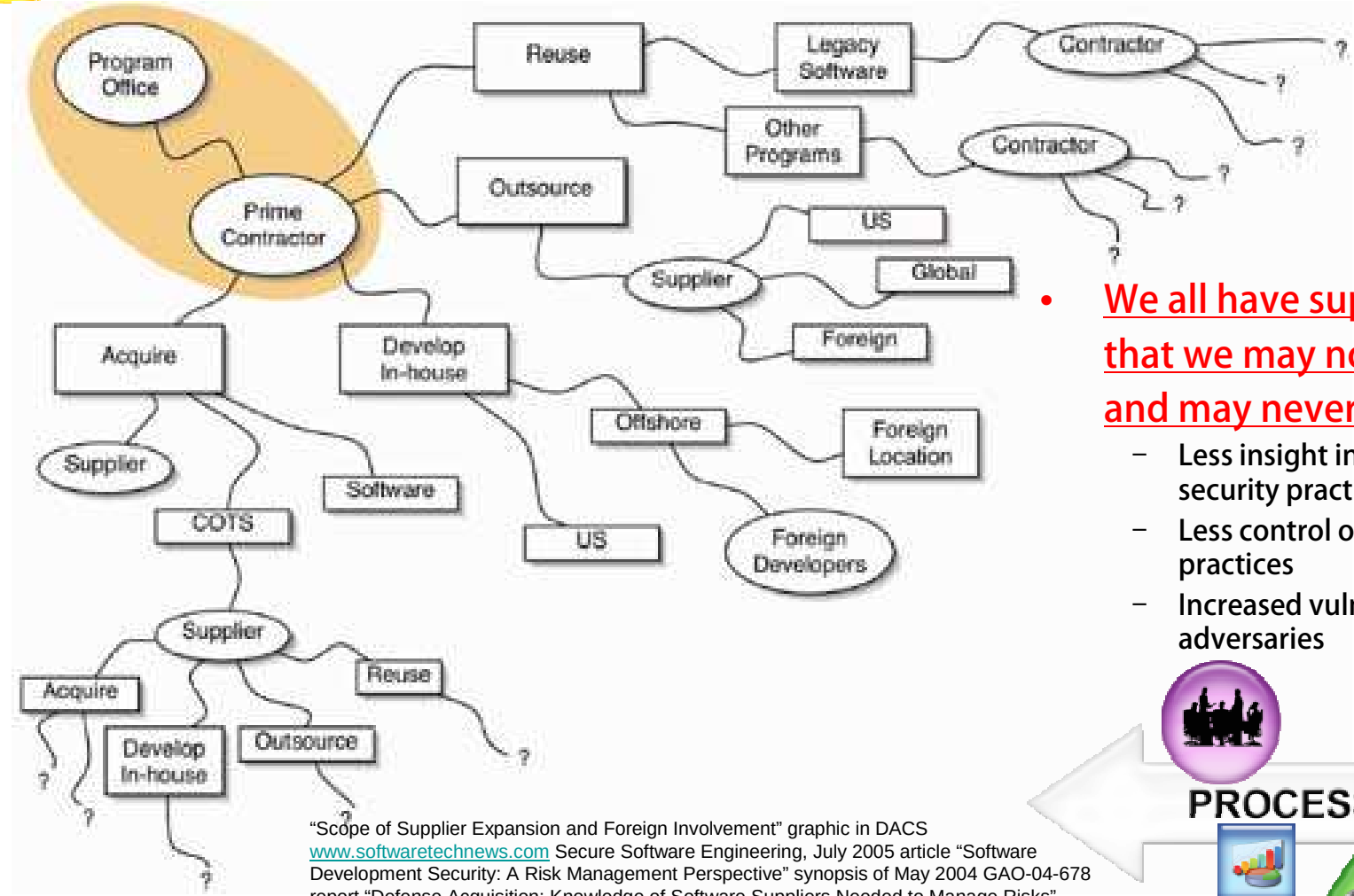
DoD introductory comments for SwA WGs (21-23 June 2010):

CYBER SECURITY, US CNCI-SCRM, & STANDARDIZATION

Don.Davidson@osd.mil
Globalization Task Force
OASD-NII / DoD CIO

CYBERSECURITY

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 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

