NDIA Section 224 Workshop

Thursday, October 15, 2020

1:00PM – 5:00PM EDT

Welcome to NDIA Section 224 Workshop

- Introduce Slido Polling Application

Introduction

- NDIA Subcommittee Workshop for Section 224 Legislation
- Workshop duration from 1:00PM – 5:00PM EDT
- High-level background for workshop
- Workshop Agenda

Background and Motivation for Workshop – Ezra Hall

- **OSD deadline to provide final report for Section 224 implementation approach**
  - Final NDIA Coordination 10/22/2020
  - OSD Report for Congress (Final) 12/4/2020
- **NDIA subcommittee would like to help gather inputs, concerns, recommendations for approach proposed in OSD response**
- **The intent is to have a collaborative effort that includes recommendations on how the standards can assist with coordination, cooperation and incentivization for supply chain adoption and robust execution of Section 224 requirements**

Workshop Agenda

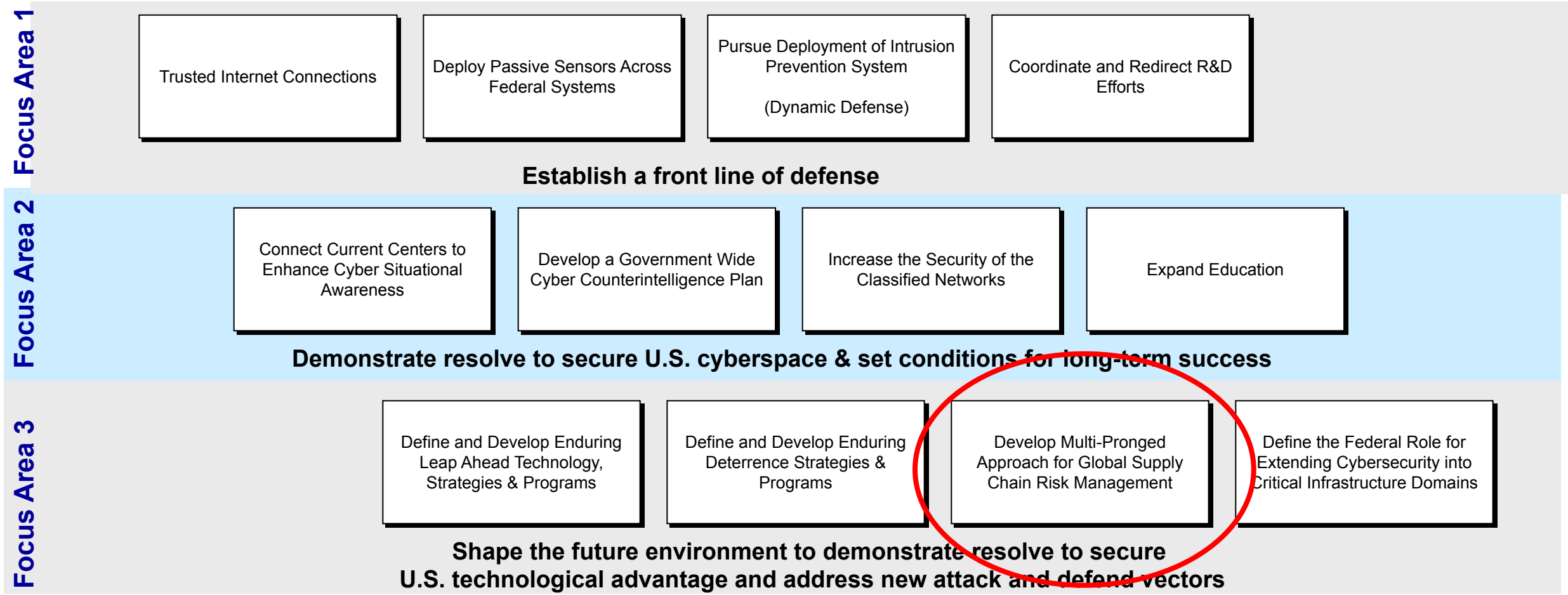
Time/Duration *Eastern Daylight Time zone*	Agenda Topic
1:00PM-1:10PM 10 min. duration	Introduction – Ezra Hall - Background, motivation, and review of workshop outline - Review of workshop goals and objectives
1:10PM-1:30PM 20 min. duration	Review of Section 224 and intent of legislation – Donald Davidson - High-level review of Section 224 legislation and intent *(10 min.)* - Group discussion of legislation and intent *(10 min.)*
1:30PM – 1:40PM 10 min. duration	Overview and discussion of importance of focused concepts – Coordination, Cooperation, and Incentivization within 6 tenants – Jeremy Muldavin - Group Discussion, polls, survey questions - Are there potential concerns within these 3 focused areas? - What are key items that are important to standards for the 6 tenetts of 224?
1:40PM – 1:50PM 10 min. duration	Break
1:50PM – 2:20PM 30 min. duration	Review of current OSD approach – Randy Woods - OSD approach to Section 224 (20 min.) - Wrap-up (10 min.) - Running question poll under Slido (Top 3 Q&A)

Time/Duration *Eastern Daylight Time zone*	Agenda Topic
2:20PM – 2:45PM 25 min. duration	Breakout Instructions & Assignments – Joy Angelle - Instructions and agenda of breakout groups - Assign workshop members to each breakout group
2:45PM – 4:00PM 75 min. duration	**Breakout Session Activity** – **Break-out group 1**: Manufacturing location & company ownership. Breakout Leader: Jeremy Muldavin **Break-out group 2**: Workforce composition & Access during manufacturing. Breakout Leader: Ken Heffner **Break-out group 3**: Reliability of supply chain & operational security. Breakout Leader: Donald Davidson **Breakout Team Objectives:** - Discuss and document team's response to discussion questions provided - Prioritize team's response and determine top 3 team responses for problems/solutions - Develop breakout team summary to present to the main workshop group during breakout report-outs
4:00PM – 4:55PM 55 min. duration	Breakout final outbrief presentations - - Breakout Team 1 (15 min.) - Breakout Team 2 (15 min.) - Breakout Team 3 (15 min.) - Q&A (5 min.)
4:55PM – 5:00 PM 5 min. duration	Workshop wrap-up and next steps – Ezra Hall

