Wisconsin Procurement Institute

APEX ACCELERATORS

Emerging Issues:

Supply Chain Risk Management (SCRM)

November 2| 1:00 – 2:00 pm

Presented by:

Marc Violante, WPI

NCMA WISCONSIN

Webinar Etiquette

PLEASE

- § Log into the GoToWebinar session with the name that you registered with online
- § Place your phone or computer on MUTE
- § Use the QUESTIONS option to ask your question(s).
  - § We will share the questions with our guest speaker who will respond to the group

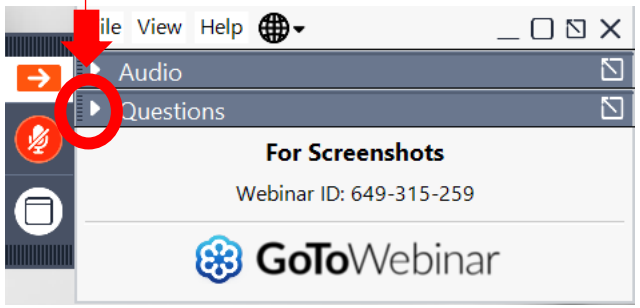
THANK YOU!

Wisconsin Procurement Institute

NCMA WISCONSIN

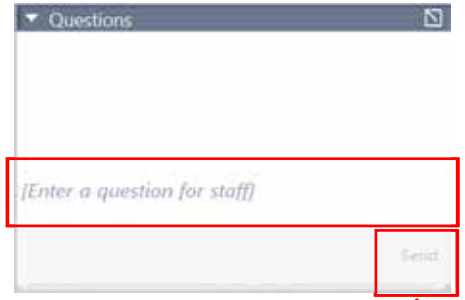
OPENING THE QUESTIONS BOX

Click here to access
within the Control Panel



USING THE QUESTIONS BOX

Type questions
here at any time
during a
presentation



Click Send when ready to submit a question

Wisconsin Procurement Institute

NCMA WISCONSIN

Wisconsin Procurement Institute

APEX ACCELERATORS

Assisting Wisconsin businesses compete in the government marketplace.

WPI is Wisconsin's APEX ACCLERATOR

The APEX Accelerators program, under management of the Department of Defense (DOD) Office of Small Business Programs (OSBP), plays a critical role in the Department's efforts to identify and engage with a wide range of businesses entering and participating in the defense supply-chain. The program provides the education and training that all businesses need to participate to become capable of participating in DOD and other government contracts.

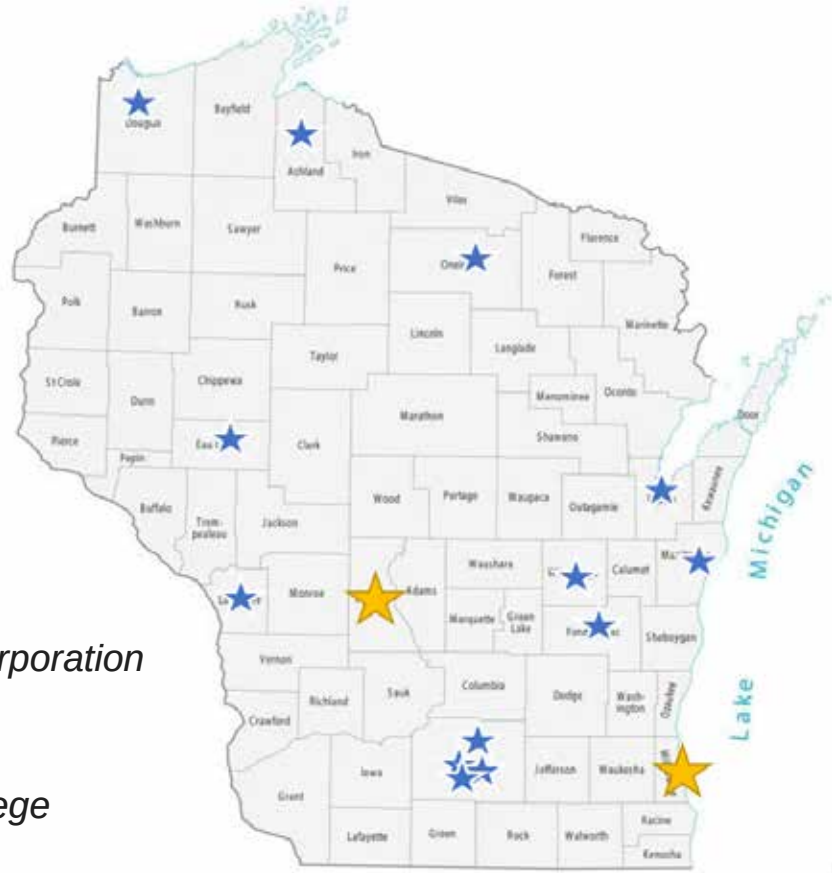
WPI provides services to all of Wisconsin's 72 counties

- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops
- Conferences including one on one buyer meetings – Marketplace, The Contracting Academy, Small Business Academy, Wisconsin Federal Contractor Forum, Acquisition Hour, Cyber Fridays, DOD Roadmap series, Government Opportunities Business Conference, End of Year Federal Contractor Update, Annual DOD Contract Management Update, Evening FAR sessions and more……

