Supply Chain Risk Management (SCRM)
~OVERVIEW~

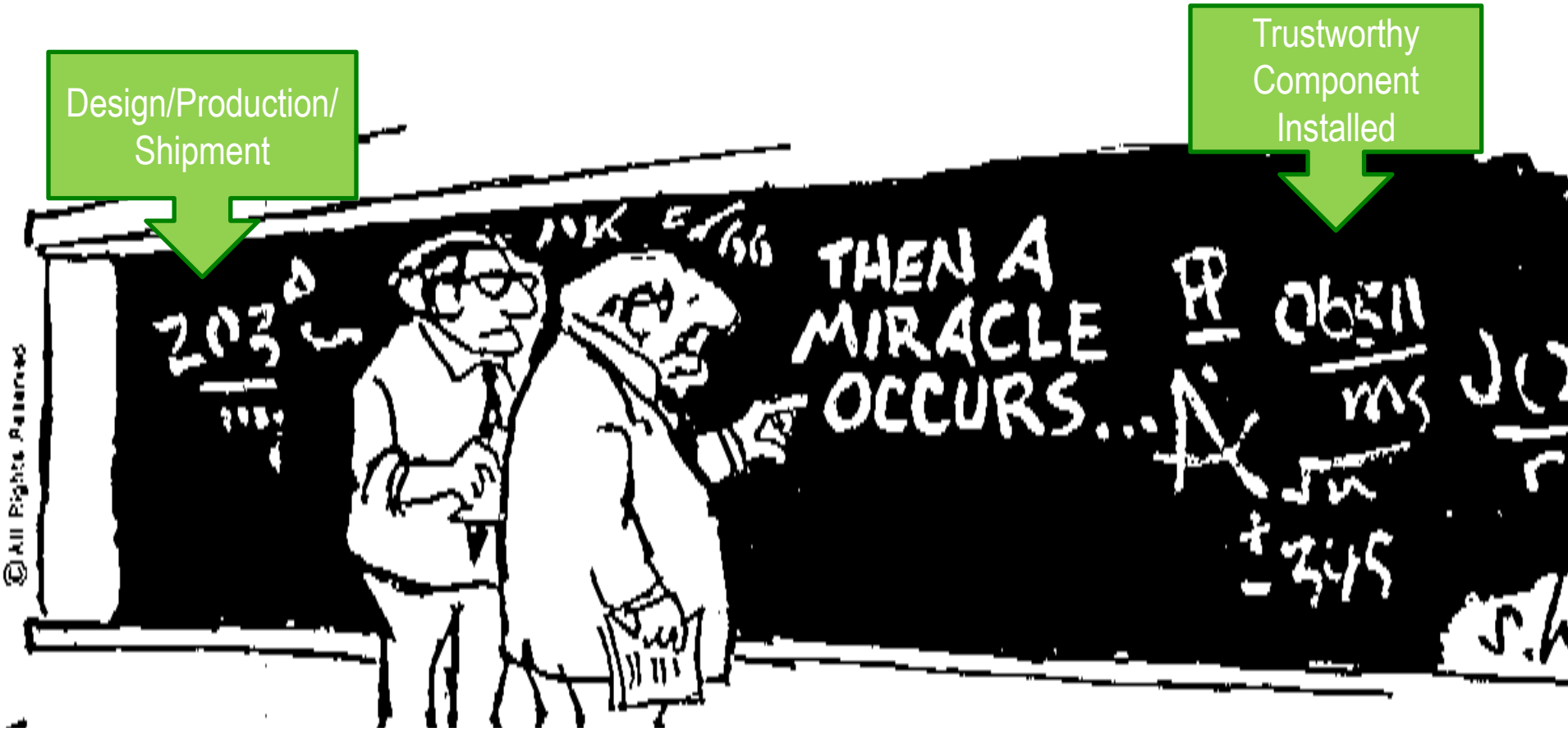
AFCEA C4ISR - SCRM PANEL
Apr 26 2016

Grant Merkel
SPAWARSYSCOM/SSC Pacific
~Operations Security Manager
~Research & Technology Protection (RTP) Manager
~Supply Chain Risk Management (SCRM) Lead
Ph. (619) 553-2800/DSN 553
grant.merkel@navy.mil

Agenda

- Supply Chain Risk Management (SCRM) Policy Overview
- SCRM/Trusted Systems & Networks (TSN)
- SCRM Risk Overview
- Impacts to DON
- Impacts to Government contractors
- SPAWAR SCRM Efforts
- SSC PAC SBO Information

Global Supply Chain?