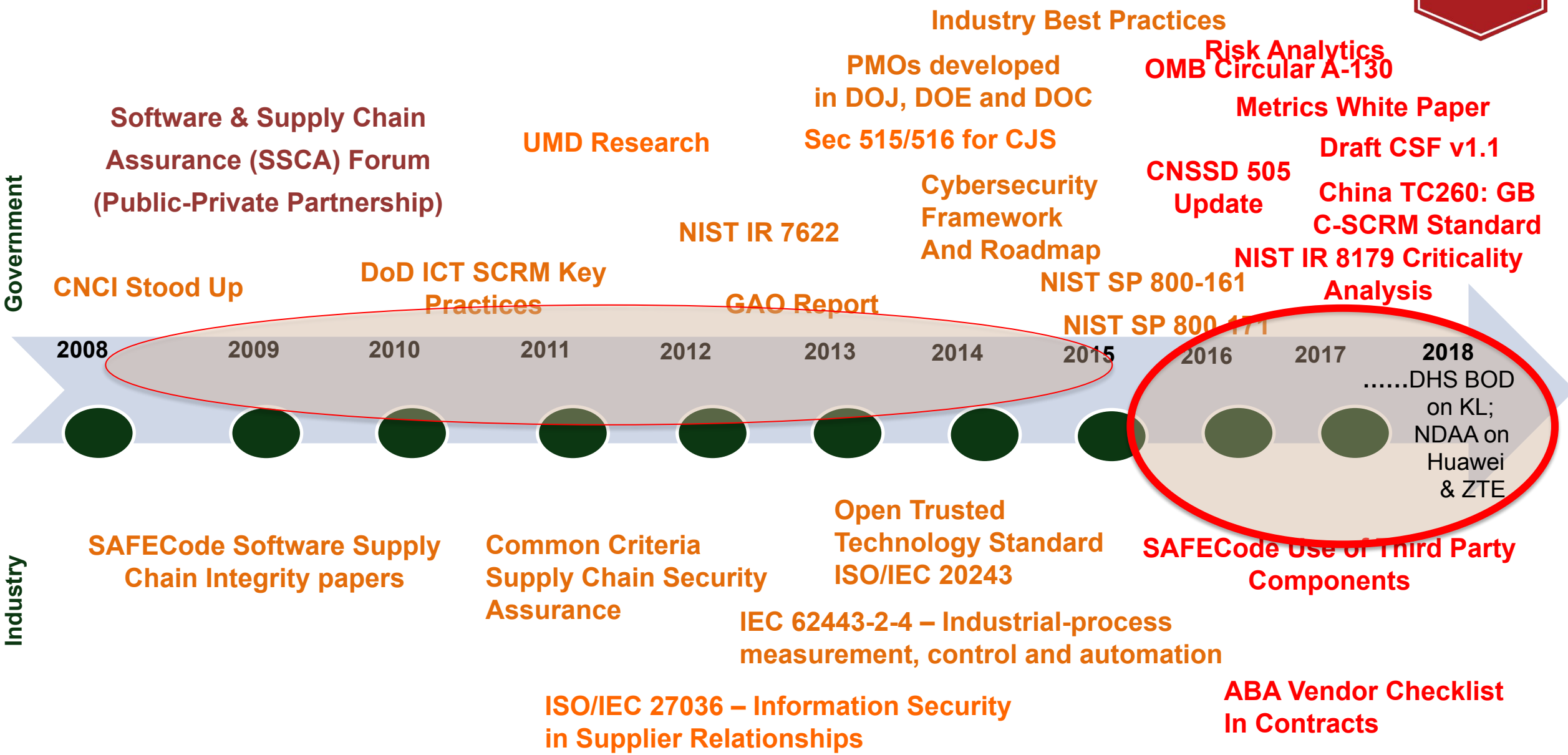
BACKGROUND
Cyber-SCRM, to include Hardware Assurance &
Standards for Microelectronics Security
iaw Section 224 of NDAA 2020

Don Davidson
Director, Cyber-SCRM Programs
Don.Davidson@Synopsys.com

Comprehensive National Cybersecurity Initiative (CNCI)



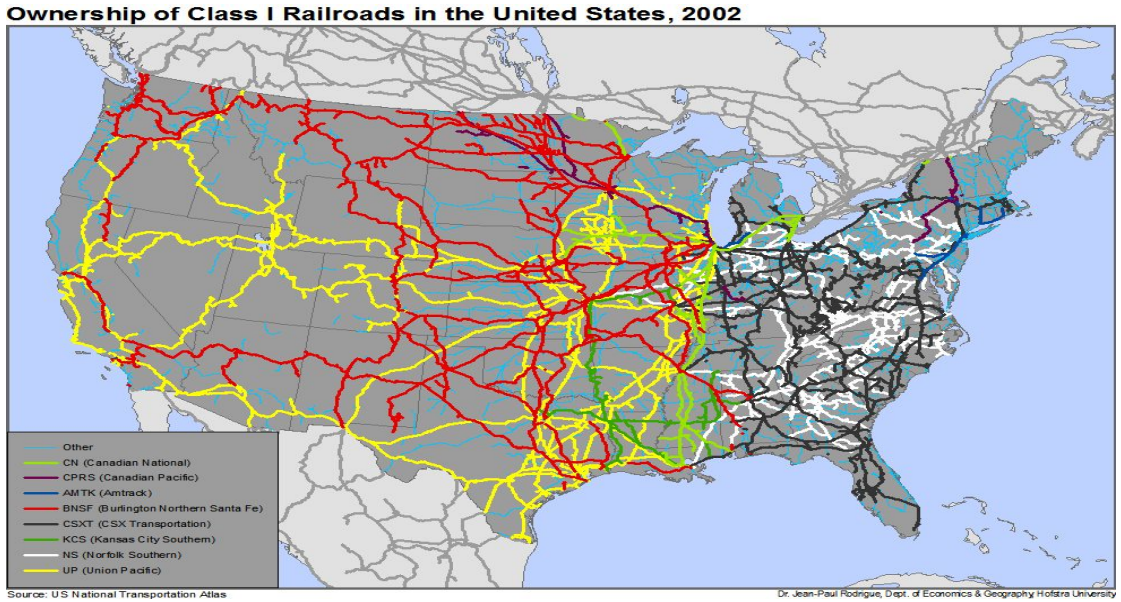
Existing and Emerging SCRM Research, Policy, Standards and Practices