www.wispro.org

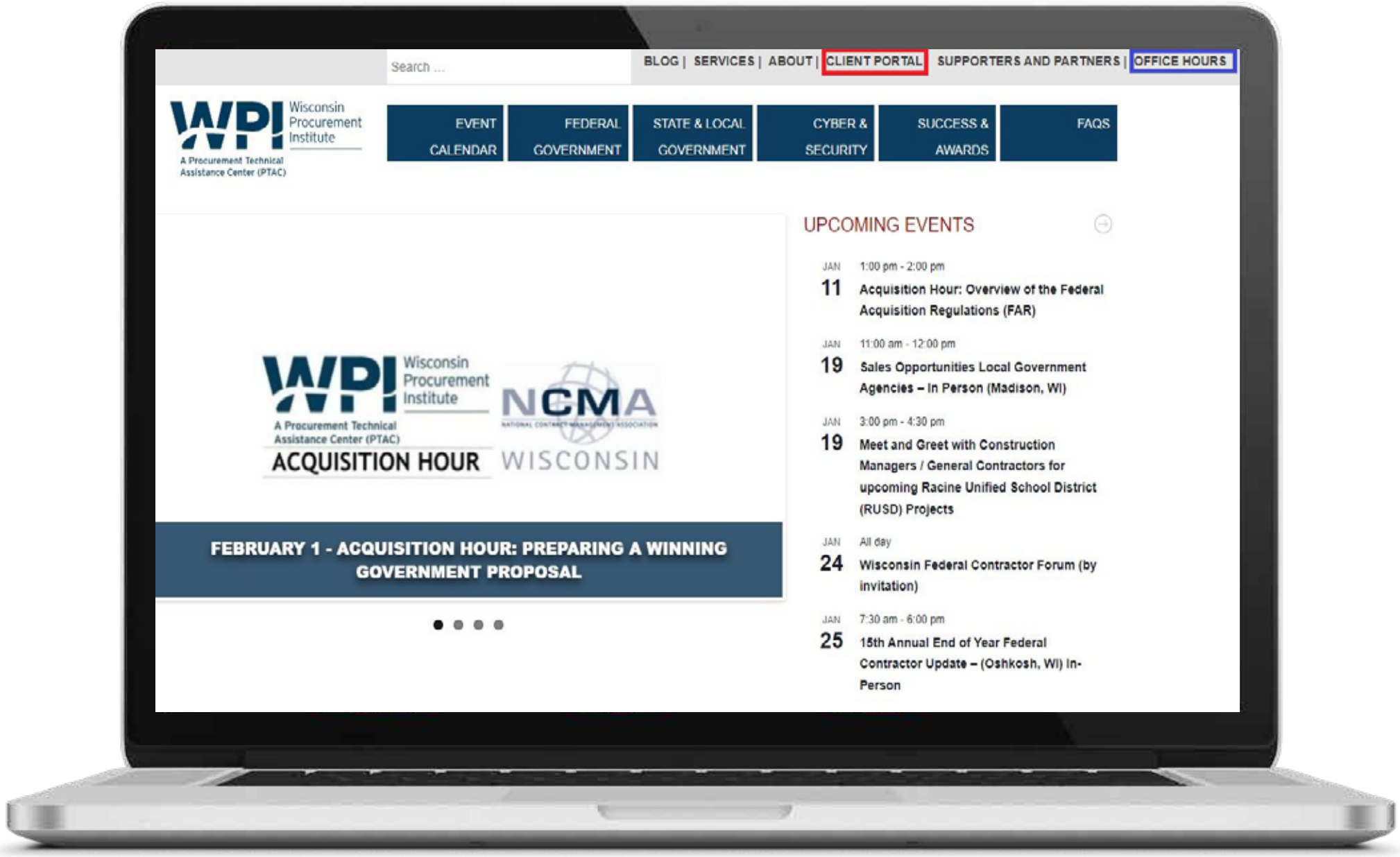
WPI OFFICE LOCATIONS

- **MILWAUKEE**
  - *Technology Innovation Center*
- **MADISON**
  - *FEED Kitchens*
  - *Dane County Latino Chamber of Commerce*
  - *Wisconsin Manufacturing Extension Partnership (WMEP)*
  - *Madison Area Technical College (MATC)*
- **ASHLAND**
  - *Ashland Area Development Corporation*
- **CAMP DOUGLAS**
  - *Juneau County Economic Development Corporation (JCEDC)*
- **EAU CLAIRE**
  - *Western Dairyland*
- **FOND DU LAC**
  - *Envision Greater Fond du Lac*
- **GREEN BAY**
  - *NWTC Startup Hub*
- **LACROSSE**
  - *Veterans in Professions*
- **MANITOWOC**
  - *Progress Lakeshore*
- **OSHKOSH**
  - *Greater Oshkosh Economic Development Corporation*
- **RHINELANDER**
  - *Nicolet Area Technical College*
- **SUPERIOR**
  - *Small Business Dev Center; UW Superior*



WPI Wisconsin Procurement Institute

NCMA WISCONSIN



WPI Wisconsin Procurement Institute APEX

NCMA WISCONSIN

Supply Chain Risk Management (SCRM) "A look into the future"

Marc N. Violante

Wisconsin Procurement Institute

November 2, 2023

Webinar Overview

- This webinar will provide an overview of DoD's current Supply Chain Risk Management Framework and critical elements related to acquisition security and contract performance.

Supply Chain – simply defined

All entities and resources involved in delivering a specified product or service to a destination at or within a required time-frame

Supply Chain Elements

Figure 5. Supply Chain Elements

Defense Logistics Agency Supply Chain Security Strategy, page 7

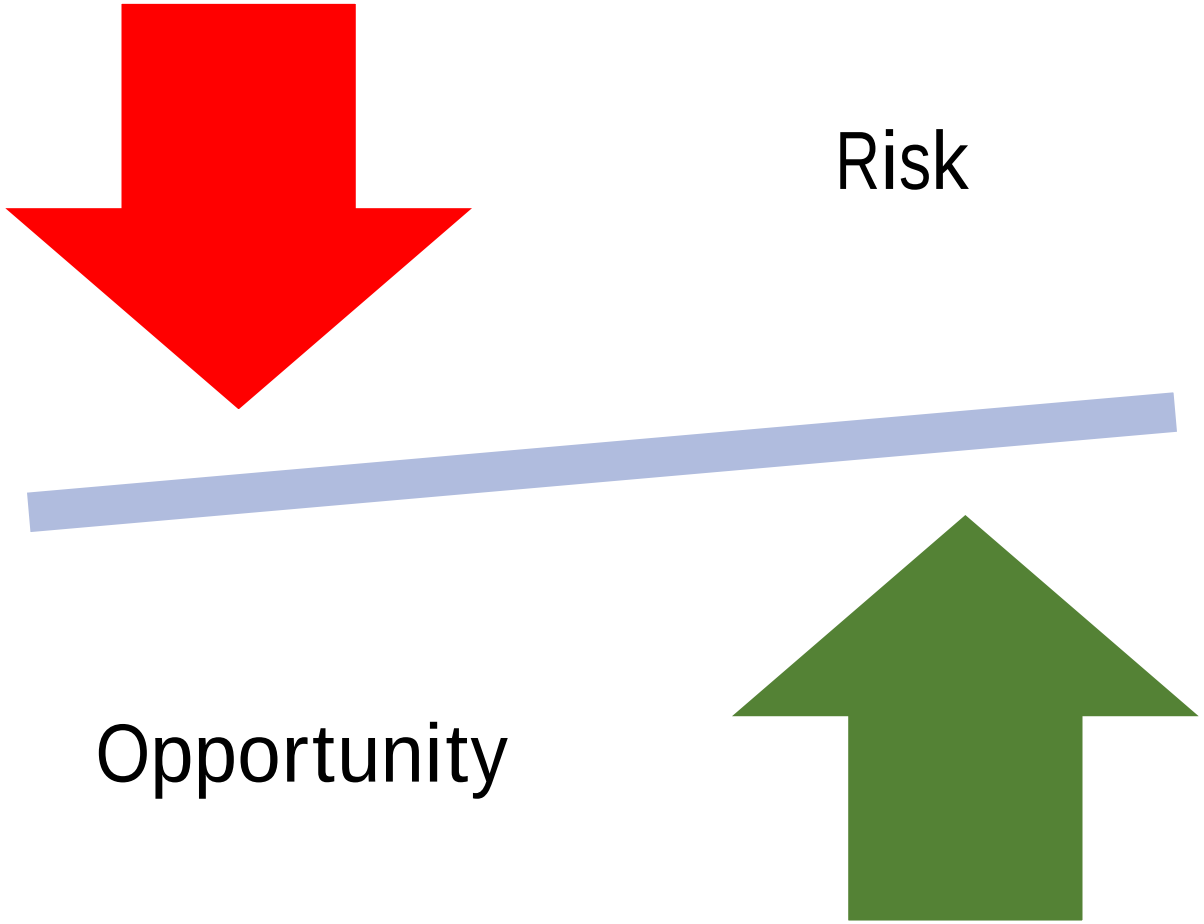
Supply Chain Risk

Anything that threatens or impacts the quantity, quality, delivery

Supply Chain Elements

- Numerous (DoD Framework lists 112 sub-categories)
- Span numerous industries (financial, environment, compliance, …)
- Applicable to all levels of the supply chain - ties
- Identify Risk
- Separates Risk from Resilience
- Requires policies, procedures that **enhance/enable Resilience**
- Requires monitoring

Supply Chain – two sides



Awareness is key

Awareness is key

- Having a mechanism to identify the truly important elements, determine what information is necessary, creating a system and/or process to develop – identify relevant information and manage it.