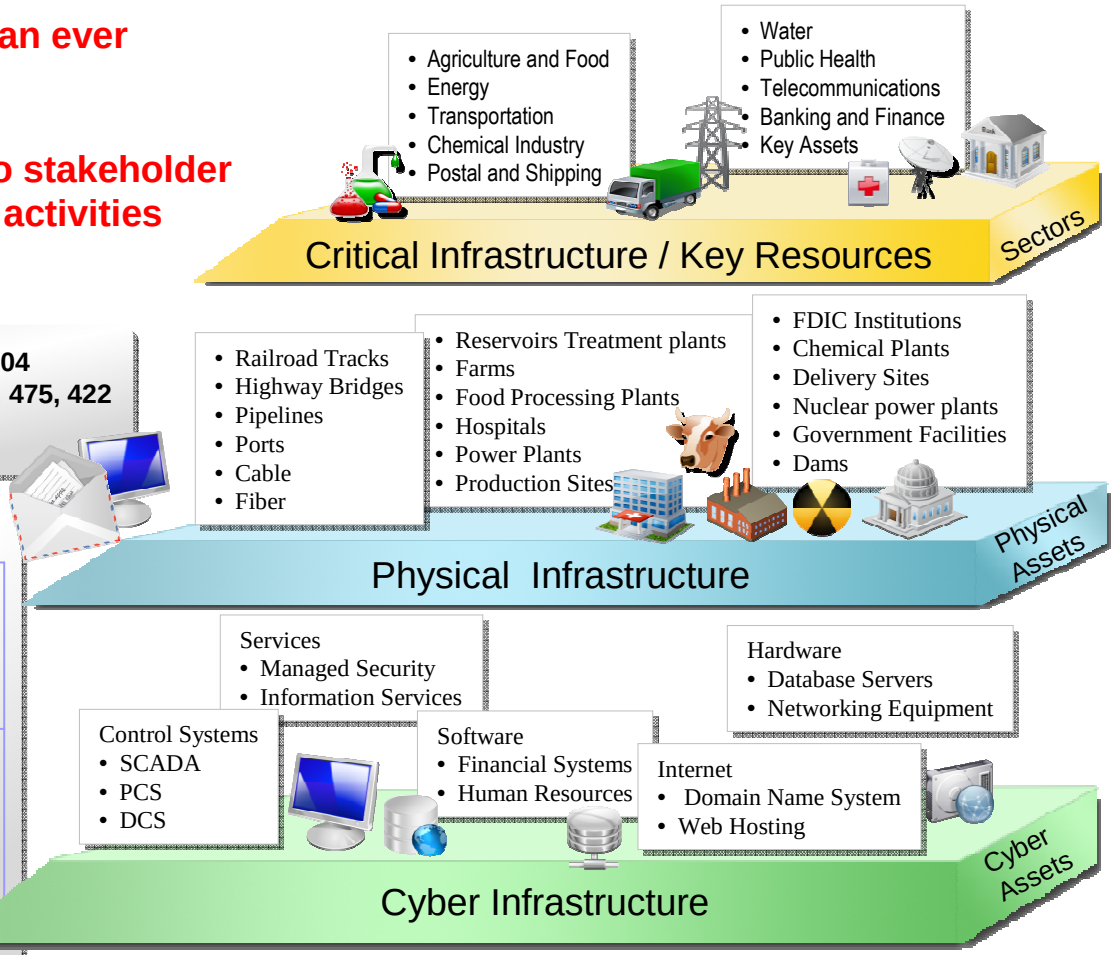
-- Possibility of disruption is greater than ever because software is vulnerable

--- Loss of confidence alone can lead to stakeholder actions that disrupt critical business activities