Supply Chain: PERSPECTIVES – Traditional Supply Chain Management

Supply Chain SECURITY

- Nodes of storage & throughput
- Lines of transport (& communication)



Supply Chain RESILIENCE

- Multi-sources
- Multi-nodes
- Multi-routes

Supply Chain: PERSPECTIVES - Value Chain

Set Of Activities That A Firm Operating In A Specific Industry Performs In Order To Deliver A Valuable Product Or Service

Primary activities

- **Inbound Logistics**
- **Operations**
- **Outbound Logistics**
- **Marketing and Sales**
- **Service**

Support activities:

- **Procurement**
- **Human Resource Management**

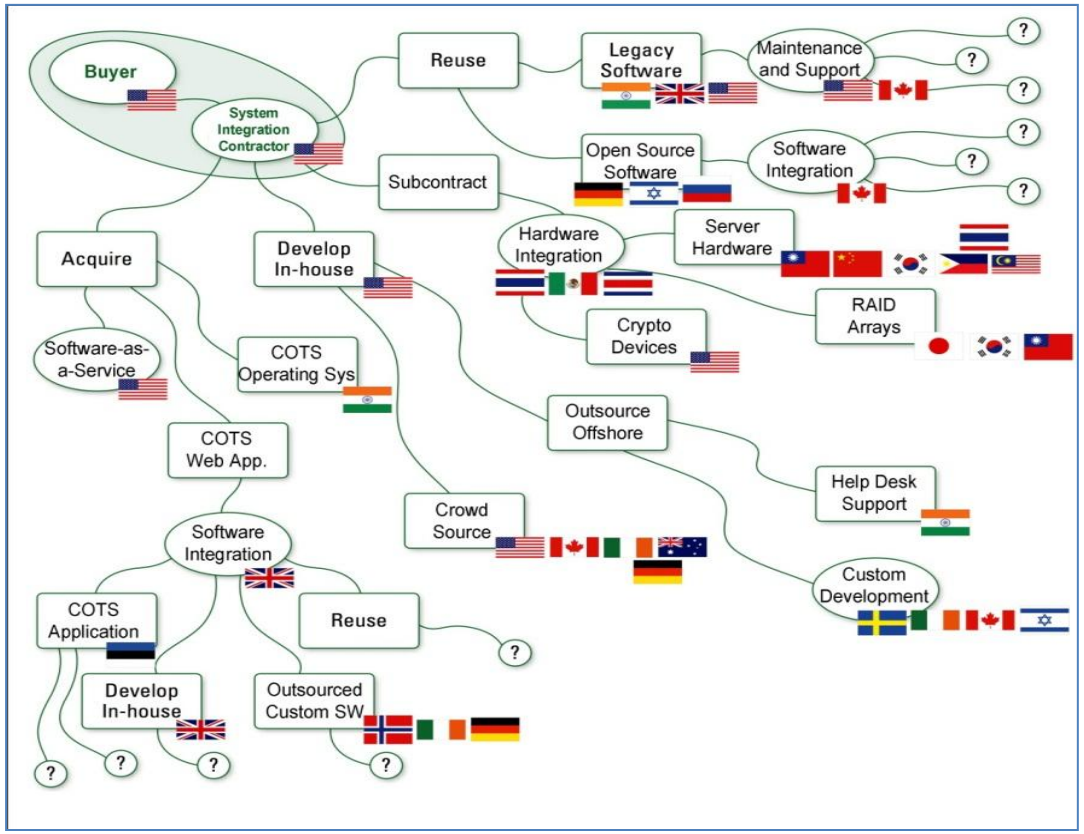
Simplistic Representation of Component List for a Dell Laptop

Component	Supplier or Potential Suppliers
Intel Microprocessor	US-owned factory in the Philippines, Costa Rica, Malaysia, or China *(Intel)*
Memory	South Korea *(Samsung)*, Taiwan *(Nanya)*, Germany *(Infineon)*, or Japan *(Elpida)*
Graphics Card	China *(Foxconn)*, or Taiwanese-owned factory in China *(MSI)*
Cooling fan	Taiwan *(CCI and Auras)*
Motherboard	Taiwan *(Compal and Wistron)*, Taiwanese-owned factory in China *(Quanta)*, or South Korean-owned factory in China *(Samsung)*
Keyboard	Japanese company in China *(Alps)*, or Taiwanese-owned factory in China *(Sunrex and Darfon)*
LCD	South Korea *(Samsung, LG.Philips LCD)*, Japan *(Toshiba or Sharp)*, or Taiwan *(Chi Mei Optoelectronics, Hannstar Display, or AU Optronics)*
Wireless Card	Taiwan *(Askey or Gemtek)*, American-owned factory in China *(Agere)* or Malaysia *(Arrow)*, or Taiwanese-owned factory in China *(USI)*
Modem	China *(Foxconn)*, or Taiwanese company in China *(Asustek or Liteon)*
Battery	American-owned factory in Malaysia *(Motorola)*, Japanese company in Mexico, Malaysia, or China *(Sanyo)*, or South Korean or Taiwanese factory *(SDI and Simplo)*
Hard Disk Drive	American-owned factory in Singapore *(Seagate)*, Japanese-owned company in Thailand *(Hitachi or Fujitsu)*, or Japanese-owned company in the Philippines *(Toshiba)*
CD/DVD	South Korean company with factories in Indonesia and Philippines *(Samsung)*, Japanese-owned factory in China or Malaysia *(NEC)*, Japanese-owned factory in Indonesia, China, or Malaysia *(Teac)*, or Japanese-owned factory in China *(Sony)*
Notebook Carrying Bag	Irish company in China *(Tenba)*, or American company in China *(Targus, Samsonite, and Pacific Design)*
Power Adapter	Thailand *(Delta)*, or Taiwanese-, South Korean-, or American-owned factory in China *(Liteon, Samsung, and Mobility)*
Power Cord	British company with factories in China, Malaysia, and India *(Volex)*
Removable Memory Stick	Israel *(M-System)*, or American company with factory in Malaysia *(Smart Modular)*