Supply Chain Risks

Geopolitical

Cyber

Nefarious actors

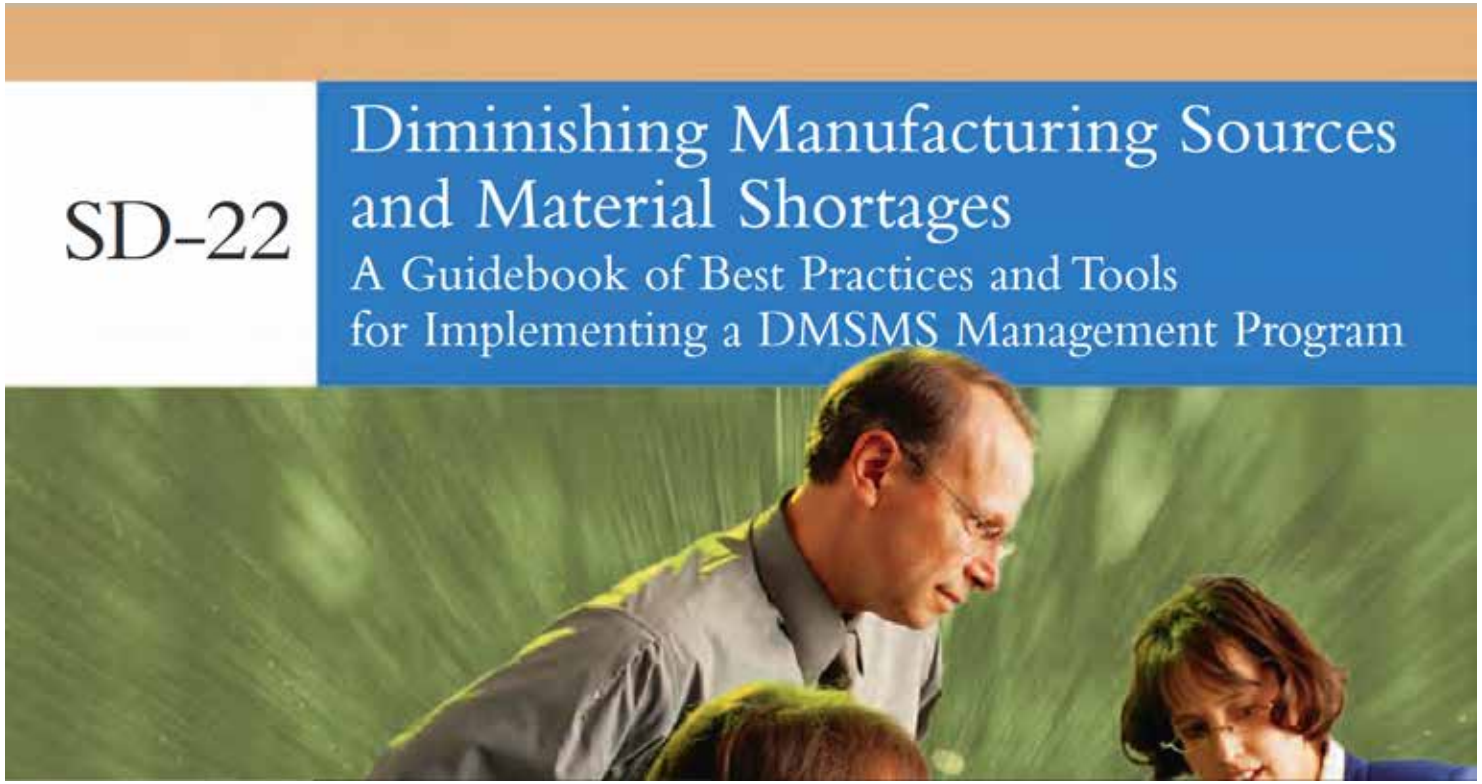
Natural Disasters

Diminishing Manufacturers

Sole Source

SUPPLY CHAIN SECURITY STRATEGY Strengthening Operational Resiliency - Appendix 1 to DLA's 2018 - 2026 Strategic Plan; Introduction

Diminishing Manufactures



https://www.dla.mil/Portals/104/Documents/LandAndMaritime/V/VA/PSMC/LM_SD22FINAL_151030.PDF

DLA – No Bid Solicitation List

- **No Bid Solicitation List** - DLA Land and Maritime and DLA Aviation: This list contains requirements that have not received quotes as of the posting date. This list can contain requirements that were awarded or cancelled since the posting date, so it is recommended to check DIBBS prior to attempting to prepare a quote on a requirement to ensure that it is still open for quoting. Email the DLA Land & Maritime Business Counseling Center for assistance for Land and Maritime No Bids at SmBizLandCols@dla.mil. For DLA Aviation No Bids, please email the Aviation Small Business Office at dlaavnsmallbus@dla.mil.

No Bid – by the numbers

Row Labels	Count of SUPPLY_CHAIN
Aviation	5103
Land	2952
Maritime	2556
(blank)	
Grand Total	**10611**

Row Labels	Count of SOLE_SOURCE_NAME
	3303
BAE SYSTEMS LAND & ARMAMENTS L.P.	1039
THE BOEING COMPANY	540
IVECO DEFENCE VEHICLES S.P.A.	401
LESLIE CONTROLS, INC.	232
SIKORSKY AIRCRAFT CORPORATION	201
PARKER-HANNIFIN CORPORATION	195
NORTHROP GRUMMAN SYSTEMS CORPORATIO	176
BELL TEXTRON INC	159
HAMILTON SUNDSTRAND CORPORATION	132
Grand Total	**6378**

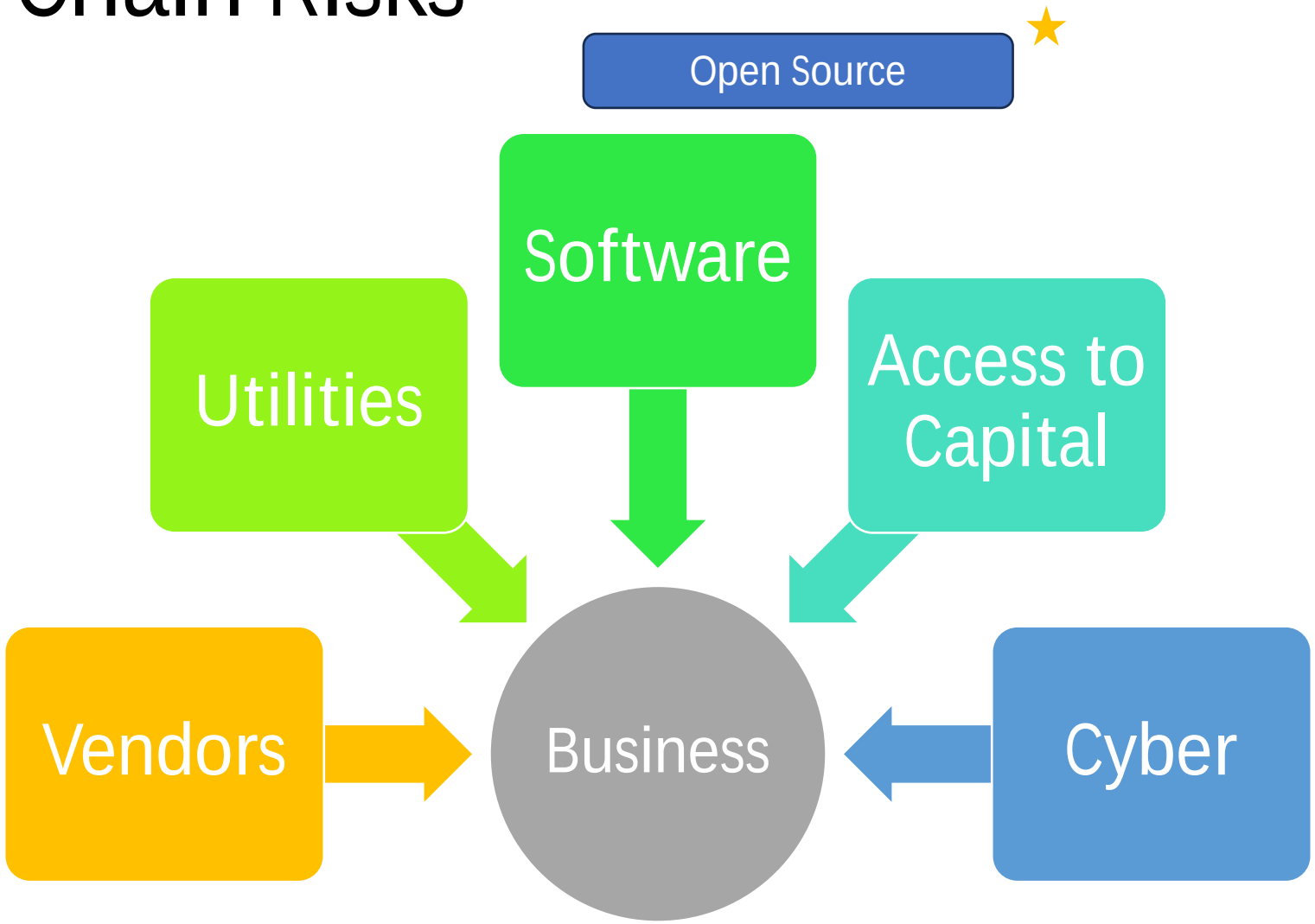
No Bid – possible issues

- Source requirements
- Materials
- Specifications
- Access to TDP/Drawings
- Economic Order Quantity
- Set Aside status

Partners – Knowing & Communicating

- Ownership
- Staff
- Key personnel
- Systems
- Experience
- Training
- Policies/procedures
- Their supply chain

Supply Chain Risks



Open Source Software

- **Software Security in Supply Chains: Open Source Software Controls**
- **EO 14028 – Improving the Nation's Cybersecurity**

