Making Smart Decisions about Global Supply Chain Security in the Age of Globalization

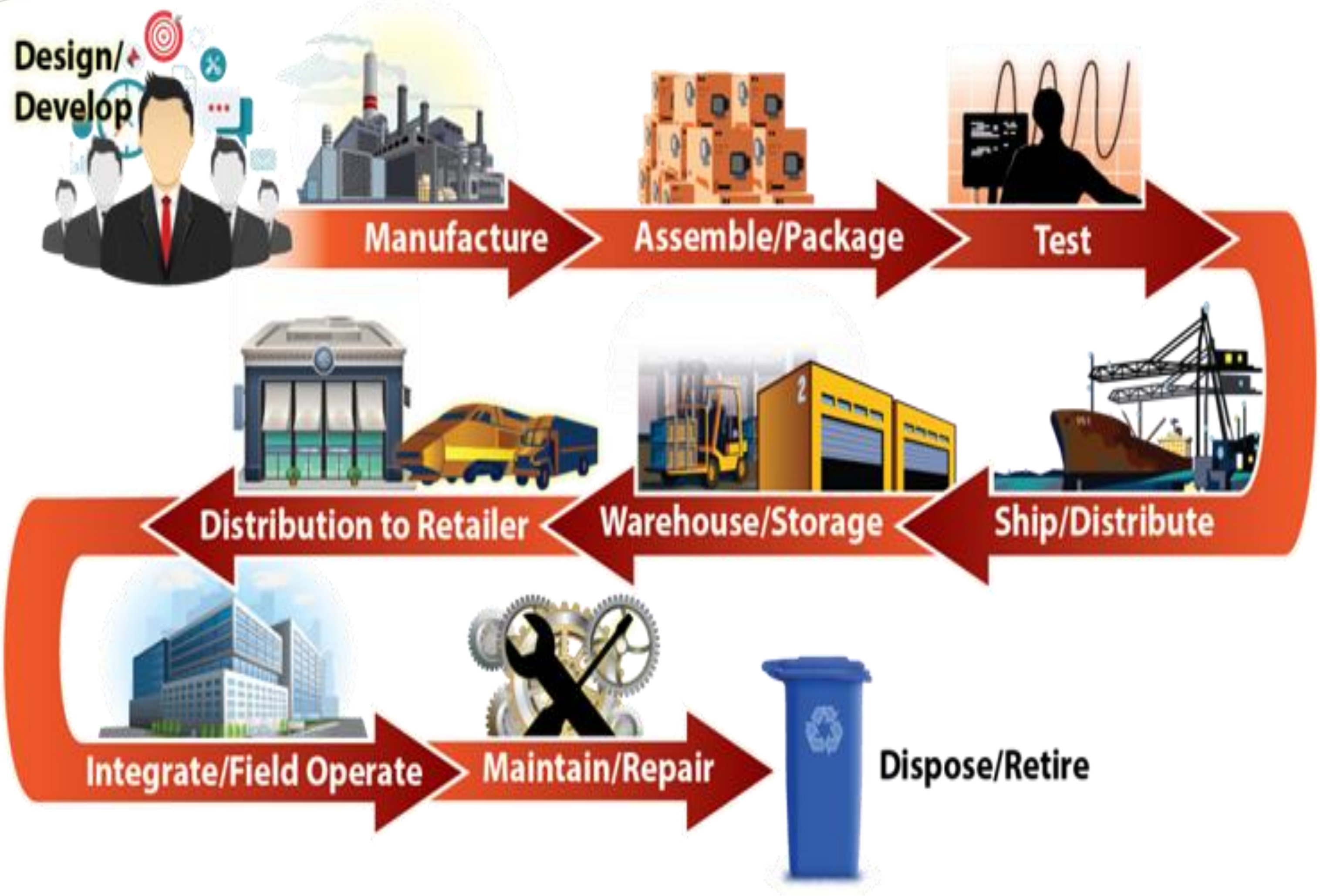
Elizabeth A. McDaniel, IDA

Michelle G. Albert, IDA

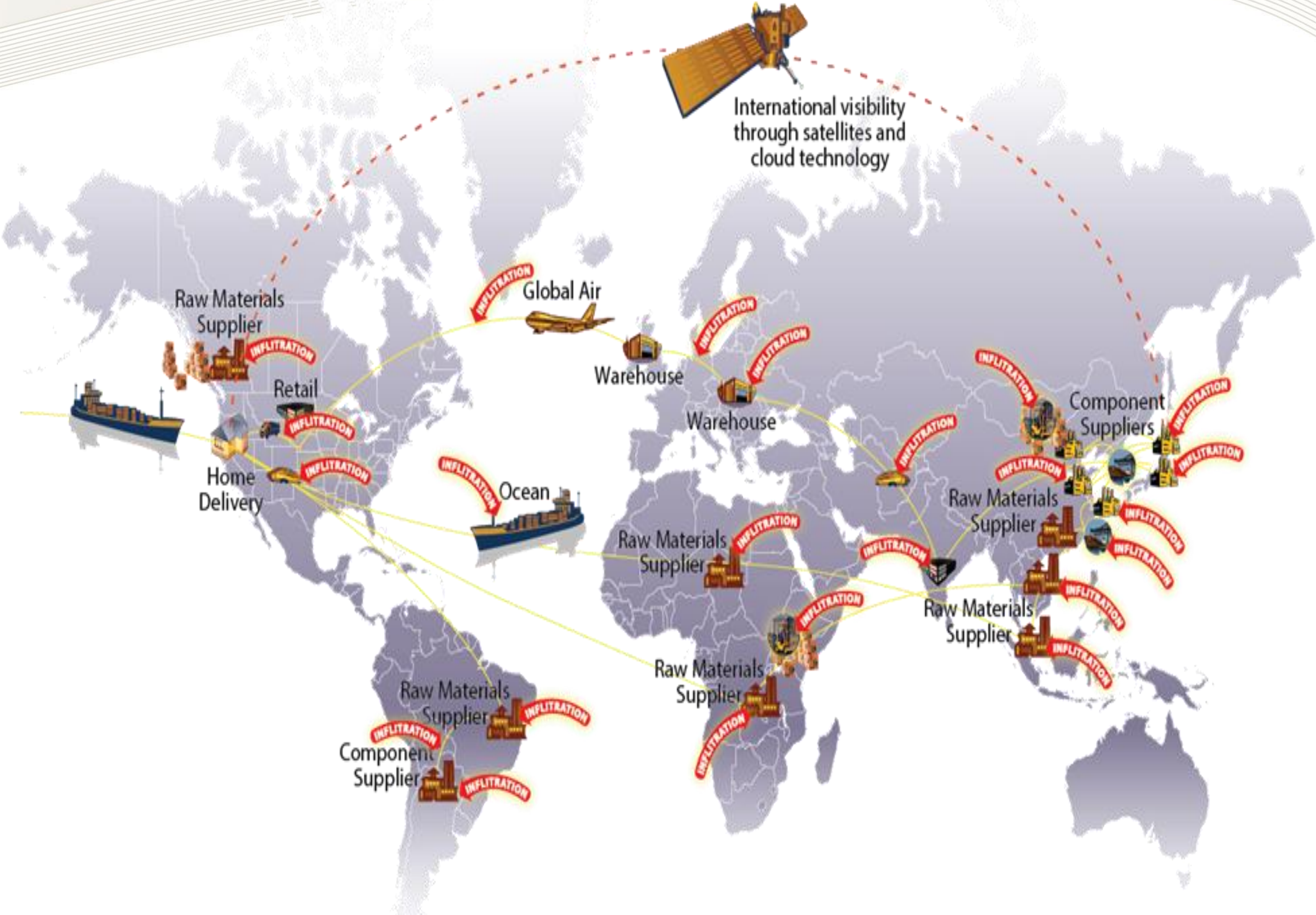
Brian S. Cohen, IDA

Catherine Ortiz, Defined Business Solutions, LLC

The Supply Chain



A Notional Global Supply Chain



Terminology

- *Supply chain security* refers to the security and integrity of a component as it travels along its supply chain.

- *Supply chain risk management*, historically considered a logistics-based discipline, focuses on the movement of the component through its supply chain and threats to this movement. DoD applies the term in acquisition to refer to the threat of malicious actors who seek to intervene in the supply chain to impair the security of DoD systems and missions.

Education, Training, Awareness, plus Guidance

Awareness seeks to focus attention on a topic by presenting facts and issues in a manner meant to generate interest and desire for further learning and to shift thinking or level of concern.

Training is functional and is focused on the “how to” aspect, is designed to change behavior by developing specific skills or behaviors.

Education is conceptual, strategic, and future-focused. It seeks to enhance critical and creative thinking and to develop depth and breadth of understanding of principles, concepts, and ideas, and their application in novel situations.

Guidance evolves from engagement of experts, researchers, and practitioners who share, refine, and disseminate standards and best practices.