From *The World Is Flat by Thomas Friedman*
Dell Inspiron 600m Notebook: Key Components and Suppliers

Adapted from: https://en.wikipedia.org/wiki/Value_chain

Supply Chain: PERSPECTIVES - Product Integrity /
Software Assurance And Hardware Assurance (Anti-Counterfeit)



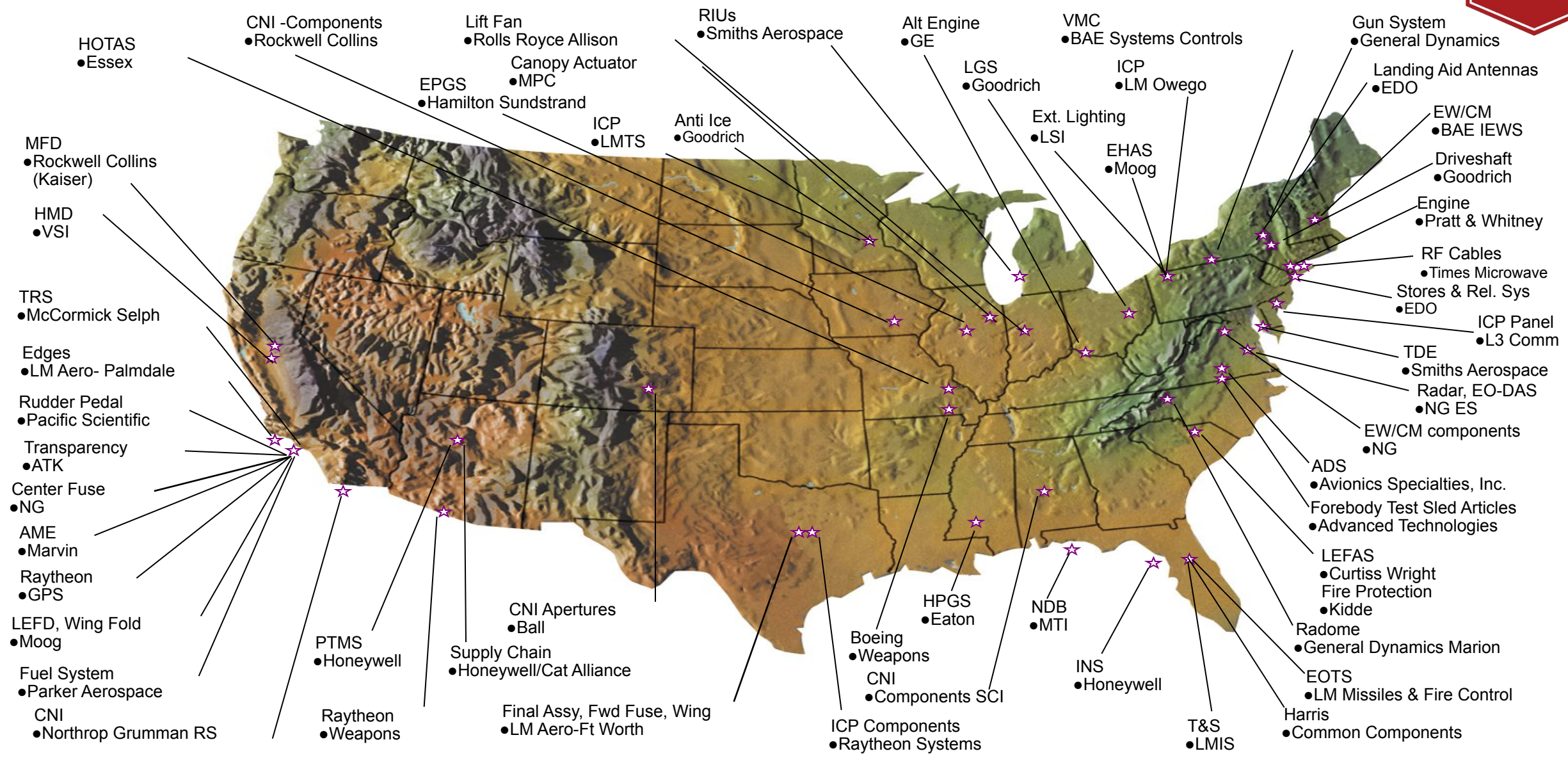
IT and Communications products are assembled, built, and transported by multiple vendors around the world.

Software contributions include reusable libraries, custom code, commercial products, open source

One telecom provider had software with 84 different first tier suppliers for the software.

How do we improve our trust & confidence from a global ICT supply chain?

JSF Extended Team – U.S.



Source: Lockheed Martin Aeronautics Company

F-35 Extended Team - International Industrial Participation

U.K.

BAE SYSTEMS
Goodrich Adv. Sys
Helmet
Integrated Sys.
Martin Baker
Hambles Sturc.
Smiths +Others
Beaufort
Smiths
GKN
Microfiltrex
HS Claverham
HS Marston
QinetiQ
Didsbury Engr
Kennard
+ Others

Turkey

TAI
Ayesas
Havelsan
KaleKalip
TAI
Aselsan
MIKES
Hema
KaleKalip
ALP
Parsans

Gate Elektronic
ALP Aviation
Aselsan
AYESAS
Gate Elektronic
Havelsan
Hema/Alp
Kale Kalip
Marconi
Mikes
Parsan Steel Forging
TAI
TEI
+ Others

Netherlands

ATS Kleizen
Fokker Elmo, Aero, Defense
Sun Electronic
Philips Aerospace
SP Aerospace
Thales Cyrogenics
DAP
Thales Optronics
Sun Electronic
Phillips Aerospace
Thales Cyrogenics + Others
Axxiflex
Senior Aerospace Bosman
PHM Group
Urenco
+ Others