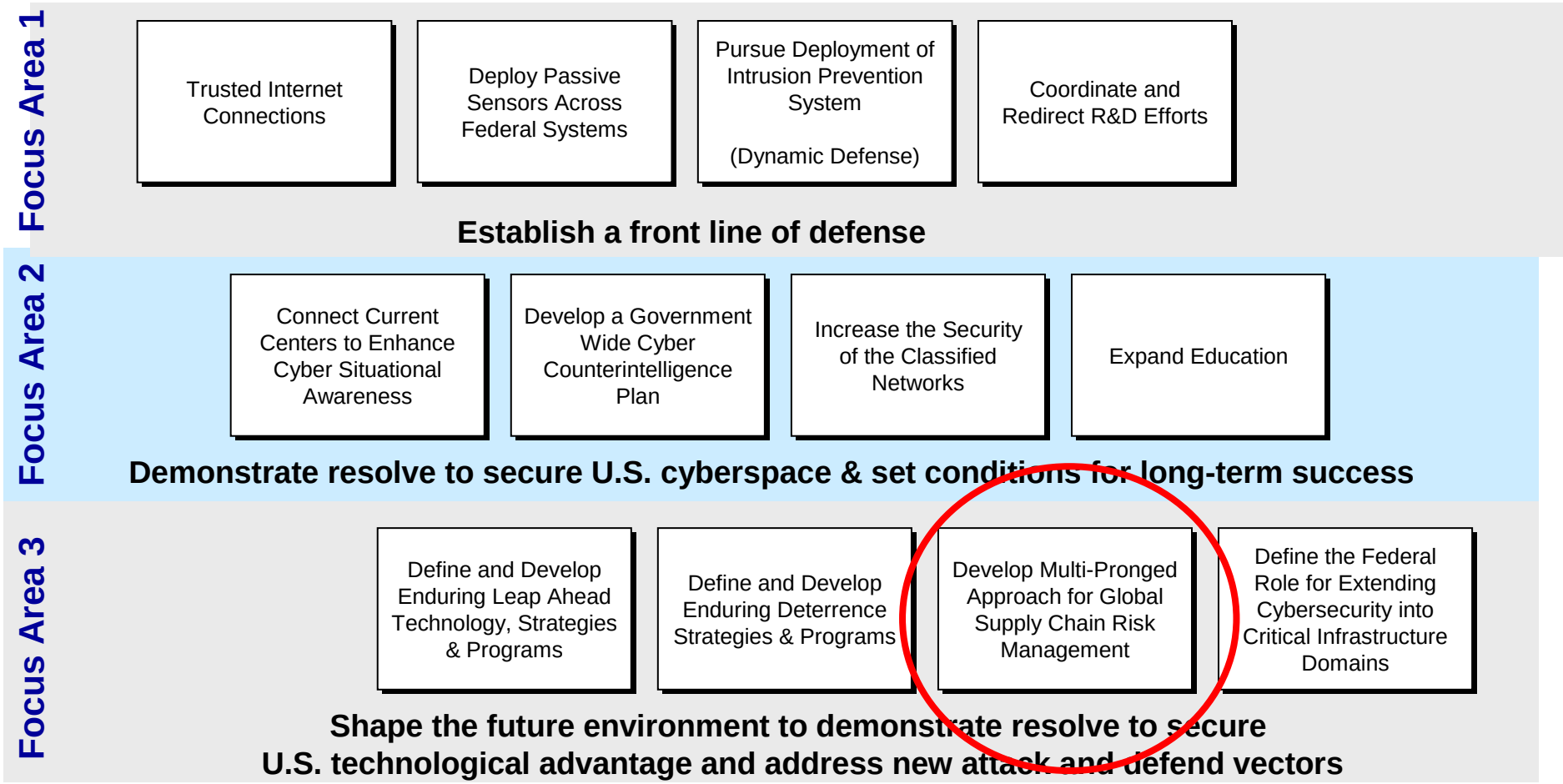
Internet users in the world: 1,766,727,004
E-mail messages sent today: 215, 674, 475, 422
Blog Posts Today: 458, 972
Google searches Today: 2,302,204,936

