ASSISTANT SECRETARY OF DEFENSE
SUSTAINMENT

Supply Chain Risk Management (SCRM)

Ms. Jan Mulligan

ODASD(Logistics), Director of Supply

May 15, 2019

Agenda

- SCRM Definitions
    - DoDI 4140.01
    - Cyber Security
- SCRM Environment
- SCRM Communities of Practice
- Government SCRM Focus Areas
- ASD(Sustainment) SCRM Studies
- Sample Supply Chain Map
- DoD SCRM Way Forward
- Notional SCRM Governance Model
- What You Can Do
- Questions

SCRM Definition – DoDI 4140.01

DoDI 4140.01, DoD Supply Chain Material Management Policy (03/06/2019)

Supply Chain Risk Management (SCRM) - The process for managing risk by identifying, assessing, and mitigating threats, vulnerabilities, and disruptions to the DoD supply chain from beginning to end to ensure mission effectiveness. Successful SCRM maintains the integrity of products, services, people, and technologies, and ensures the undisrupted flow of product, materiel, information, and finances across the lifecycle of a weapon or support system. **DoD SCRM encompasses all sub-sets of SCRM**, such as cybersecurity, software assurance, obsolescence, counterfeit parts, foreign ownership of sub-tier vendors, and other categories of risk that affect the supply chain.

SCRM Definition – Cyber Security

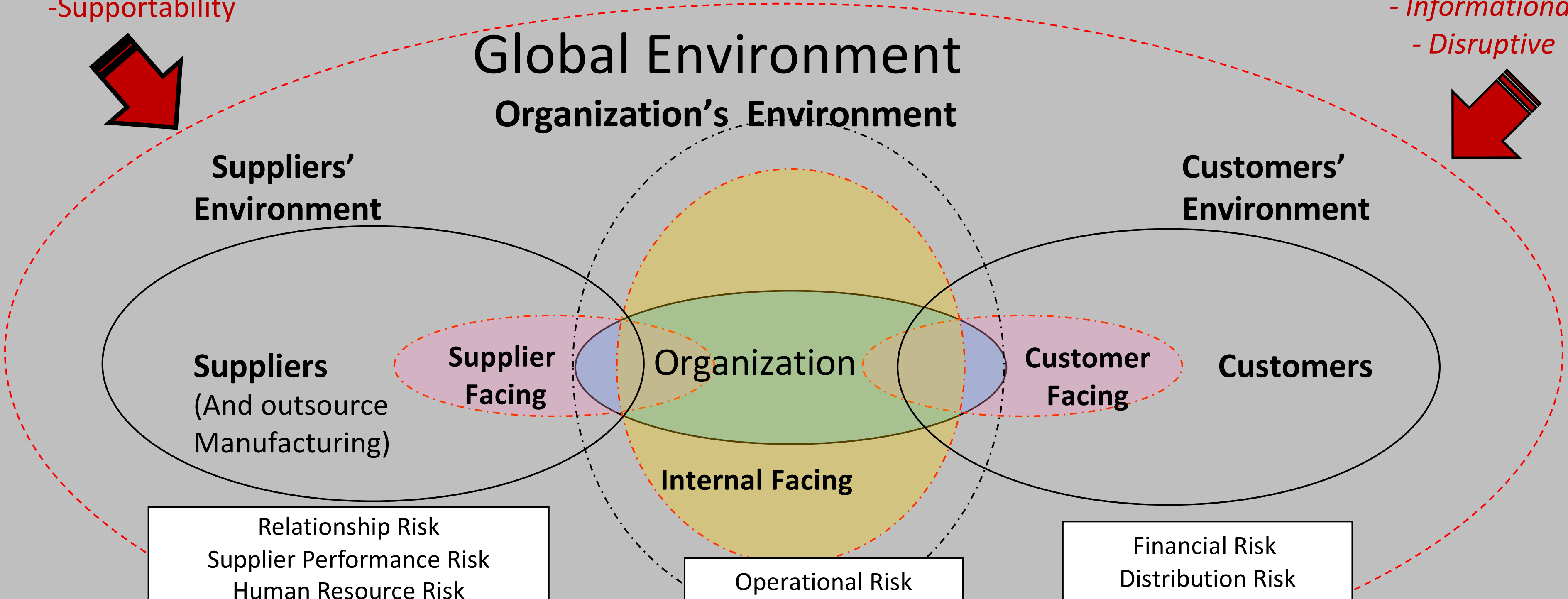
Cyber SCRM Definition – National Institute of Standards and Technology