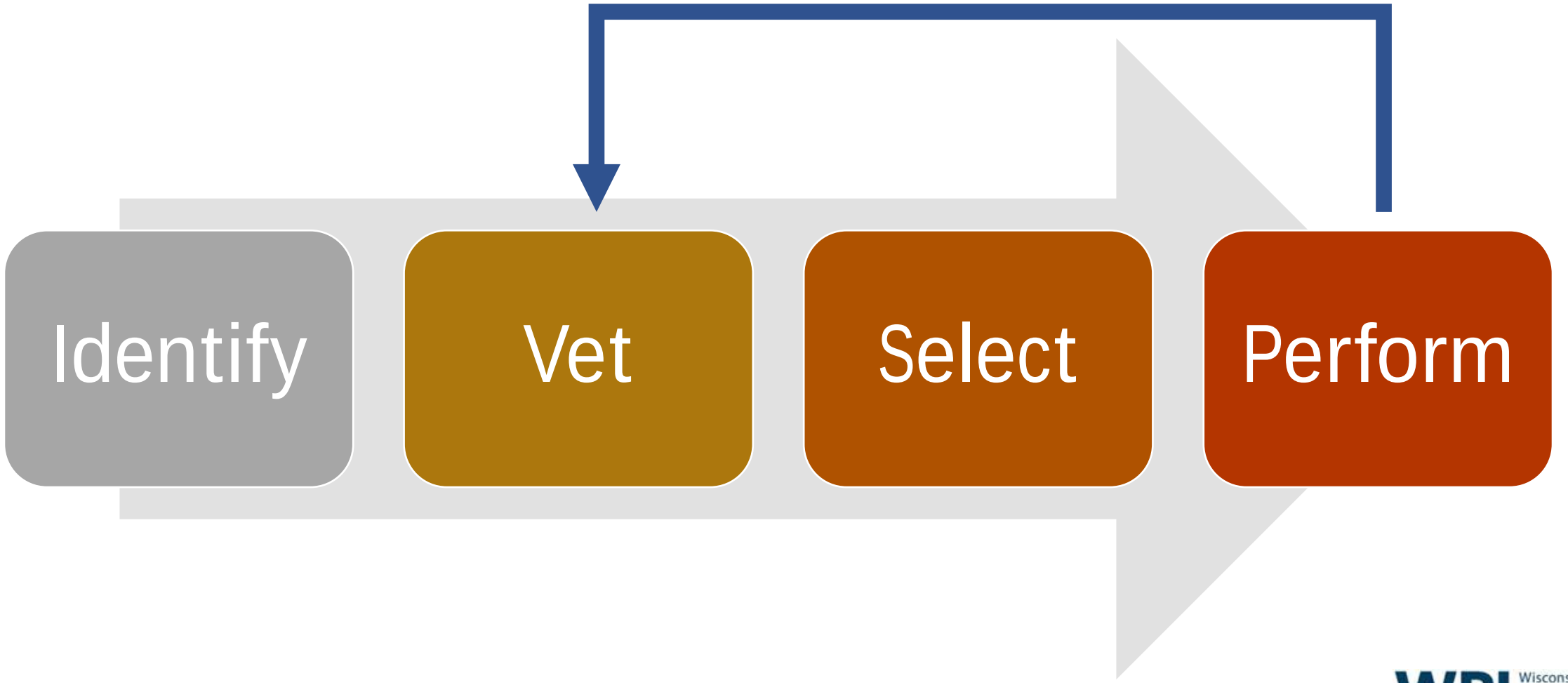
- As stated in the EO, "ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software components used within any portion of a product[1]" is a central driver behind many flagship initiatives like the SBOM.

Executive Office of the President. (2021). Executive Order 14028 on Improving the Nation's Cybersecurity. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

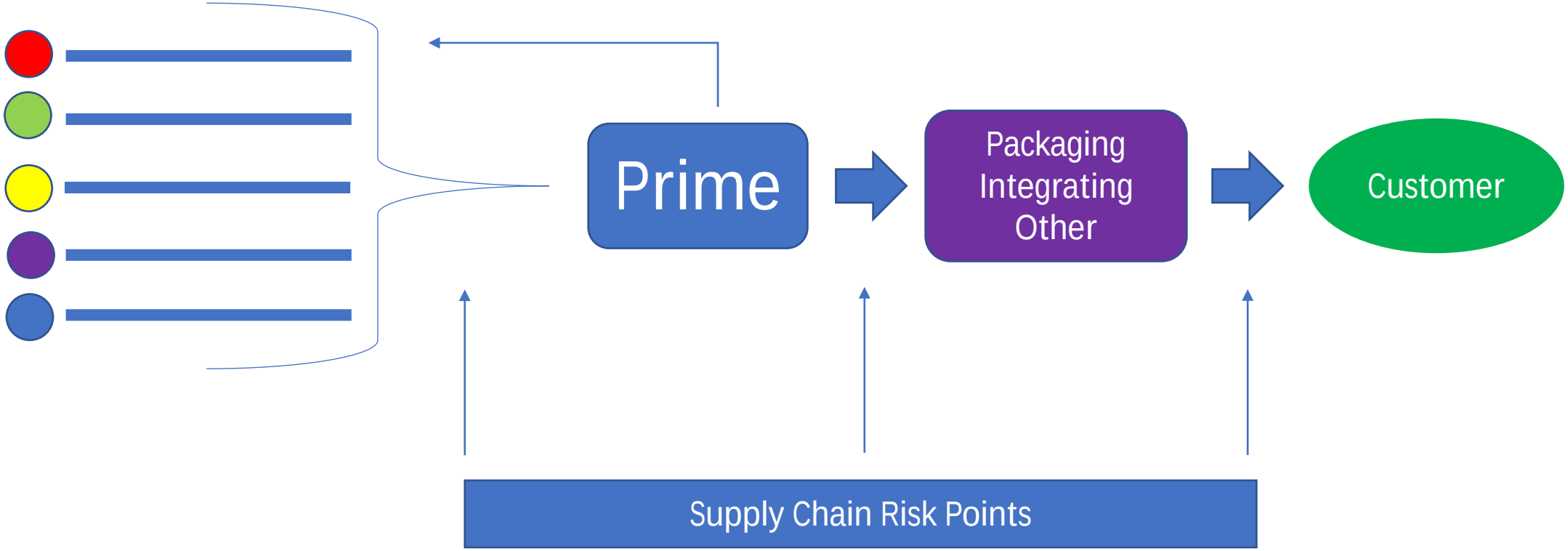
Supply Chain Risks

- Vendor selection/dependence
- Mistake/Accident
- Procedure
- Training (insufficient/general v. tailored)
- Insider threat
- Theft – piracy
- Cyber – intrusion; ransomware
- Counterfeit