"I think you should be more explicit here in step two"

SCRM Policy Overview

- SCRM is a relatively new effort within the DoD, but has Congressional, OSD, SECNAV, CNO high-vis attention
- Current policy requirements are directed toward Programs of Record and government contractors
- National Defense Authorization Act (NDAA Fy11, 12 &13) contain SCRM requirements for DoD with a focus on DoD contractors
- Recent SCRM language added to DFARS (begins implementation of NDAA's)
- DoD has issued only one policy specific to SCRM (DODI 5200.44), a couple Memorandums, but GAO, NIST and SECNAV have all issued additional guidance and requirements
- SECNAVINST 4855.20, Counterfeit Materiel Prevention Policy

SCRM Key Terms

▼ Supply Chain Risk:

- The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a national security system (as that term is defined at 44 U.S.C. 3542(b)) so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system. (source: FY2011 NDAA Section 806)
  **Note: Yes, this risk is inherent to the global supply chain*

▼ Supply Chain Risk MANAGEMENT:

- A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats throughout DoD's "supply chain" and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal). (Source: DoDI 5200.44)

  **Note: similar processes are used in DLA, NSA and other U.S. Government and Private entities*

SCRM Process in DON

▼ Criticality Analysis/Critical Function Analysis

- An end-to-end functional decomposition performed by Systems Engineers, Operations, Logistics, and other program personnel to identify mission critical functions and components. Includes identification of system missions, decomposition into the functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions. Criticality is assessed in terms of the impact of function or component failure on the ability of the component to complete the system missions(s).

▼ Mission Critical Functions

- Any function, the compromise of which would degrade the system effectiveness in achieving the core mission for which it was designed.*

*Source: DODI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

SCRM Risk Overview

▼What's the Risk?

- Supply Chain 'Risk" perspective is risk ***from*** the supply chain, vice risk ***to*** the supply chain.
- Risk is always based on Threat × Vulnerability. In the case of the (global) supply chain, it's the risk that an adversary (threat) will compromise a component or system *via* the supply chain.
  - A threat may exploit a vulnerability in the supply chain to:
    - Maliciously introduce unwanted function, directly sabotage, subvert the design, integrity, production, or operation of a component
    - Be able (through the above actions) to deny, disrupt, surveil, or degrade the functions, intended use, or operations of the component.
- Risk to a program (cost/schedule/performance), to IA/CYBER (Confidentiality/Integrity/Availability), to the military mission.
- Costs associated with the realization of these risks can be severe, both financial and up to and including loss of life.

SCRM Implementation Impacts

▼Impacts to DON

- Every program of record (POR) is addressing SCRM, at every MS & FRP/FDD
  - Mitigations or countermeasures may be required, and may impact contract requirements
- Costs associated with SCRM mitigations may be significant
  - New/unforseen costs of component replacement
  - Accelerated tech refresh
  - Change of supplier(s)
  - Supplier diversification
  - Alternative purchase methods
  - Use of Trusted Foundry

SCRM Implementation Impacts

Impacts to Government contractors

- Will need to integrate SCRM into operations/business processes if Information and Communications Technology (ICT) products or services are provided.
- Will need to meet SCRM requirements placed on a contract solicitation in order to win award (i.e. do not expect a waiver, even for small business).
- May develop organic capabilities, or partner with new or different contract companies, or in ways not previously considered.
- Will need to understand the costs (financial liability) for providing a component that does not meet the contract requirements for SCRM.
- Will need to ensure that subcontractors, distributors, re-sellers used to source components may need additional scrutiny related to SCRM before and after their selection.
- May be able, through one or more of the above, to develop a competitive advantage related to contracts with SCRM requirements.