Cyber Supply Chain Risk Management (C-SCRM) - the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of Information Technology (IT)/Operational Technology (OT) product and service supply chains. It covers the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction) as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any stage.

DoD C-SCRM is Usually Defined as Information and Communication Technology (ICT) Related to National Security Systems (NSS)

SCRM Environment

Comprised of: People, Material, Processes, Software, & Relationships

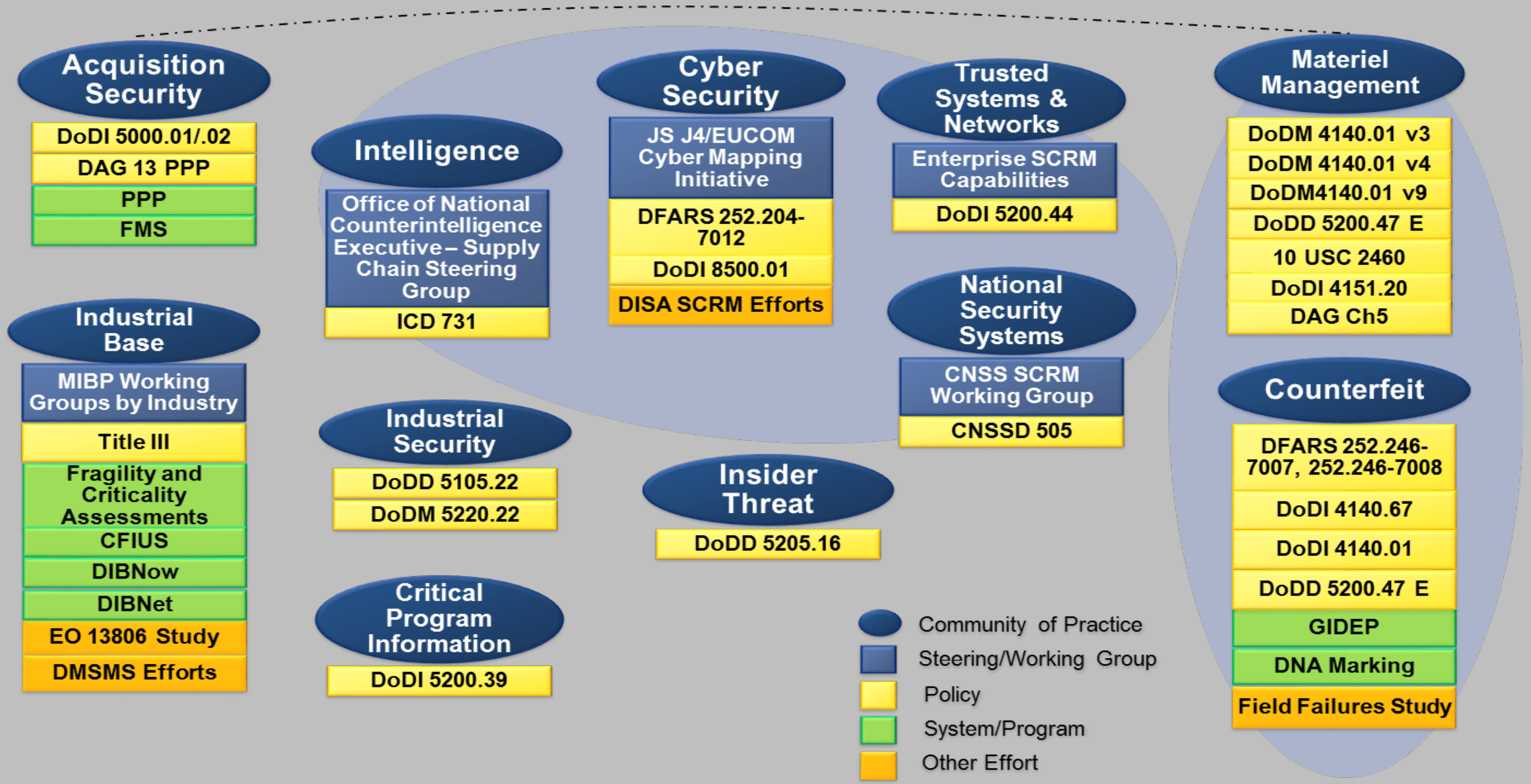


Relationship Risk
Supplier Performance Risk
Human Resource Risk
Supply chain disruption risk
Supplier Environment Risk
Market Dynamics Risk
Disaster Risk
Political / Country Risk
Supplier Financial Risk
Regulatory Risk

Operational Risk
Technical Risk
Financial Risk
Legal / Regulatory Risk
Environmental Risk
HR / Health and Safety Risk
Political/ Country Risk

Financial Risk
Distribution Risk
Relationship Risk
Market Risk
Brand / Reputation Risk
Product Liability Risk
Environmental Risk
Political/ Country Risk

SCRM Communities of Practice



Acquisition Security
- DoDI 5000.01/.02