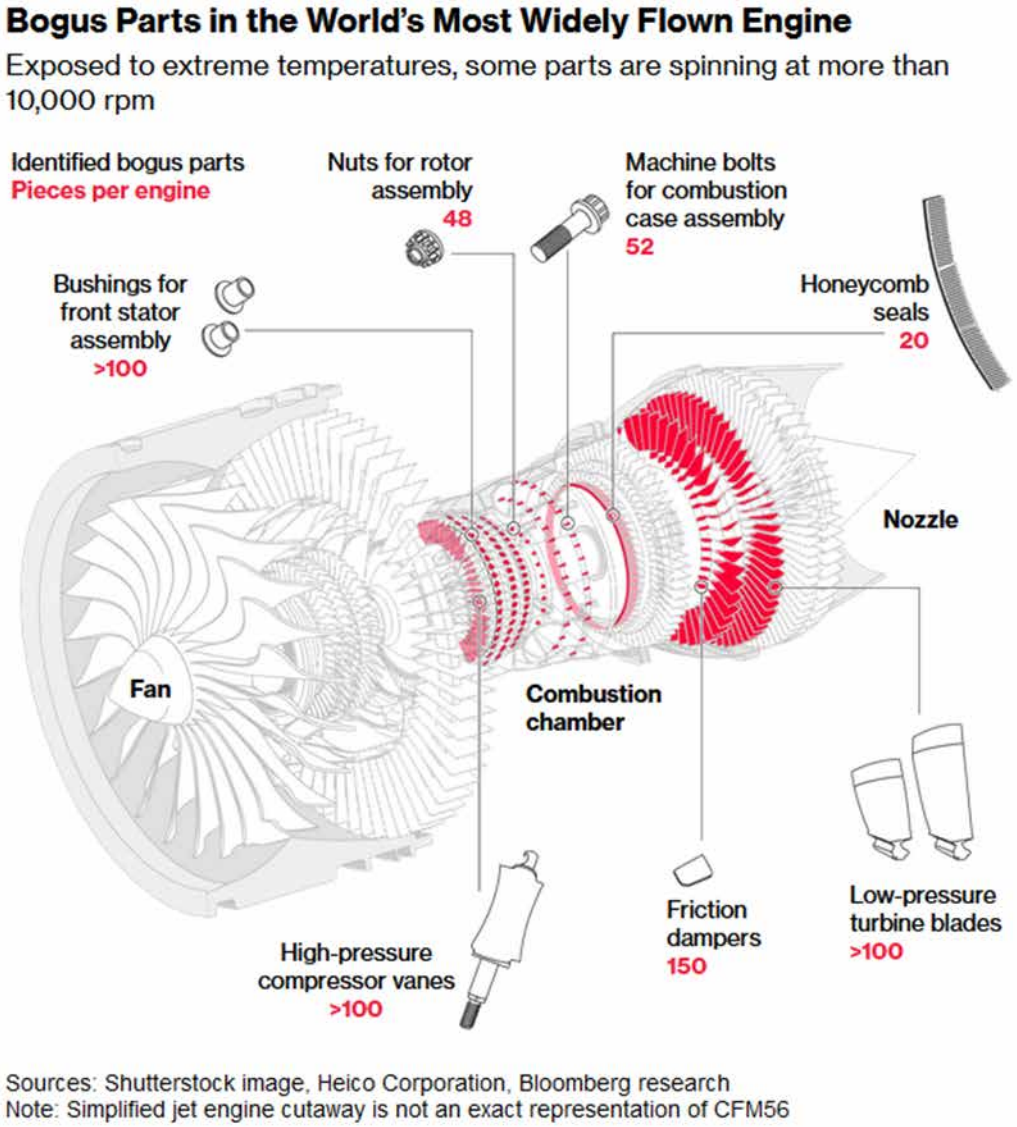
Business partner vetting



Resource Selection



Supply Chain Security



https://www.bloomberg.com/news/features/2023-10-11/fake-parts-found-on-boeing-airbus-jets-plague-airlines

Supply Chain Risk – entry points

To date, Safran and GE have uncovered more than 90 other certificates that had similarly been falsified. Bogus parts have been found on 126 engines, and all are linked to the same parts distributor in London: AOG Technics Ltd., a little-known outfit started eight years ago by a young entrepreneur named Jose Alejandro Zamora Yrala.

https://www.bloomberg.com/news/features/2023-10-11/fake-parts-found-on-boeing-airbus-jets-plague-airlines

Supply Chain Risk

Air Warfare

Pentagon suspends F-35 deliveries over Chinese alloy in magnet

By **Stephen Losey**

Sep 7, 2022

https://www.defensenews.com/air/2022/09/07/pentagon-suspends-f-35-deliveries-over-chinese-alloy-in-magnet/

Awareness & Compliance – all levels

In a release Wednesday, Lockheed Martin said a magnet in the F-35's Honeywell-made turbomachine — an engine component that provides power to its engine-mounted starter/generator — was recently discovered to have been made with cobalt and samarium alloy that came from China.

Lockheed said the alloy for this part is magnetized in the United States.

Company spokeswoman Laura Siebert said magnets on F-35s already delivered will not be replaced with magnets made from non-Chinese materials because the Pentagon has decided the magnets are safe for flight and do not put sensitive program information at risk.

Two lessons

But due to a concern about compliance with the Defense Federal Acquisition Regulation Supplement, or DFARS, the F-35 Joint Program Office has ordered the Defense Contract Management Agency to stop accepting F-35s for now.

Lockheed Martin said that, going forward, turbomachine production will use magnets made from another alloy using materials from the U.S.

Defense contractor sentenced to prison for providing fraudulent parts to military

COLUMBUS, Ohio – A California man was sentenced in U.S. District Court in Columbus today to three months in prison for committing crimes related to supplying the military with faulty parts.

Timothy W. Foley, 72, was also ordered to pay restitution of more than $1.3 million.

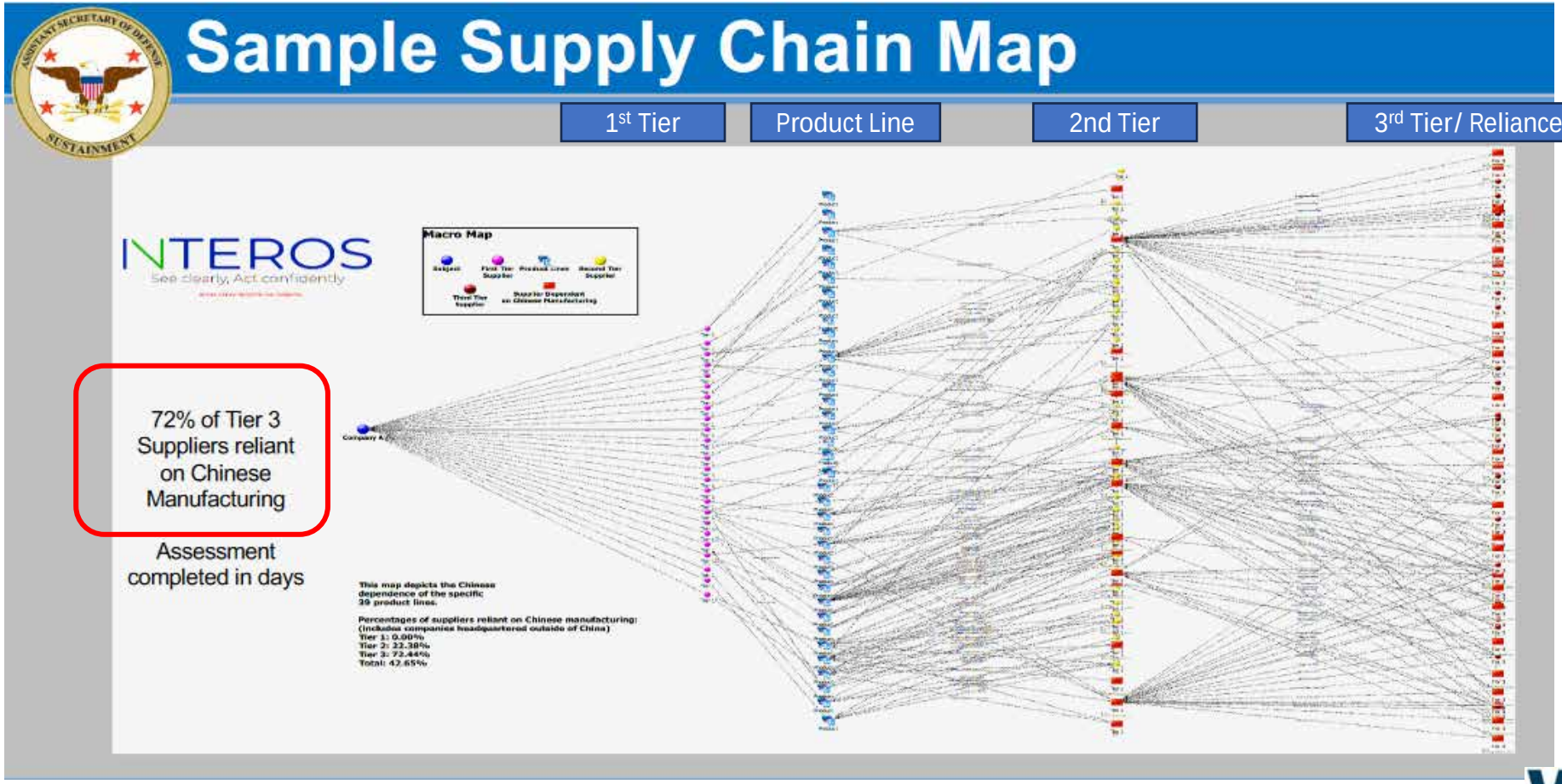
According to court documents, Foley was the operator and co-owner of Parts Source International Inc. in Goleta, California. Parts Source was a Department of Defense contractor who sold and supplied a variety of military parts to the DoD for use on military weapons systems, and some of which were critical application items, and invoiced the Defense Finance and Accounting Service (DFAS) in Columbus, Ohio, for payment.

Foley admitted that from 2012 through 2019, he conspired to supply non-conforming parts to the DoD. Foley submitted 131 quotes for purchase orders that stated he would provide the exact product as required by the government. Rather, as testing and documents revealed, Foley provided unapproved substitutions in fraudulent packaging rendering them unacceptable for use by the military.

