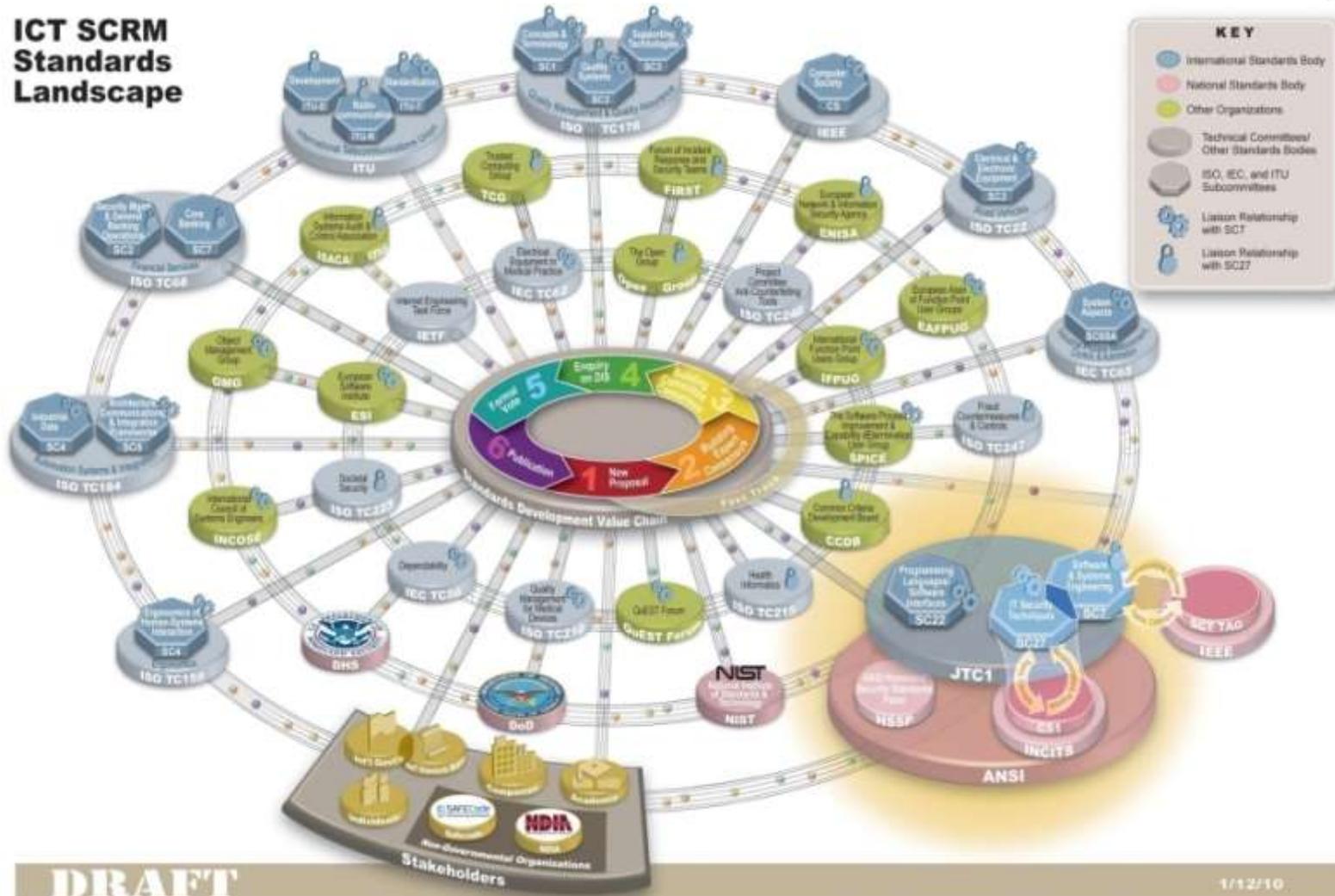


# Standards Development Organizations

## SDOs Landscape: an SCRМ Perspective



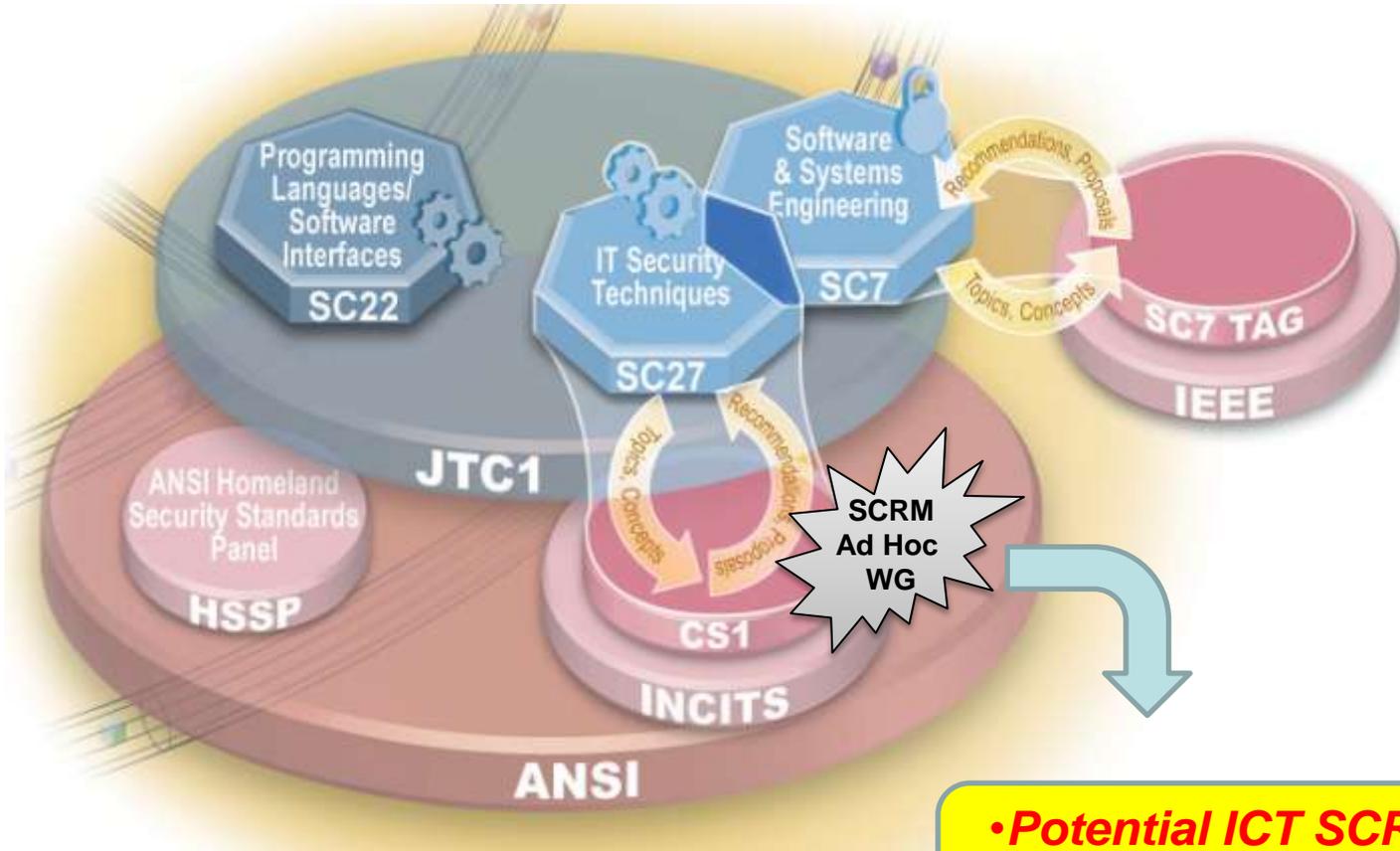
### ICT SCRМ Standards Landscape



**DRAFT**



# SCRM Study Periods: Nov'09 – Apr'10 / May-Oct'10



- **Potential ICT SCRM ISO Standard**
- **Development 2010-2013**
- **Adoption 2013-2016**