- DAG 13 PPP
- PPP
- FMS

Industrial Base
- MIBP Working Groups by Industry
- Title III
- Fragility and Criticality Assessments
- CFIUS
- DIBNow
- DIBNet
- EO 13806 Study
- DMSMS Efforts

Intelligence
- Office of National Counterintelligence Executive – Supply Chain Steering Group
- ICD 731

Industrial Security
- DoDD 5105.22
- DoDM 5220.22

Critical Program Information
- DoDI 5200.39

Cyber Security
- JS J4/EUCOM Cyber Mapping Initiative
- DFARS 252.204-7012
- DoDI 8500.01
- DISA SCRM Efforts

Insider Threat
- DoDD 5205.16

Trusted Systems & Networks
- Enterprise SCRM Capabilities
- DoDI 5200.44

National Security Systems
- CNSS SCRM Working Group
- CNSSD 505

Materiel Management
- DoDM 4140.01 v3
- DoDM 4140.01 v4
- DoDM4140.01 v9
- DoDD 5200.47 E
- 10 USC 2460
- DoDI 4151.20
- DAG Ch5

Counterfeit
- DFARS 252.246-7007, 252.246-7008
- DoDI 4140.67
- DoDI 4140.01
- DoDD 5200.47 E
- GIDEP
- DNA Marking
- Field Failures Study

●	Community of Practice
▨	Steering/Working Group
🟨	Policy
🟩	System/Program
🟧	Other Effort

Working Representation of the Many COPs Across DoD SCRM

POC: Ms. Jan Mulligan, ODASD(Logistics), 571-372-5227,
Jan.b.mulligan.civ@mail.mil