Parts Source received a total of approximately $1.36 million in payments for the parts. Foley pleaded guilty in November 2022 to conspiring to commit wire fraud and to money laundering.

https://www.justice.gov/usao-sdoh/pr/defense-contractor-sentenced-prison-providing-fraudulent-parts-military

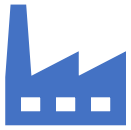
Need to understand the supply chain



Supply Chain Risk Management (SCRM), Ms. Jan Mulligan, ODASD(Logistics), Director of Supply, May 15, 2019, slide 9

Wisconsin Procurement Institute

Chinese Dependencies – break down



72% of Tier 3 suppliers reliant on Chinese Manufacturing

Tier 1 – 0.00%

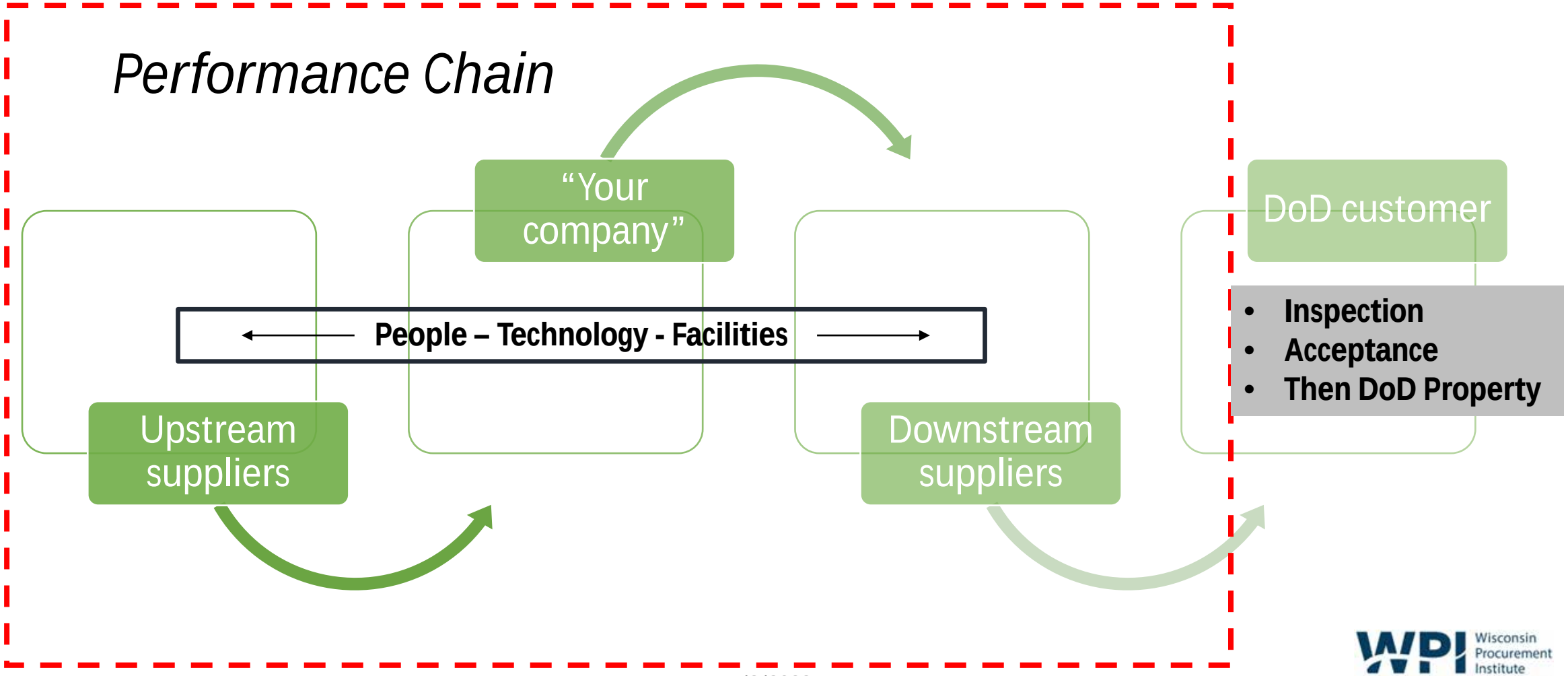
Tier 2 – 22.38%

Tier 3 – 72.44%

Total – 42.65%

Supply Chain Risk Management (SCRM), Ms. Jan Mulligan, ODASD(Logistics), Director of Supply, May 15, 2019, slide 9

Key Idea – Security concerns



Non-manufacturing Rule – (creates risk)

- Essential elements - ideas
  - Procurement coded under Manufacturing NAICS code
  - Purchase from a small business, thresholds apply
  - Take ownership in accordance with industry practices
  - Perform

Exact product - definition

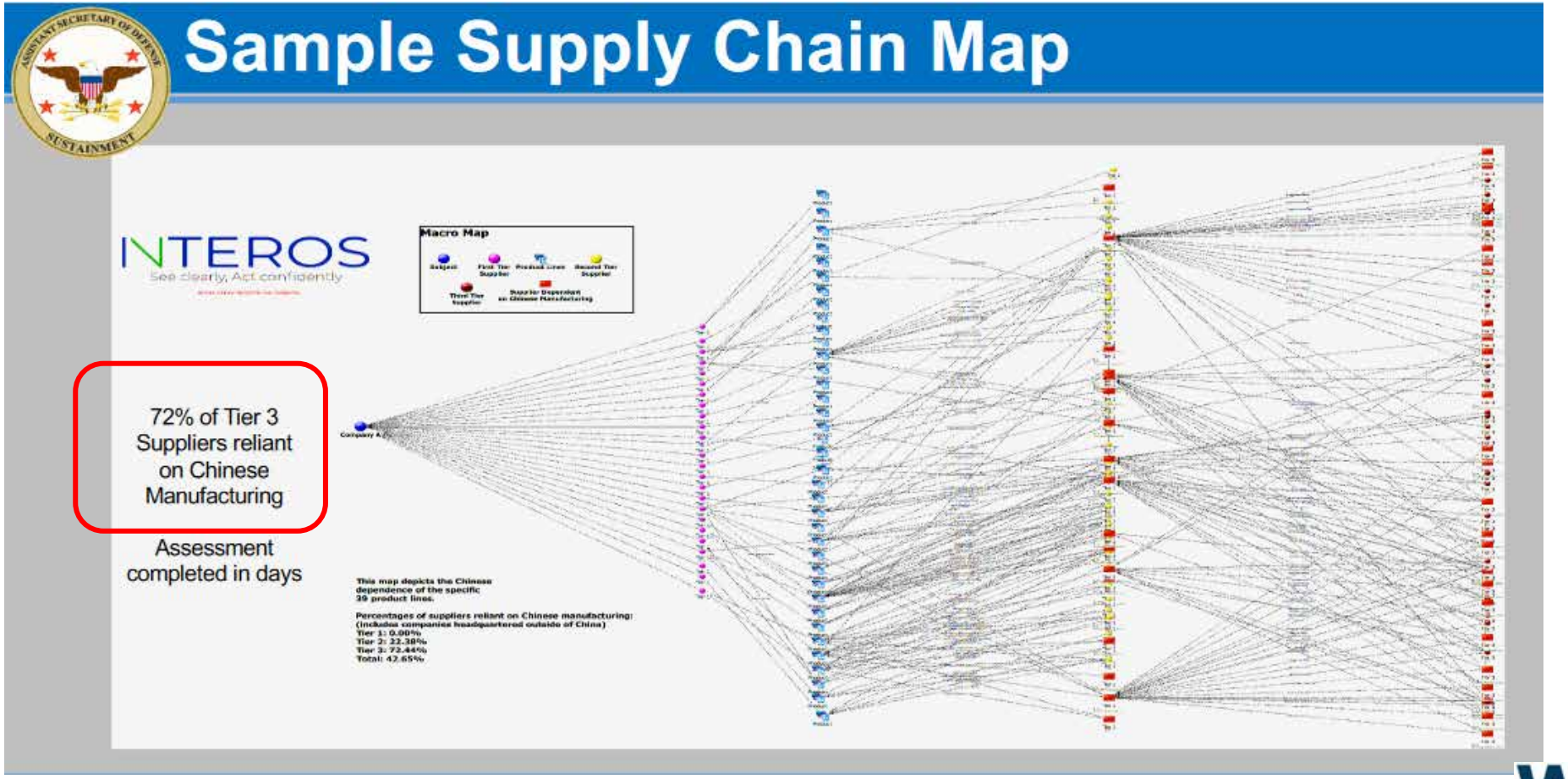
- The DLAD states –

- Exact product means a product described by the name of an approved source and its corresponding part number cited in the item description; and manufactured by, or under the direction of, that approved source. An offeror of an exact product must meet one of the descriptions below.
  (1) An approved source offering its part number cited in the item description;
  (2) A dealer/distributor offering the product of an approved source and part number cited in the item description;
  (3) A manufacturer who produces the offered item under the direction of an approved source; and has authorization from that approved source to manufacture the item, identify it as that approved source's name and part number, and sell the item directly to the Government.
  (4) A dealer/distributor offering the product of a manufacturer that meets the description in subparagraph (3) above.