ICT Global Supply Chain Risk Management Awareness Module

IDA published an awareness module in 2014 on DVD that contains:

- A video
- A narrative
- A set of slides designed to be modified by users
- A comprehensive list of references
- A repository of all cited documents, policies, and directives

Three Themes:

1. The New Insider Threat is Not a Person – It is ICT
2. Supply Chain Risk is a Condition to be Managed, not a Problem to be Solved
3. Take Action to Manage Supply Chain Risk

Current Guidance for Global Supply Chain Security

DoD Instructions, Directives, and Regulations

- DoDI 5200.39 Critical Program Information Protection within Research, Development, Test, and Evaluation
- DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks
- DoDI 5000.02 Operation of the Defense Acquisition System (PPP process)
- DoDI 8500.01 Cybersecurity
- DoDI 8510.01 Risk Management Framework for DoD Information Technology
- DoD Program Managers Guidebook for Integrating the Cybersecurity Risk Management Framework into the System Development Life Cycle
- DoDI 5000.02 Operation of the Defense Acquisition System

National Institute of Standards and Technology (NIST) Standards

- Framework for Improving Critical Infrastructure Cybersecurity (aka The Cybersecurity Framework)
- NIST SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations

Activities Described in Interviews with Representatives of 28 Organizations in 2017

Education – a few institutions offer lessons on supply chain security, and fewer offer courses that address supply chain security more comprehensively

Training and Awareness efforts appear to be:

- more awareness than training
- generic, but moving toward more role-based
- suggesting general best practices, standards, and requirements
- increasingly delivering content in small segments, via video and online lessons

Guidance activities in the form of:

- forums and roundtables
- standards and requirements – development and dissemination
- consulting with and for private sector organizations
- tools and risk maturity assessments
- best practices and advocacy
- certifications
- research

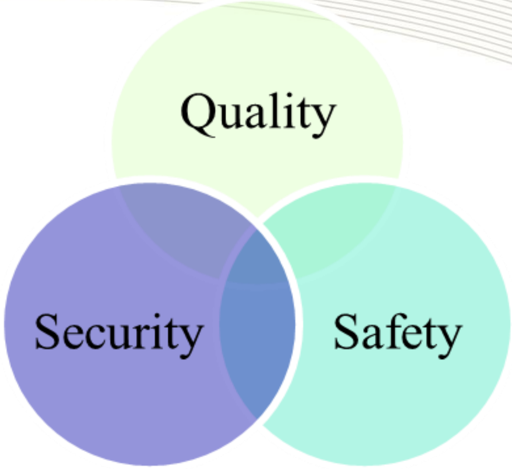
IDA | Trustworthy Supplier Framework (TSF)

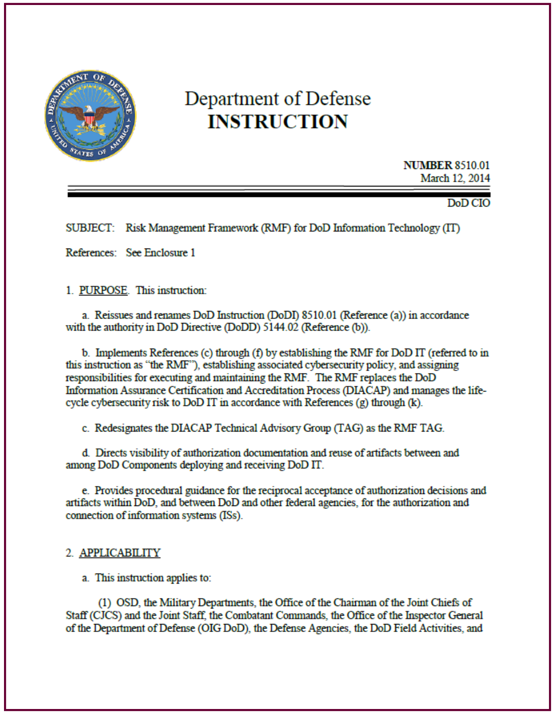
- Based on NIST SP 800-161 as foundational organization of supply chain vulnerabilities

- Intended to help DoD buyers assess risks when purchasing electronic components outside traditional defense base
  - Tool to help DoD buyers select appropriate supply chain risk mitigations when buying standard products
  - Focuses on actions a buyer can take to increase confidence in a supplier's trustworthiness

- Provides a way for a DoD electronics component buyer to organize the landscape of existing standards and practices that mitigate supply chain risks . . .
  - *Then allows the buyer to compare the mitigations and select those that best fit their program's risk and cost profiles*

- Clarifies selection criteria / requirements for vendors who wish to make offers





Department of Defense
INSTRUCTION

NUMBER 8510.01
March 12, 2014

DoD CIO

SUBJECT: Risk Management Framework (RMF) for DoD Information Technology (IT)

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues and renames DoD Instruction (DoDI) 8510.01 (Reference (a)) in accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (b)).

b. Implements References (c) through (f) by establishing the RMF for DoD IT (referred to in this instruction as "the RMF"), establishing associated cybersecurity policy, and assigning responsibilities for executing and maintaining the RMF. The RMF replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) and manages the life-cycle cybersecurity risk to DoD IT in accordance with References (g) through (k).

c. Redesignates the DIACAP Technical Advisory Group (TAG) as the RMF TAG.

d. Directs visibility of authorization documentation and reuse of artifacts between and among DoD Components deploying and receiving DoD IT.

e. Provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other federal agencies, for the authorization and connection of information systems (ISs).