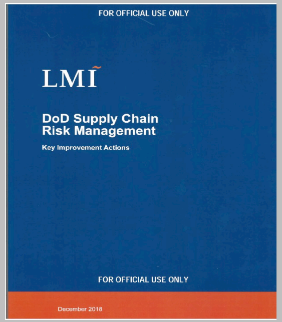
Government SCRM Focus Areas

Document Name	Title	Type	Owner	Applies to	Topic	Applicability to SCRM
NIST-IR 7622	**Notional Supply Chain Risk Management Practices for Federal Information Systems**	**Regulation/Guidance**	**NIST**	**Gov-wide**	**Cybersecurity**	**Cybersecurity controls**
NDAA Section 1639 (2018)	**Measurement of Compliance with Cybersecurity Requirements for Industrial Control Systems**	**NDAA**	**Congress**	**DoD**	**Cybersecurity**	**Cyber scorecard for Industrial Control Systems**
NDAA Section 807 (2018)	**Process for Enhanced Supply Chain Scrutiny**	**NDAA**	**Congress**	**DoD**	**Risk Management**	**Stricter acquisition practices**
NDAA Section 881 (2019) - ***Makes FY11 NDAA Section 806 Permanent***	**Permanent Supply Chain Risk Management Authority**	**NDAA**	**Congress**	**DoD**	**Acquisition/Cyber Risk Management**	**Information Communication Technology Risk to National Security Systems**
DoDI 4140.01	**DoD Supply Chain Materiel Management Policy**	**Instruction**	**USD(AT&L)**	**DoD**	**Materiel Management**	**Materiel management across life cycle**
DODI 5200.44	**Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)**	**Instruction**	**USD(AT&L) CIO**	**DoD**	**TSN**	**Counterfeit/Integrity of Mission Critical Infrastructure**
DoDI 8510.01	**Risk Management Framework (RMF) for DoD Information Technology (IT)**	**Instruction**	**CIO**	**DoD**	**Cybersecurity**	**Cybersecurity platform for DoD, integrating information**
Committee on National Security Systems Directive 505 (CNSSD 505)	**Supply Chain Risk Management**	**Directive**	**CNSS**	**Gov-wide**	**NSS/SCRM**	**Logistics for National Security Systems SCRM sustainment**
OMB Circular A-123	**Management's Responsibility for Enterprise Risk Management and Internal Control**	**Directive**	**OMB**	**Federal**	**Enterprise Risk Management**	**Full Supply Chain Risk Management Application**

POC: Ms. Jan Mulligan, ODASD(Logistics), 571-372-5227,
Jan.b.mulligan.civ@mail.mil

ASD(Sustainment) SCRM Studies

- SCRM Study Phase I - Findings
  - Not organized to address SCRM holistically
  - Lack common definitions
  - Little information sharing
- SCRM Study Phase II - Recommendations
  - Devise a notional governance structure
  - Conduct vendor vetting & info sharing pilot
  - Pilot SCRM process and technology solutions
- Stakeholder feedback, independent studies, and Executive Orders agree with the conclusion that we can do better
- BLUF: We need to identify and address seams/gaps to secure our supply chains in a unified manner