Norway

Kongsberg
Metronor
Techni
NERA
Kongsberg
Kitron
3D Perception
Applica
Ericsson
Kitron

Metronor
Nammo
Natech
NERA
Presens
SensoNor AS
SINTEF
T & G Elektro
Thales Comm.
+Others

Australia

Micro LTD
Ferra Engineering
Hovitt
Cablex
Varley
Production Parts
Calytrix Technologies
+ Others
Micreo
Cablex
Lovitt + Others
Compucat
Rosebank Eng
+ Others

Denmark

Terma AS
GPV
SSE
IFAD
HiQ Wise
Corena
Terma
SSE
GPV
E.Falk Schmidt
Maersk Data Def
Elbo Production
Danish Aerotech
Hamann Electronics
+ Others

Italy

Alenia
Marconi Sirio Panel
Galileo
Piaggio
Moog- Caselle
UOP
Secondo Mona
Samputensilli
Marconi Selenia
York
+Others

OMA Mecaer
Aerea
Aermacchi
Galileo
ASE
Forgital
Inossman
Logic
+ Others

Canada

Herovx-Devtek
Magellan-Chicopee
Honeywell Eng. Sys
DY4
Mindready
Howmet
Virtek +Others
Mustang Surv. Co
Bristol Aerospace
Graphico
Novatronics
DMG + Othes
Bombardier
Air Data Inc
CMC Electronics
Noranco + Others