SPAWAR SCRM efforts

SPAWAR HQ SCRM WG

- Developed model for PORs to use to address SCRM requirements
- Working with other IPT's to develop SCRM processes for SPAWAR enterprise
- Draft SPAWARINST for SCRM/TSN
- Draft Wiki page for SCRM efforts

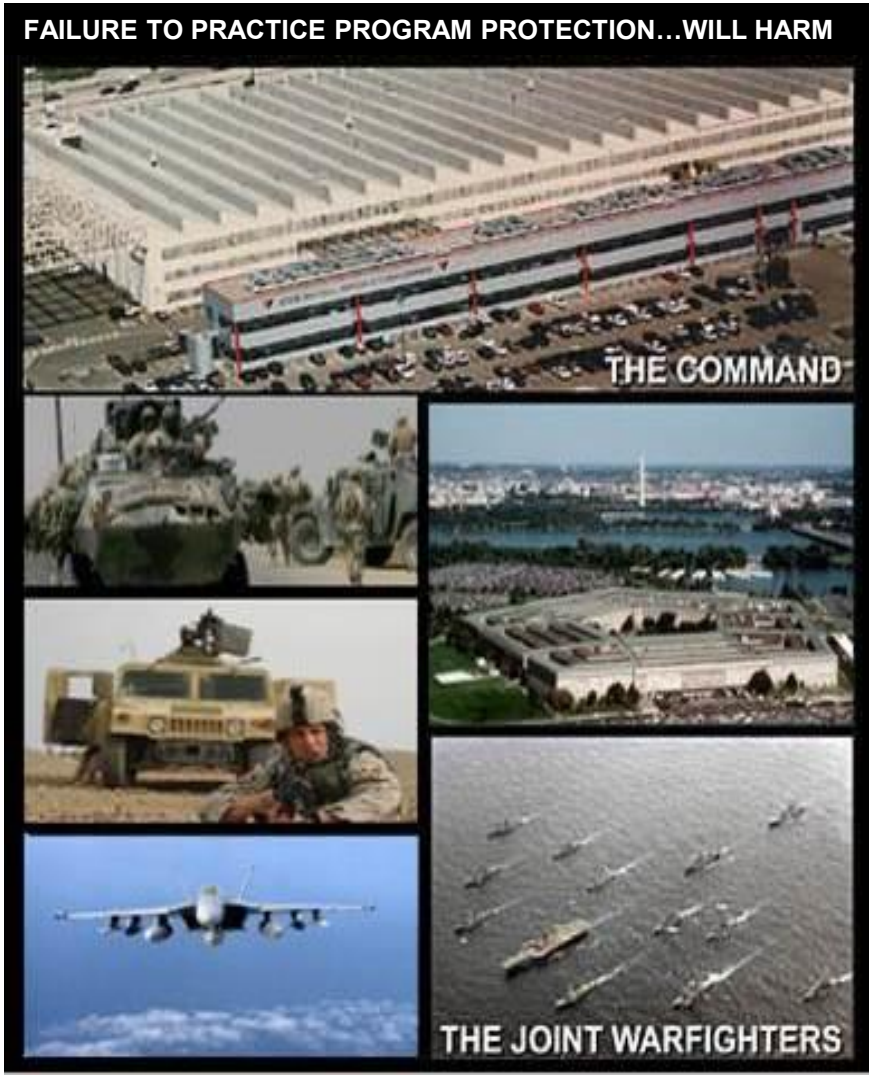
SPAWAR HQ and SSC PAC Contracts IPTs

- Focused on developing and integrating standardized SCRM requirements and practices into all ICT related procurements

SSC PAC SCRM IPT

- Focused on developing procedures to holistically integrate SCRM by addressing prevention, detection, mitigation and reporting.