FOR OFFICIAL USE ONLY

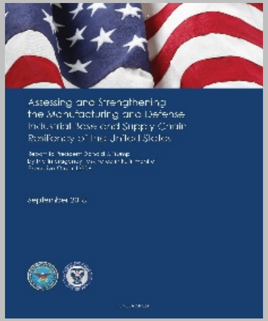
LMI

DoD Supply Chain Risk Management

Key Improvement Actions

FOR OFFICIAL USE ONLY

December 2018

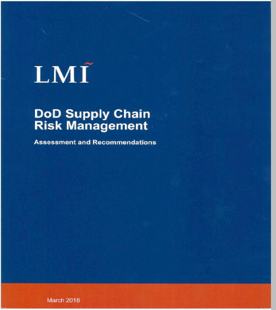


Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States

Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806

September 2018

UNCLASSIFIED

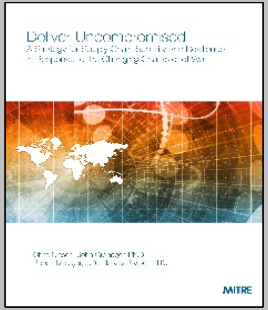


LMI

DoD Supply Chain Risk Management

Assessment and Recommendations

March 2018



Deliver Uncompromised

A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War

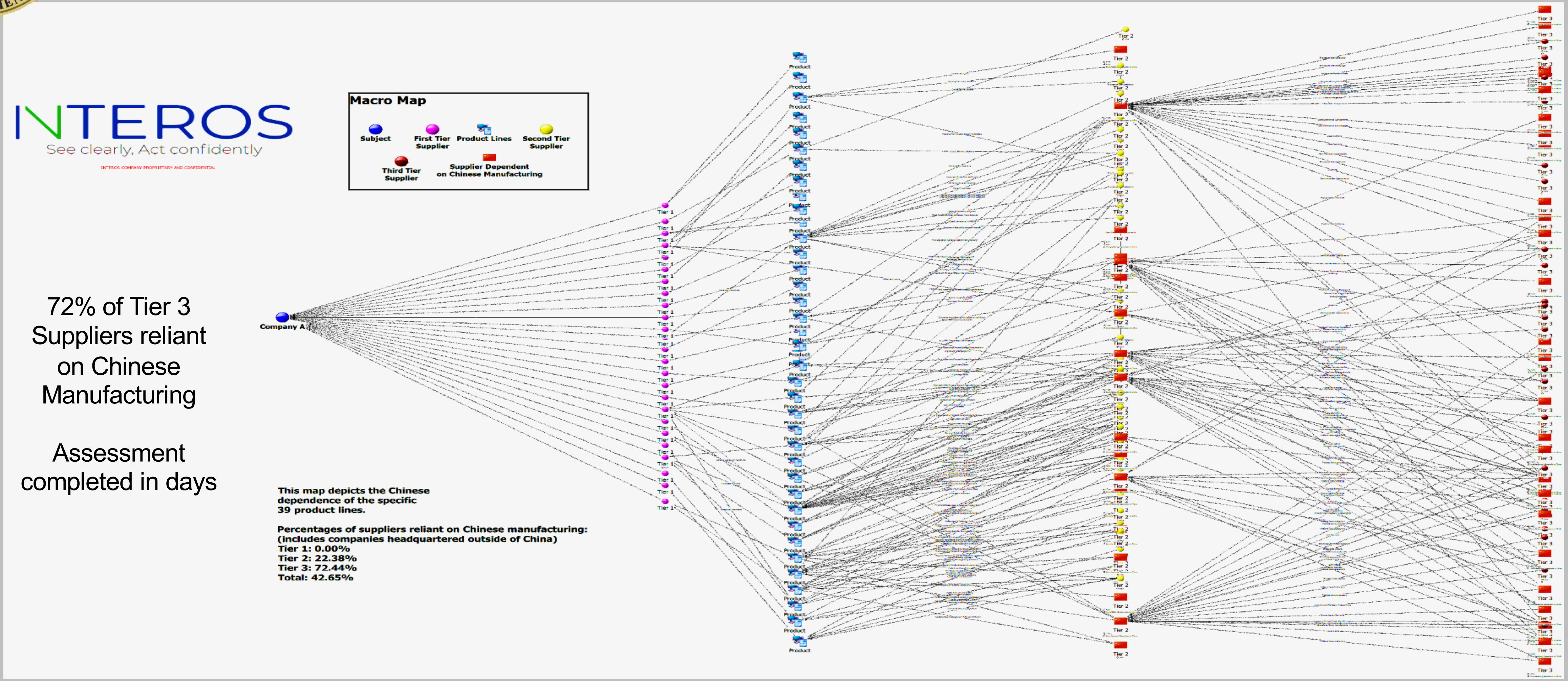
Chris Nissen, John Gronager, Ph.D.

Robert Metzger, J.D., Harvey Rishikof, J.D.

MITRE

POC: Ms. Jan Mulligan, ODASD(Logistics), 571-372-5227,
Jan.b.mulligan.civ@mail.mil

Sample Supply Chain Map



72% of Tier 3 Suppliers reliant on Chinese Manufacturing

Assessment completed in days

This map depicts the Chinese dependence of the specific 39 product lines.