2. APPLICABILITY

a. This instruction applies to:

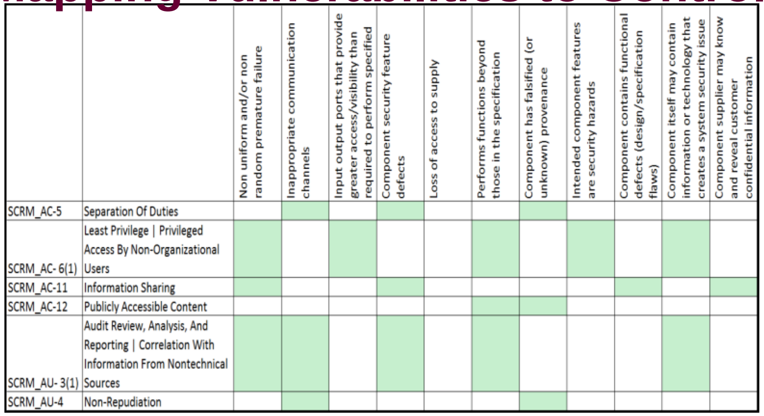
(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (OIG DoD), the Defense Agencies, the DoD Field Activities, and

Elements and Processes of TSF

Some Vulnerabilities

- Non uniform and/or non random premature failure
- Inappropriate communication channels
- Input output ports that provide greater access/visibility than required to perform specified functions
- Component security feature defects
- Loss of access to supply
- Performs functions beyond those in the specification
- Component has falsified (or unknown) provenance
- Intended component features are security hazards
- Component contains functional defects (design/specification flaws)
- Component itself may contain information or technology that creates a system security issue
- Component supplier may know and reveal customer confidential information

Mapping Vulnerabilities to Controls



		Non uniform and/or non random premature failure	Inappropriate communication channels	Input output ports that provide greater access/visibility than required to perform specified	Component security feature defects	Loss of access to supply	Performs functions beyond those in the specification	Component has falsified (or unknown) provenance	Intended component features are security hazards	Component contains functional defects (design/specification flaws)	Component itself may contain information or technology that creates a system security issue	Component supplier may know and reveal customer confidential information
SCRM_AC-5	Separation Of Duties		🟩		🟩			🟩				
SCRM_AC- 6(1)	Least Privilege | Privileged Access By Non-Organizational Users	🟩		🟩			🟩		🟩		🟩	
SCRM_AC-11	Information Sharing	🟩			🟩					🟩		🟩
SCRM_AC-12	Publicly Accessible Content						🟩	🟩				
SCRM_AU- 3(1)	Audit Review, Analysis, And Reporting | Correlation With Information From Nontechnical Sources	🟩	🟩		🟩		🟩				🟩	
SCRM_AU-4	Non-Repudiation		🟩					🟩				

Standards, Practices, Regulations

- *DMEA Trusted Suppliers*
- *DLA Qualified Suppliers List for Distributors (QSLD)*
- *QTSL Program (Qualified Testing Suppliers List)*
- *DLA Qualified Manufacturers List (QML)*
- *DLA Qualified Products List (QPL)*
- *NASA/JPL Approved Supplier List*
- *MDA Distributor Qualification Program*
- *ISO 9000*
- *NISTIR-7622*
- *Open Group O-TTPS*
- *ISO/IEC 27036*
- *SAE/G19 – AS5553, AS6171(Draft), AS6174, AS6496, ARP 6178*
- *IDEA 1010*
- *NDAA 2015 818c*
- *Section 2319 of Title 10*
- *FAR Subpart 9.2*
- *NIST SP 800-161, SP 800-53 R4 - This was identified as a foundation for the Framework*

Value

The Framework helps the Buyer articulate security requirements and translate them to controls and actionable implementations, and helps Vendors make offers related to selection criteria / requirements,

Buyer makes candidate selections of standards and practices to be employed

Buyer evaluates measures of effectiveness and cost for the standards and practices

Buyer chooses standards and practices that will manage the risk