Additionally, the DLAD states –

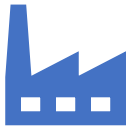
If the offeror is an authorized dealer/distributor, or manufactures the item for an approved source, a copy of the contractual agreement with, or the express written authority of, the approved source to buy, stock, repackage, sell, or distribute the part. The agreement must specifically identify the exact item, or otherwise ensure that the offeror is authorized by the approved source to manufacture or distribute the exact item being acquired. If the agreement covers a general product line or is otherwise not product-specific, the offeror must furnish additional documentation to address the exact item being acquired.

Need to understand the supply chain



Supply Chain Risk Management (SCRM), Ms. Jan Mulligan, ODASD(Logistics), Director of Supply, May 15, 2019, slide 9

Chinese Dependencies – break down



72% of Tier 3 suppliers reliant on Chinese Manufacturing

Tier 1 – 0.00%

Tier 2 – 22.38%

Tier 3 – 72.44%

Total – 42.65%

Supply Chain Risk Management (SCRM), Ms. Jan Mulligan, ODASD(Logistics), Director of Supply, May 15, 2019, slide 9

Operations Security

- Operations Security (OPSEC) is a systematic process to preserve friendly essential secrecy by identifying, controlling and protecting critical information and indicators that would allow adversaries or potential adversaries to identify and exploit friendly vulnerabilities. DLA must be ever vigilant when handling logistics information and must protect it at all times, especially when interacting with its vendor network. *Each DLA organization maintains Critical Information and Indicators Lists that identify unclassified but sensitive information that must be protected from disclosure.*

Defense Logistics Agency Supply Chain Security Strategy, page 6

Protecting Sensitive Data

Much of DLA's data is sensitive in nature.

For example –

- Military specifications and standards,
- Technical data packages (TDP),
- Schematics,
- Customer delivery destinations
- Many other forms of exportable data
  -- subject to exploitation if in the wrong hands.

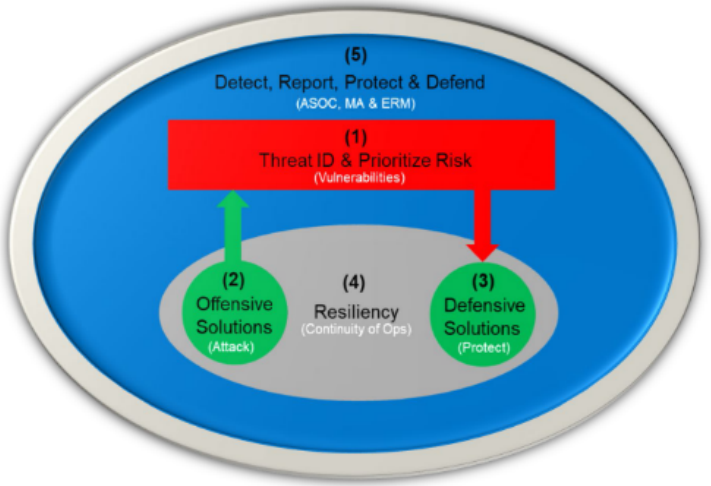
Defense Logistics Agency Supply Chain Security Strategy, page 5

Supply Chain Security Strategy – Money Chart

Grand Strategy

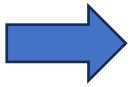
DLA's Supply Chain Security Strategy was designed to develop an **Enterprise Architecture** that …

(1) Identifies & reports threats, vulnerabilities & prioritizes risk
(2) Develops offensive solutions to minimize threats
(3) Develops defensive solutions to protect vulnerabilities
(4) Infuses resiliency into sys's, processes, infrast & people
(5) Prevents disruption thru detection, protection & defense



Proactive
Awareness
Action orientated
Resiliency focus

Supply Chain Security Strategy – Money Chart



Strategic Focus Areas

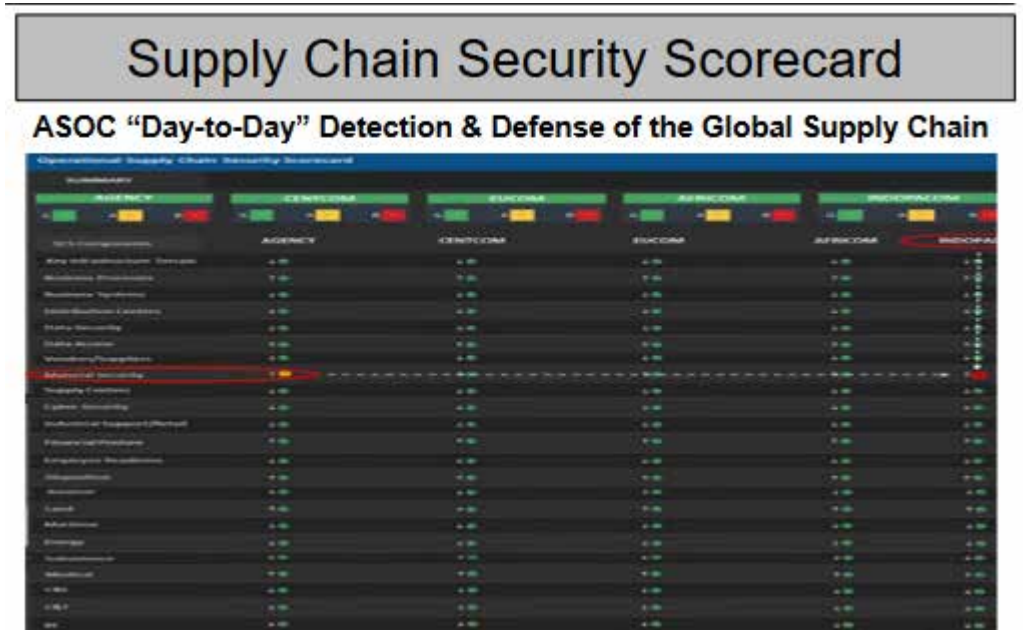
To develop the Enterprise Architecture, DLA will concentrate on four **Strategic Focus Areas**

(1) Institutionalize Supply Chain Security throughout DLA
(2) Maintain integrity & access to key data
(3) Partner with valid & reputable vendors
(4) Strengthen resiliency of sys's, processes, infrast & people

Resiliency!

Strategic Focus Areas are "**strategy bins**" that house supply chain security-related initiatives that are mapped to objectives in the Agency's **Strategic Plan**. The initiatives put the strategy in motion by actuating the Strategic Focus Areas for the purpose of developing the architecture.

Supply Chain Security Strategy – Money Chart



Executive Order on America's Supply Chains

- Section 1. Policy.
- The United States needs resilient, diverse, and secure supply chains to ensure our economic prosperity and national security.
- Pandemics and other biological threats, cyber-attacks, climate shocks and extreme weather events, terrorist attacks, geopolitical and economic competition, and other conditions can reduce critical manufacturing capacity and the availability and integrity of critical goods, products, and services.
- Resilient American supply chains will revitalize and rebuild domestic manufacturing capacity, maintain America's competitive edge in research and development, and create well-paying jobs.
- They will also support small businesses, promote prosperity, advance the fight against climate change, and encourage economic growth in communities of color and economically distressed areas.

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/

CLEARED FOR OPEN PUBLICATION 15 Feb 2023

Supply Chain Risk Management Framework

Project Report – Phase I

https://www.acq.osd.mil/log/LMR/.scrm_report.html/DoD_SCRM_Framework_Report_Phase_I.pdf

Industry and Academia Session Notes - Culture

Culture will be the hardest thing to change within the Department of Defense and with our Industry counterparts. The DoD can no longer do acquisition the way it has always been done – because the DoD must determine where they are vulnerable early during the design phase and plan the design and the supporting supply chain to be resilient despite these vulnerabilities.

- Culture = supply chain risk; a company's cultural and risk appetite.
- Culture tends to be associated with the prime and not the sub-tiers.
- Supply Chain Risk Management (SCRM) is considered overhead and eats at a company's profit. Therefore, there is no incentive to address this concern.
- Every action is charged to a cost accounting code. SCRM will be viewed as added cost.
- How the Department of Defense buys is how the primes will behave.
- How I do my ordering is very different than what parts are designed into the system.

DoD - Supply Chain Risk Management Framework – page A-1

Governance and Oversight

Governance and oversight are key functions that include management, standards, statutes, regulations, and decision makers. As the DoD continues to emphasize supply chain resiliency, vulnerabilities, and risk management, ensuring that good policy is published to provide clear roles, responsibilities and processes will be key to the successful implementation.