Percentages of suppliers reliant on Chinese manufacturing:
(includes companies headquartered outside of China)
Tier 1: 0.00%
Tier 2: 22.38%
Tier 3: 72.44%
Total: 42.65%

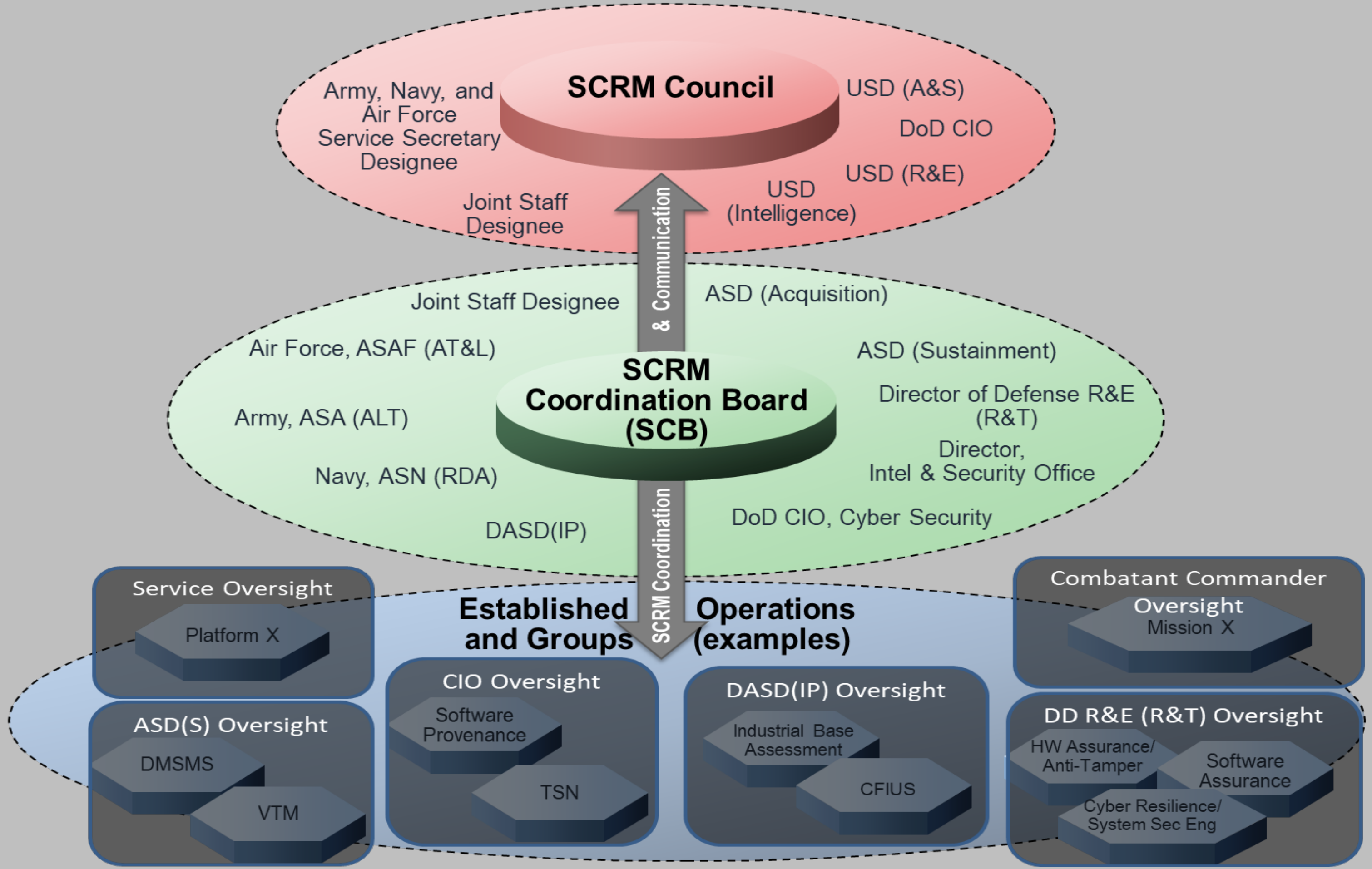
Need to Better Understand Complex Vendor Support Structures