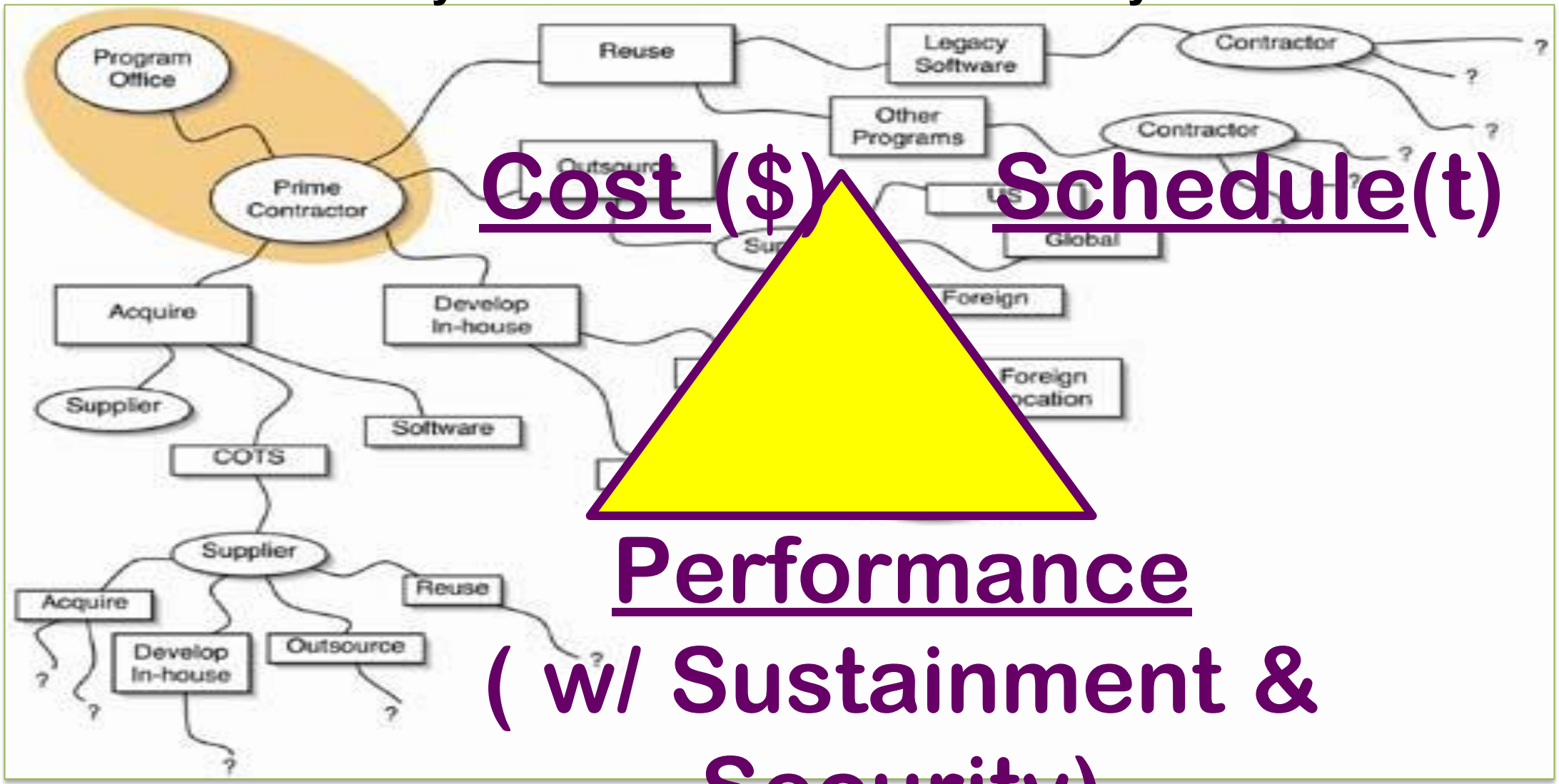
Global Development and Production

Source: Lockheed Martin Aeronautics Company

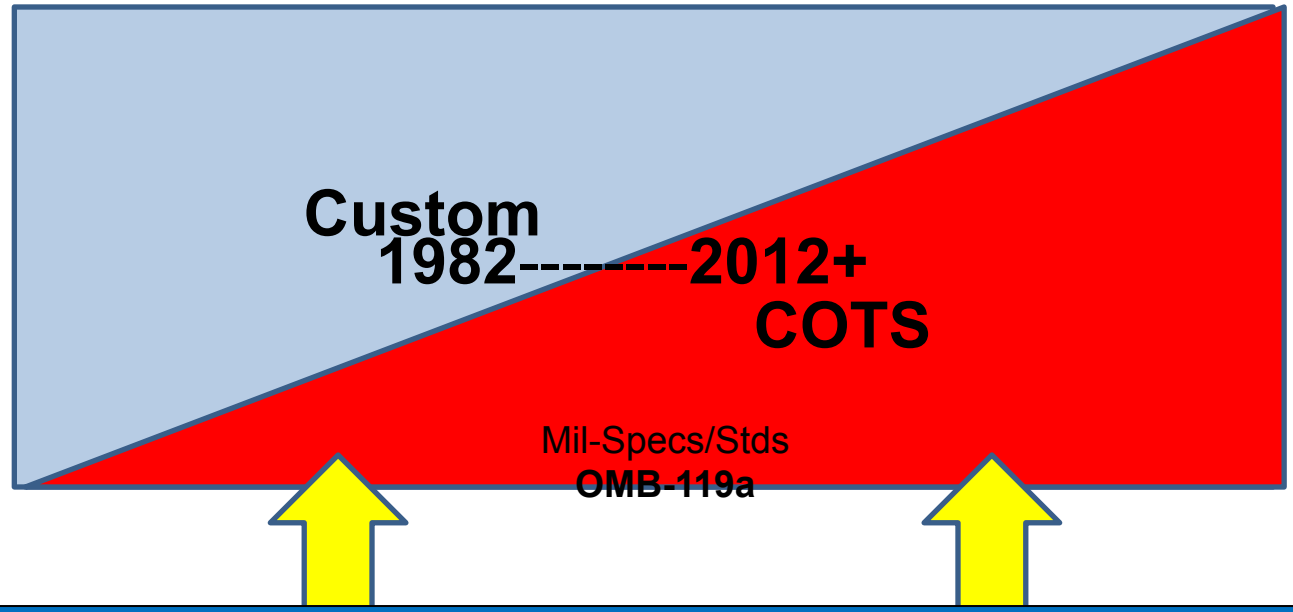
Globalization is good,

but it brings challenges **"DELIVER UNCOMPROMISED"**

says build in a 4th Pillar for Security?...



…and…we are all *increasingly* ***Dependent*** on COTS products



"This is a trend the department has frankly been willing to recognize more in policy than in practice…I'd hazard a guess that 25 years ago, 70 percent of the goods and services the department procured were developed and produced exclusively for the military. Today, that ratio has reversed. Seventy percent of our goods and services are now either produced for commercial consumption or with commercial applications in mind. And it's backed by a largely commercial-based supply chain."

– Mr Brett Lambert, former DASD for Manufacturing and Industrial Base Policy

This is even more true for our Critical Infrastructure.

SCRM informs Us

(*and our decision making processes*)

Given: We rely more & more on COTS / modular components (microelectronics & software), that are supplied through a globally sourced supply chain.

What information is needed for our

“Make-or-Buy” decision,

&

how do we make our

“Fit-for-Use” determination?