Summary



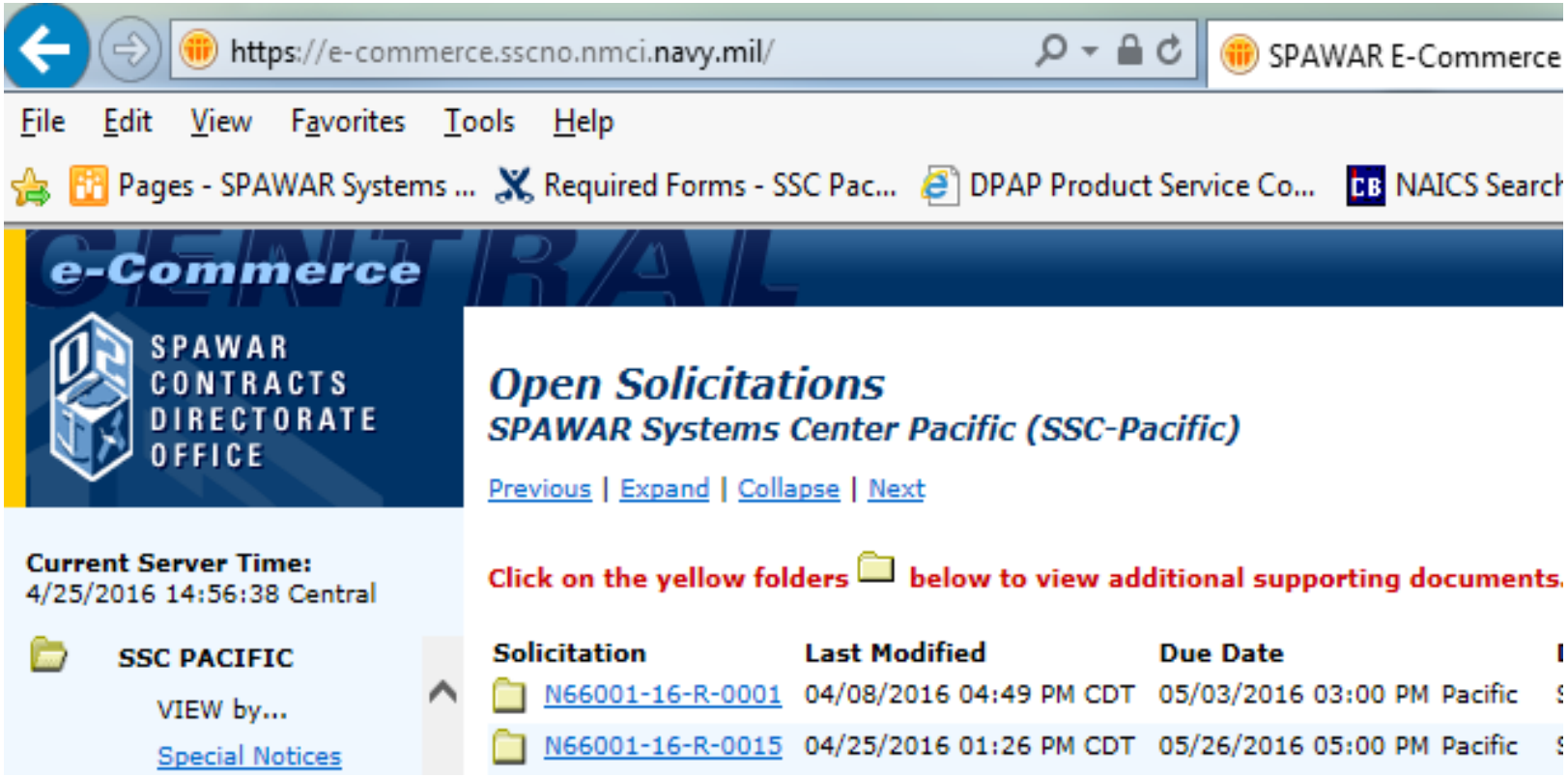
- Contractors and government sponsors will need to meet new requirements, now and in the future.
- Supply Chain Risk Management is necessary for DON programs –not just per policy, but because the threat is real.
- Failure to protect our technologies and capabilities at either contractor or government facilities will compromise them and will harm National Security.

Do not allow for the compromise of *tomorrows* capabilities *today*!

Small Business Office Information

E-Commerce / FBO opportunities

- LARGE CONTRACTS -
- E-commerce/Open Solicitations:



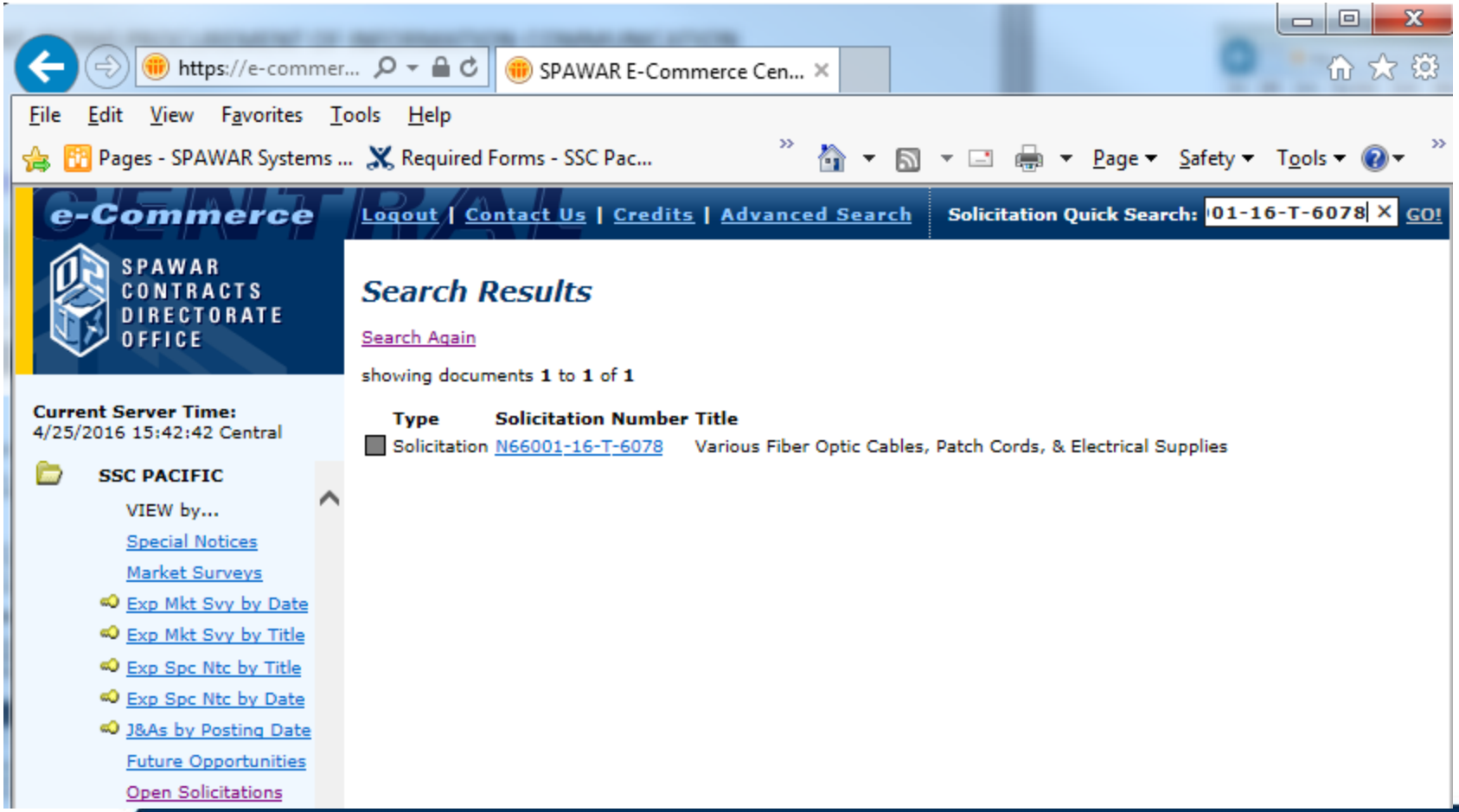
SCRM Clauses – Large Contracts

N66001-16-R-0001 and N66001-16-R-0015:

- 252.239-7017 Notice of Supply Chain Risk NOV 2013
- 252.239-7018 Supply Chain Risk OCT 2015
- 52.212-2 EVALUATION--COMMERCIAL ITEMS (OCT 2014)

E-Commerce / FBO opportunities

- Simplified Acquisition Procedures (SAP)-
- E-commerce/Open Solicitations:



QUESTIONS, ANSWERS & DISCUSSION SESSION

BACK-UPS

Direct or Related SCRM Policies

SCRM/TSN Existing Policies

- IA TA Trusted Systems and Networks (TSN) Standard (published as part of the Defense-in-Depth 62 Functional Implementation Architecture (DFIA) Standard)
- DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), of 4 Nov 12
- DoD Instruction 5200.39, Critical Program Information (CPI) Protection Within the Department of Defense, July 16, 2008
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23, “Cybersecurity Policy,” January 8, 2008
- SCRM Program Office, Trusted Mission Systems and Networks Directorate, “Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11 – Supply Chain Risk Management Pilot Program,” February 25, 2010

Direct or Related SCRM Policies

▼ SCRM/TSN Existing Policies (Cont.)

- DoDI 4140.67, DOD Counterfeit Prevention Policy, 26 Apr 2013
- NISTIR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems, of Oct 12
- NIST Special Publication 800-161, Second Public Draft, Supply Chain Risk Management Practices for Federal Information Systems and Organizations
- NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, of Apr 13
- NIST Special Publication 800-30 Revision 1, Guide for Conducting Information Security Risk Assessments, of Sep 12
- Committee on National Security Systems Instruction (CNSSI) No. 1253, Security Categorization and Control Selection for National Security System, of 27 Mar 14
- Committee on National Security Systems Directive (CNSSD) No. 505, Supply Chain Risk Management (SCRM),of 7 Mar 12