DoD SCRM Way Forward

- Potential Government Actions:
  - Establish our collective vision, goals, and objectives
  - Agree to organizational structures and approaches to SCRM solutions
  - Resource the effort
- Future Objectives:
  - Make SCRM easier for KOs to execute
  - Devise “pre-screening” strategies for vendors
  - Leverage and incentivize industry to protect supply chains
  - Consider process resiliency in addition to system resiliency
  - Look at more than ACAT I systems
  - Develop impact legislation and policy
  - Bridge the threat classification gap to enable SCRM

POC: Ms. Jan Mulligan, ODASD(Logistics), 571-372-5227,
Jan.b.mulligan.civ@mail.mil

Notional DoD SCRM Governance Model



SCRM Council

Army, Navy, and Air Force Service Secretary Designee

Joint Staff Designee

USD (A&S)

DoD CIO

USD (R&E)

USD (Intelligence)

& Communication

SCRM Coordination Board (SCB)

Joint Staff Designee

Air Force, ASAF (AT&L)

Army, ASA (ALT)

Navy, ASN (RDA)

DASD(IP)

ASD (Acquisition)

ASD (Sustainment)

Director of Defense R&E (R&T)

Director, Intel & Security Office

DoD CIO, Cyber Security

SCRM Coordination

Established and Groups

Operations (examples)

Service Oversight

- Platform X

ASD(S) Oversight

- DMSMS
- VTM

CIO Oversight

- Software Provenance
- TSN

DASD(IP) Oversight

- Industrial Base Assessment
- CFIUS

Combatant Commander Oversight

- Mission X

DD R&E (R&T) Oversight

- HW Assurance/ Anti-Tamper
- Software Assurance
- Cyber Resilience/ System Sec Eng

Level 1

- Chartered by USD(A&S)
- Semi-annual meetings or ad-hoc for critical risks
- USD/Executive-level
- Scope: strategy, monitoring, NDAA, strategic risk items

Level 2

- Chartered by USD(A&S)
- Quarterly meetings or ad-hoc for critical risks
- ASD/General Officer-level
- Supported by GS-15/O-6 level SCRM action group
- Scope: monitoring, sharing practices

Level 3

- Chartered/managed by various leads
- Monthly/bi-monthly meetings or daily operations
- Grade of participating personnel determined by group
- Scope: troubleshooting risk items for the function, sharing data, sharing practices, operations

POC: Ms. Jan Mulligan, ODASD(Logistics), 571-372-5227,
Jan.b.mulligan.civ@mail.mil

What You Can Do

- Understand Acq and Sustainment are Two Points on Same Continuum
- Create Agile LCSP's to Address Eventual Obsolescence
- Understand Where Risk is Acceptable
- Share Information on Risks Discovered in Your Program
- Conduct Due Diligence on Understanding Lower Tiers of Supply Chain
- Plan for Eventual Disruption to Your Supply Chain
- Use Best Practices … No Need to Duplicate Effort of Others
- Make PPP's & LCSP's Living Documents
- Practice Good Cyber Hygiene, and Recognize Threats
- Train and Exercise Your Organization to be Resilient

POC: Ms. Jan Mulligan, ODASD(Logistics), 571-372-5227,
Jan.b.mulligan.civ@mail.mil

QUESTIONS?

POC: Ms. Jan Mulligan, ODASD(Logistics), 571-372-5227,
Jan.b.mulligan.civ@mail.mil