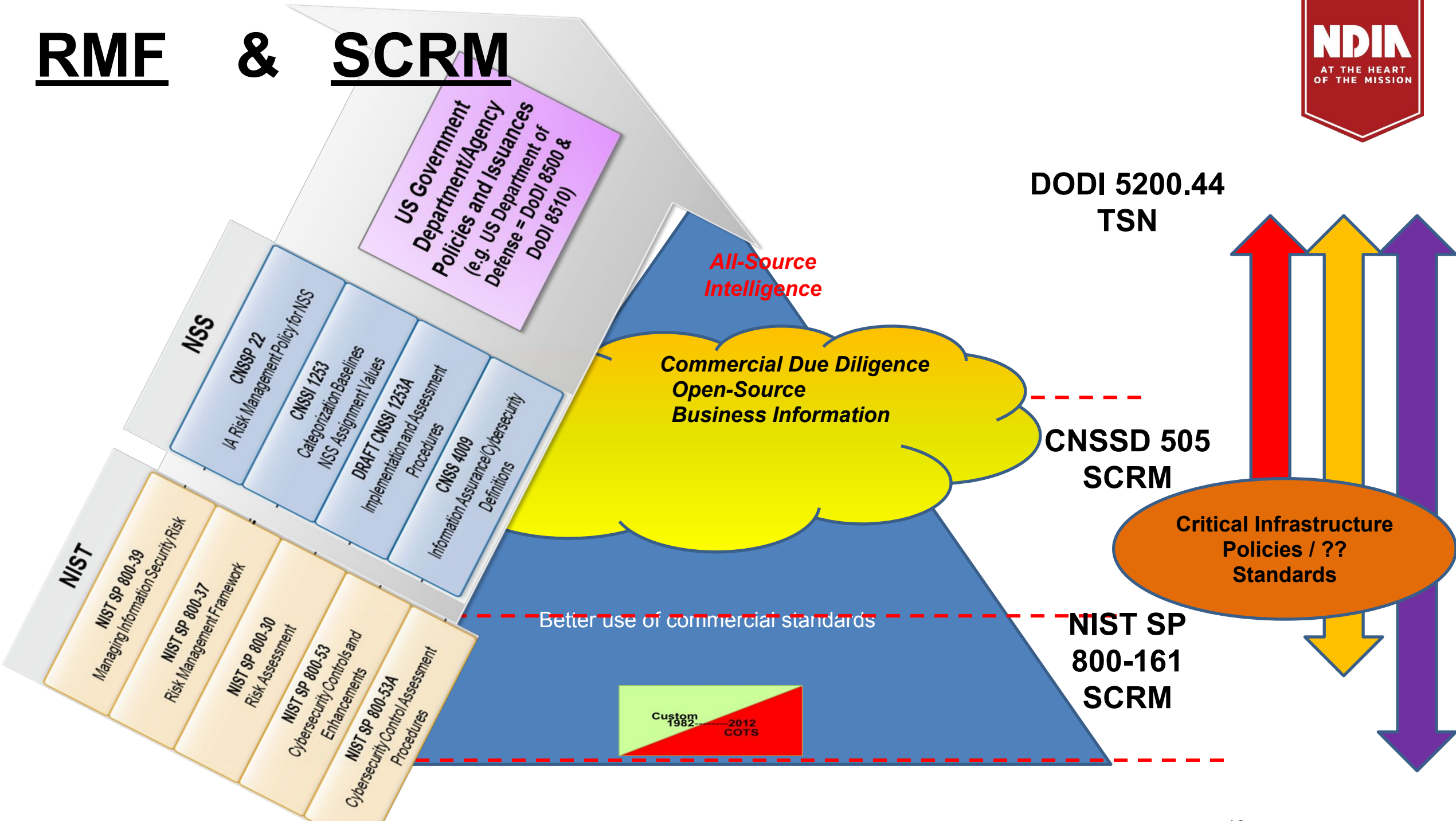
Ensuring Confidence in Defense Systems

- ***Threat*: Nation-state, terrorist, criminal, or rogue developer who:**
  - Gain control of systems through supply chain opportunities
  - Exploit vulnerabilities remotely
- ***Vulnerabilities***
  - All systems, networks, and applications
  - Intentionally implanted logic
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- ***Traditional Consequences*: Loss of critical data and technology**
- ***Emerging Consequences*: Exploitation of manufacturing and supply chain**

Today's acquisition environment drives the increased emphasis:

Then		Now
Stand-alone systems	>>>	Networked systems, IT / OT
Some software functions	>>>	Software-intensive
Known supply base	>>>	Prime Integrator, hundreds of suppliers
CPI (technologies)	>>>	CPI and critical components

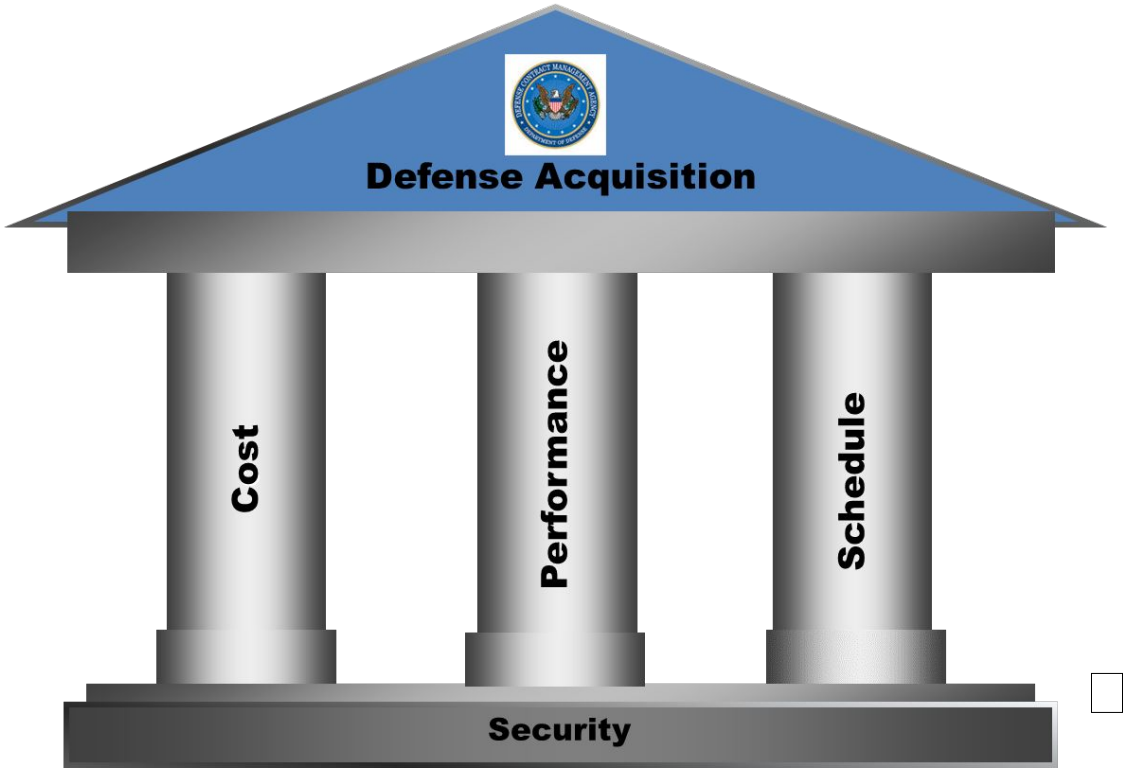
RMF & SCRM


US Government Department/Agency Policies and Issuances (e.g. US Department of Defense = DoDI 8500 & DoDI 8510)
NSS
CNSSP 22
IA Risk Management Policy for NSS
CNSSI 1253
Categorization Baselines
NSS Assignment Values
DRAFT CNSSI 1253A
Implementation and Assessment Procedures
CNSS 4009
Information Assurance/Cybersecurity Definitions
NIST
NIST SP 800-39
Managing Information Security Risk
NIST SP 800-37
Risk Management Framework
NIST SP 800-30
Risk Assessment
NIST SP 800-53
Cybersecurity Controls and Enhancements
NIST SP 800-53A
Cybersecurity Control Assessment Procedures
All-Source Intelligence
Commercial Due Diligence
Open-Source
Business Information
Better use of commercial standards
Custom
1982
2012
COTS
DODI 5200.44
TSN
CNSSD 505
SCRM
Critical Infrastructure
Policies / ??
Standards
NIST SP
800-161
SCRM

We need to make Security the Foundation
We need to *Deliver Uncompromised*

Cost, Schedule, Performance

ARE ONLY EFFECTIVE IN A SECURE ENVIROMENT



- **CMMC**

There is a need to develop the Science of Cybersecurity and Cyber-SCRM

- **Hardware**
- Software
- Services

We need to better understand how to measure cybersecurity / supply chain risk?...
Hardware Assurance (HwA) / Microelectronic Security?

What's the balance between commercial standards & regulation ?

ISO/IEC 27002

Confidentiality=
Ensuring that information is accessible only to those authorized to have access.

Integrity=
Safeguarding the accuracy and completeness of information and processing methods.