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

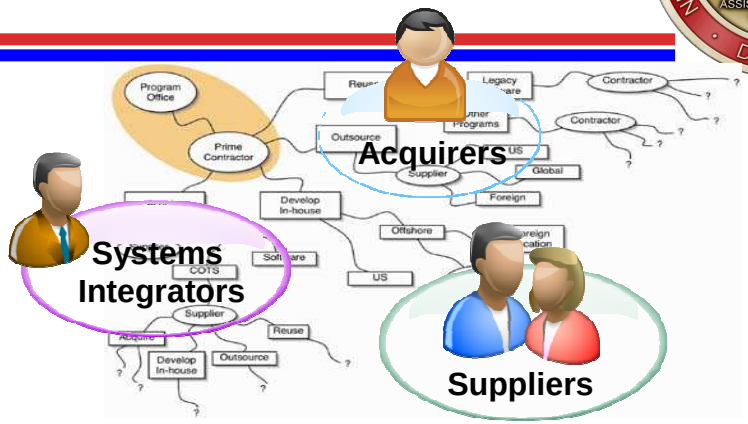
** Source – 2009 Verizon Data Breach Investigations Report*



Comprehensive National Cybersecurity Initiative (CNCI)



Systems Assurance
TRADESPACE



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.

Unique Requirements

Higher COST can buy Risk Reduction

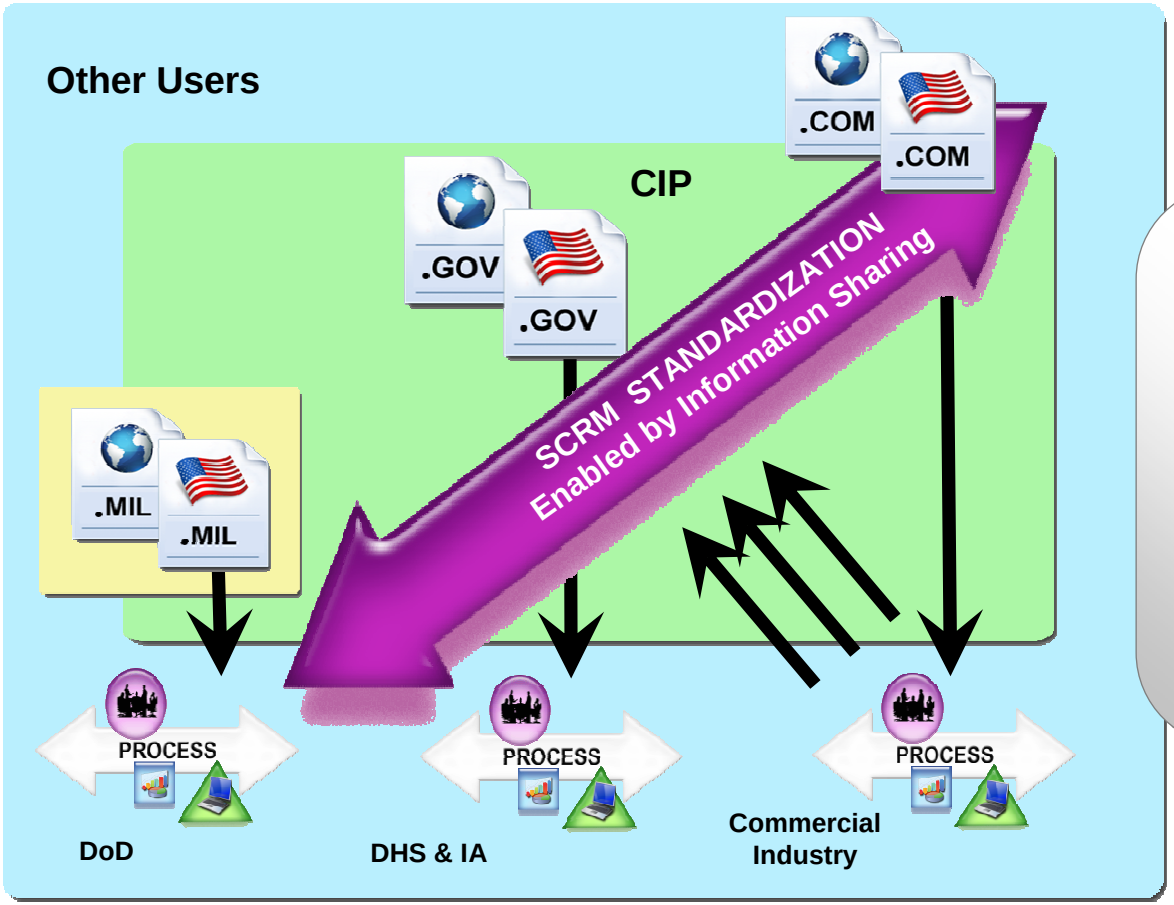
COTS products

Slippery Slope / Unmeasurable Reqts

Lower Cost usually means Higher RISK

SCRM Stakeholders

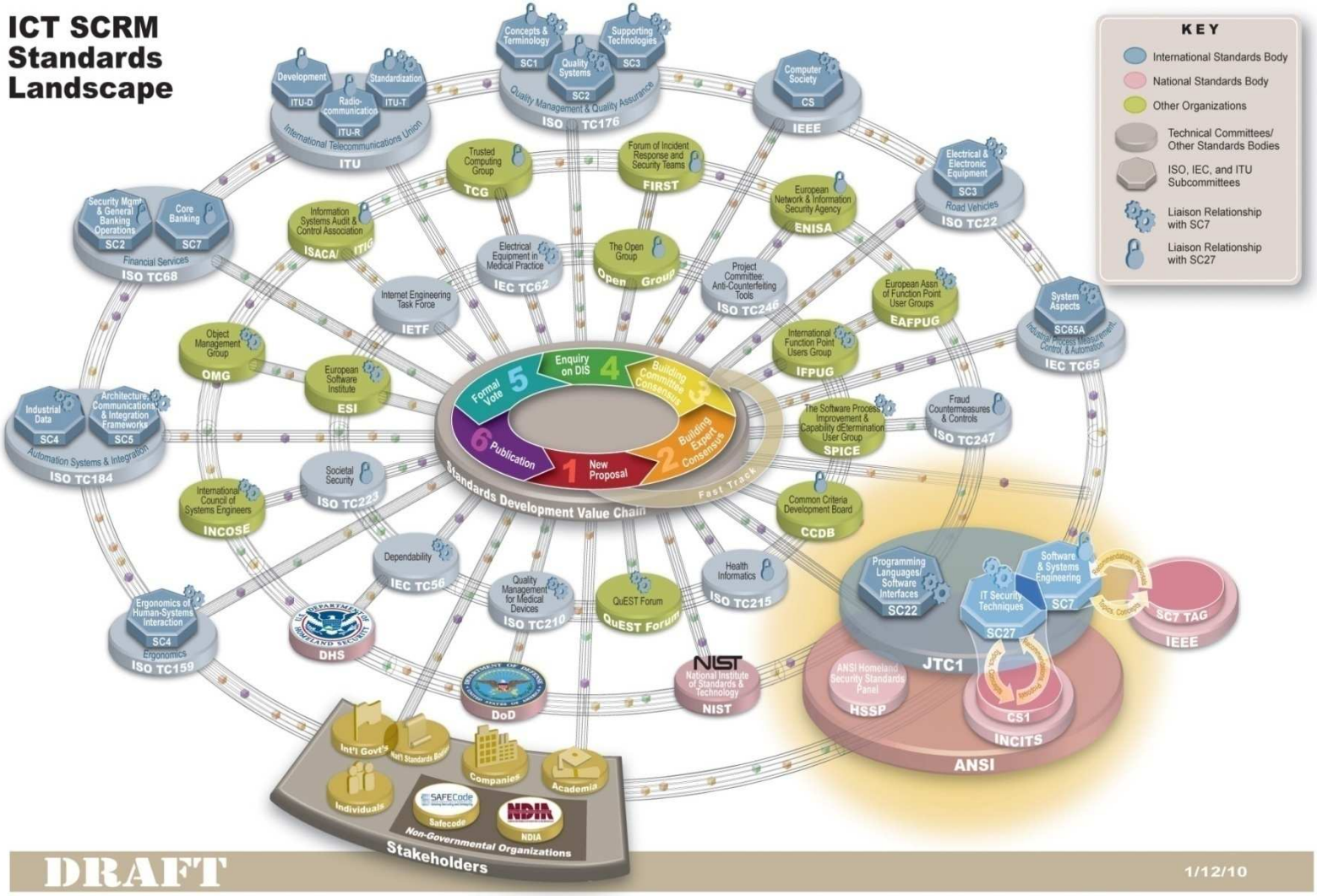
US (CNCI) has vital interest in the global supply chain.