Availability=
Ensuring that authorized users have access to information and associated assets when required.

DMEA Trusted IC Program

https://www.dmea.osd.mil/TrustedIC.aspx

- DMEA is the program manager for the DoD Trusted Foundry program. The program provides a cost-effective means to assure the *integrity and confidentiality* of integrated circuits during design and manufacturing while providing the US Government with *access to leading edge* microelectronics technologies for both Trusted and non-sensitive applications.

- *Trusted* - Is the confidence in one's ability to secure national security systems by assessing the integrity of the people and processes used to design, generate, manufacture and distribute national security critical components (i.e. microelectronics).

- OUSD-R&E is now pursuing "*Zero Trust & Quantifiable Assurance*"

USG participation in SDOs & Cyber Standards Coverage

Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity

NISTIR 8074 (Volume 1 & Volume 2) December 2015

- https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v1.pdf
- https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf

IoT Security Presentation (June 2020)

- https://www.nist.gov/news-events/events/2020/06/foundational-cybersecurity-guidance-iot-device-manufacturers-nistir-8259

2019 NSTAC Report on Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem

THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE (NSTAC) Report on *Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem* (dtd September 3, 2019)--- specifically says,

> **"With respect to ensuring we have the ability to assess whether ICT products are trustworthy…We need to evolve the science and the standard."**
>
> **(by Mr. Donald Davidson, Synopsys)**

- https://www.cisa.gov/sites/default/files/publications/nstac_letter_to_the_president_on_advancing_resiliency_and_fostering_innovation_in_the_ict_ecosystem_0.pdf

NDAA 2020 Section 224 on Microelectronics Security Standards

"To protect the United States from intellectual property theft and to ensure national security and public safety in the application of new generations of wireless network technology and microelectronics, beginning no later than January 1, 2023, the Secretary of Defense shall ensure that each microelectronics product or service that the Department of Defense purchases on or after such date meets the

***applicable trusted supply chain and operational security standards*"… Addressing:**

- ***manufacturing location***
- ***company ownership***
- ***workforce composition***
- ***access during manufacturing, suppliers' design, sourcing, manufacturing packaging, and distribution processes***
- ***reliability of the supply chain; and***
- ***other matters germane to supply chain and operational security… not MIL-STD***

DoD delivers 224 report to Congress by Jan 2021… & implements in DoD by Jan 2023.

https://docs.house.gov/billsthisweek/20191209/CRPT-116hrpt333.pdf

Section 224 starts on page 136 of the NDAA 2020 **Cyber Space Solarium Commission Report**

Overview of Key Concepts and Considerations for NDAA Section 224

Jeremy Muldavin

Three Key Concepts

- **Coordination**
  - Within USG?
  - Industry and Critical Infrastructure?
  - Allied nations and trade partners?
- **Cooperation**
  - Microelectronics industry- design, manufacturing, test, end-users?
  - Interagency?
  - Allied nations & standards bodies?
- **Incentivization**
  - Quantification and Valuation of Assurance
  - Barriers vs. Opportunities to help deliver assured domestic supply and capability
  - Acquisition, Market, and Consumer preference & incentives?

Sect. 224 Tennant Groups and Considerations

1) Manufacturing Location & Ownership

2) Workforce Composition & Access to Articles

3) Supply Chain & Operational Security

Sect. 224 Implementation Considerations

- **Quantified Assurance across supply chain**
  - Risk Assessment methodology
    - System Program Perspective
    - Supply Chain Perspective
  - standard process for assessment, reporting, validation, etc.
- **Tiers of Trust/Assurance**
  - What categories and quantitative levels are appropriate to enable tailored risk assessments
- **Standards applicability to address above?**
  - Mapping, analysis, effectivity evaluation, gaps, translation
- **Incentives and valuation of tiers of quantified assurance**
  - within acquisition for DoD, USG?
  - within the DIB and critical domestic infrastructure
  - auxiliary industries (insurance, finance, medical, automotive, IoT etc.)
  - with allied and partner nations

Create a value proposition to raise security as a common requirement buyers consider in a decision making process

Break – 1:40PM – 1:50PM EDT 10 minutes

- Return back to main conference line at 1:50PM EDT

NDAA FY20 Section 224 Overview

Randy Woods

Breakout Instructions & Assignments – Joy Angelle

- **High-level overview of breakout groups**
  - Breakout group 1: Manufacturing Location & Company Ownership
  - Breakout group 2: Workforce Composition & Access During Manufacturing
  - Breakout group 3: Reliability of Supply Chain & Operational Security
- **Discussion instructions**
  - Breakout teams will review their assigned tenets and answer the 5 questions:
    - What's the problem?
    - What is the cost of taking action?
    - What could be the possible desired end state of a solution?
    - What are the 3 key steps that can be taken to implement?
    - Who are the stakeholders who care about these tenets?

Breakout Instructions & Assignments – Joy Angelle

- Breakout conference links - add to zoom chat
- Please return to workshop main conference line at 4:00 PM for Breakout session outbriefs and workshop wrap-up

Breakout Final Outbrief

- Breakout group 1 - Manufacturing Location & Company Ownership
- Breakout group 2 - Workforce Composition & Access During Manufacturing
- Breakout group 3 - Reliability of the Supply Chain & Operational Security

Workshop Wrap-up

- **Thank you for your support!**
- **Industry sectors of interest:**
  - Automotive
  - 5G
  - Wifi 6
  - Medical devices
  - transportation
  - industrial control systems
  - Aerospace
  - Financial
  - Energy
  - Insurance

Workshop Wrap-up

- **Next steps:**
  - Group 2 follow-up session to be scheduled
  - Curation of all ideas and information that was shared and provided to Randy
  - Follow-on discussions with B2C industry sectors
    - Possible additional Insurance discussions
  - What standards should be evaluated? Please provide to OSD for review (other standards, obscure standards, company guidance)
  - Would it be useful to develop a joint working group developed by NDIA to support Section 224 efforts over time?
  - Facilitate meetings with other inter-agency groups for additional discussion
  - 4 NDIA reports review/scrub (reports from 2017)