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

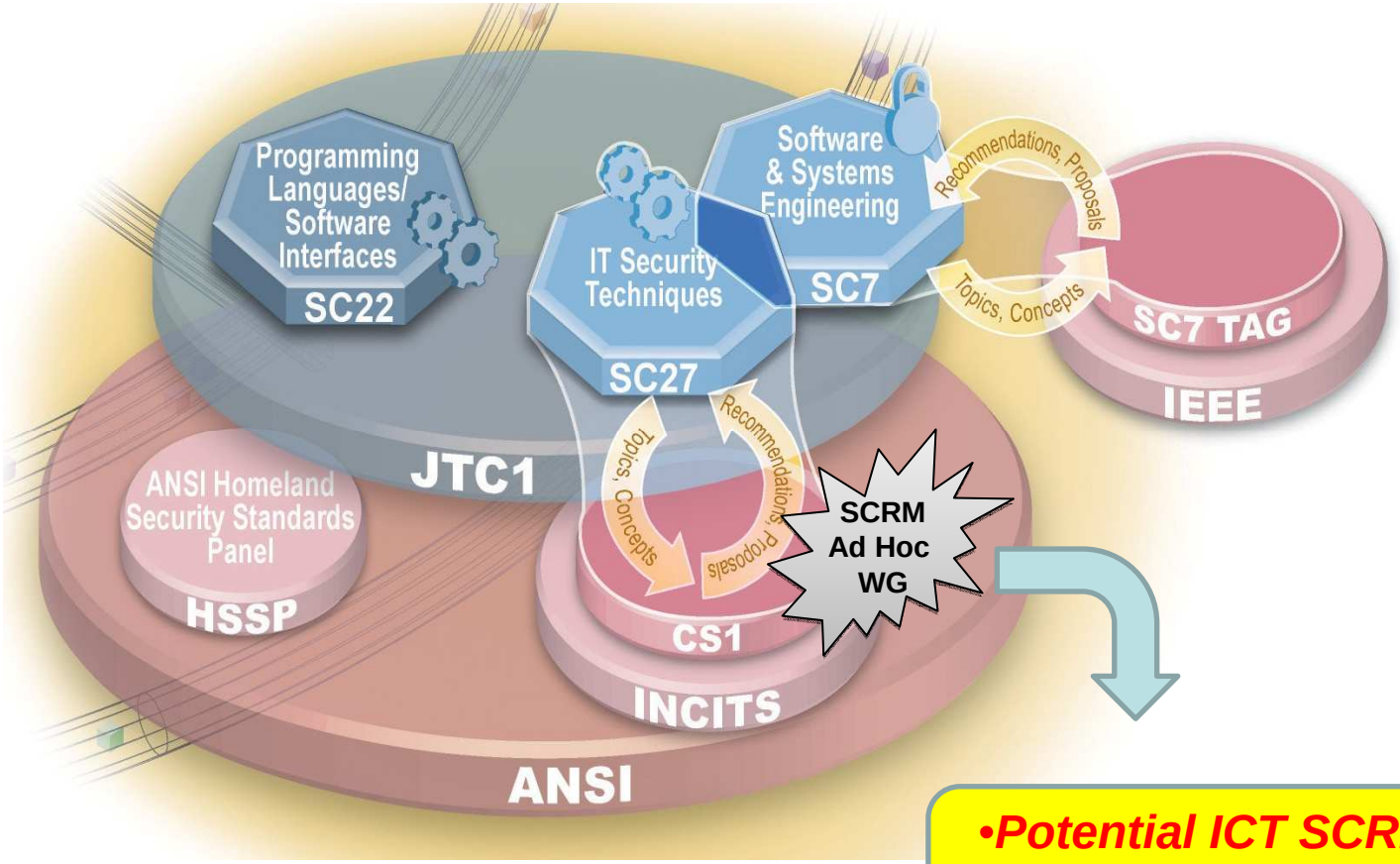
SCRM Standardization Requires Public-Private Collaborative Effort

Standards Development Organizations SDOs Landscape: an SCRM Perspective



SCRM Study Periods:

Nov'09 – Apr'10 / May-Oct'10



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