- There are three categories of governance: management, accountability and taking an enterprise approach. This includes the people and framework with highly trained workforce who know their supply chains.
- Supply chain risk management must be built into the beginning of the acquisition process. When you are designing the item, review vendor profiles through a score key of how likely they will perform, review on-time deliveries, quality of product, etc.
- Decisions made by a centralized group, engineers, and PMs.
- Use of Standards. AS 9100 clearly defines risk management procedures that are closely integrated. This helps organizations ensure they meet customer and other stakeholder needs within statutory and regulatory requirements related to a product or service. But other companies should be adhering to these standards as well.

DoD - Supply Chain Risk Management Framework – page A-1

Supply Chain Resiliency vs Supply Chain Risk Management

Organizations frequently conflate supply chain resiliency with supply chain risk management, using the terms interchangeably. However, SCR does not equal SCRM. Equating the two definitions demonstrates a lack of awareness about the complexities of supply chains, further, organizational naiveté about the differences between the two terms inhibits strategic decision making. It is difficult to find employees that understand the differences between resiliency and risk; these terms are generally not part of traditional purchasing, or supply chain curriculums. Supply Chain resilience is the capacity to persist, adapt and transform. Vulnerabilities and associated risk are omnipresent in supply chains. These vulnerabilities must be identified with assigned risk and developed plans to overcome supply chain failures. As a result of complex and dynamic supply chains, organizations must constantly review their supply chains, update the vulnerabilities and associated risk, and develop plans to make them resilient.

DoD - Supply Chain Risk Management Framework – page A-2

Vulnerability vs Risk

When considering supply chain sources of risk, it may not always be apparent where that risk lies, and thus organizations should analyze and identify vulnerabilities within supply chains for such things as single-sourced components, or shared sourcing of components across multiple OEMs. Once an organization understands where its areas of most value, and risk, reside, it can work to develop mitigation plans.

- When viewed as individual product supply chains, each product has its own story, perhaps with points of aggregation, but the individual nature necessitates examining each product uniquely. Evaluate products to assess the most critical to prioritize; not all products carry the same level/types of risk. Product lines with higher reputational risk have priority - in order to maintain trust. This prioritization helps segment the portfolio.
- Vulnerability must consider normal market variations vs. disruption. Where are you vulnerable? Where do you have single sources? Normal market variation is managed and matured; however, vulnerabilities are key. Which materials are high risk? Where is an organization the most vulnerable? What are the single sources of failure?

DoD - Supply Chain Risk Management Framework – page A-2

The Airport(s)

Rather than assessing the risks, a method to assess vulnerabilities, is to assume you've already lost supply chain availability, and then you can start quantifying impacts. Knowing your vulnerabilities in advance can help create resilience; understanding how vulnerable you are before a disaster occurs changes profile of risk. For example, a vulnerability assessment of a large network, like an airport, introduces risk. Significant product volumes travel through specific airports. If something happens to a critical airport, then how products get distributed to customers? In this example, transportation has vulnerabilities that would need to be considered - with identification of alternative solutions. These solutions need to be in alignment throughout the supply chain.

DoD - Supply Chain Risk Management Framework – page A-2

Metrics

Metrics must be a corporate mandate aligned at executive level and part of management measures.

Metrics to consider:

- Define core data needed
- Focus on qualifying suppliers
- Monthly audits
- Quality standards
- On-time deliveries
- Business continuity impact metrics and forecasting likelihood of risk
- Dependency mapping

Visibility is important Supply chain intelligence – application of tools that can depict supply chain nodes, maps, ever stream analytics, risk methods, geospatial mapping of supply chain.

DoD - Supply Chain Risk Management Framework – page A-2

Other Strategic Takeaways

Keep it simple, keep it focused, build a coherent strategy, and be very practical on what you can take on.

Sometimes an organization must pick up the phone and talk to other companies (competitors) even though there is a concern over competitive advantage, organizations must work together as a team.

- There are multiple tier 1's contracting to the same tier 2 - which creates a diamond shaped supply chain. This creates huge concentrations at the tier 2 level no matter how much companies try to prevent it; they cannot mask it and it is possible to learn something from the near misses.

DoD - Supply Chain Risk Management Framework – page A-7

“Who is observing”

- Timescales are important. Vigilance is needed to watch what is happening across the world over time; things are shifting very slowly, who is observing? Vigilance equals National security – perception that there is no coordinated vigilance in the country. Vigilance is the price of economic security.

DoD - Supply Chain Risk Management Framework – page A-7

Terms used

- Supply Chain Risk
- Supply Chain Risk Management
- Supply Chain Resiliency

DoD - Supply Chain Risk Management Framework – page A-2

Missing Key Standards

ISO 28000: Supply Chain Security Management System

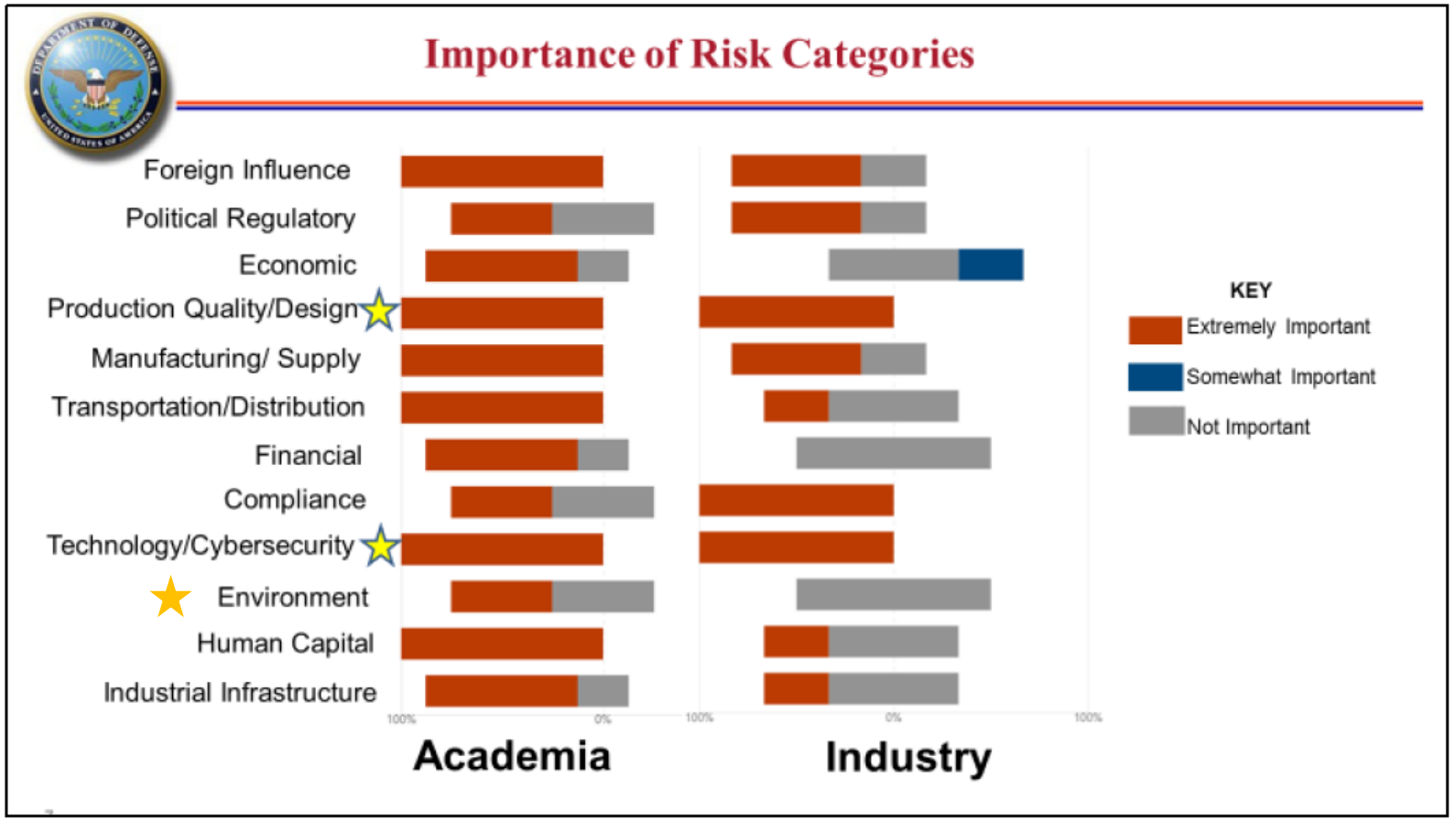
ISO 28002: Security Management Systems for the Supply Chain – Development of Resilience in the Supply Chain

ISO 31000: Risk Management

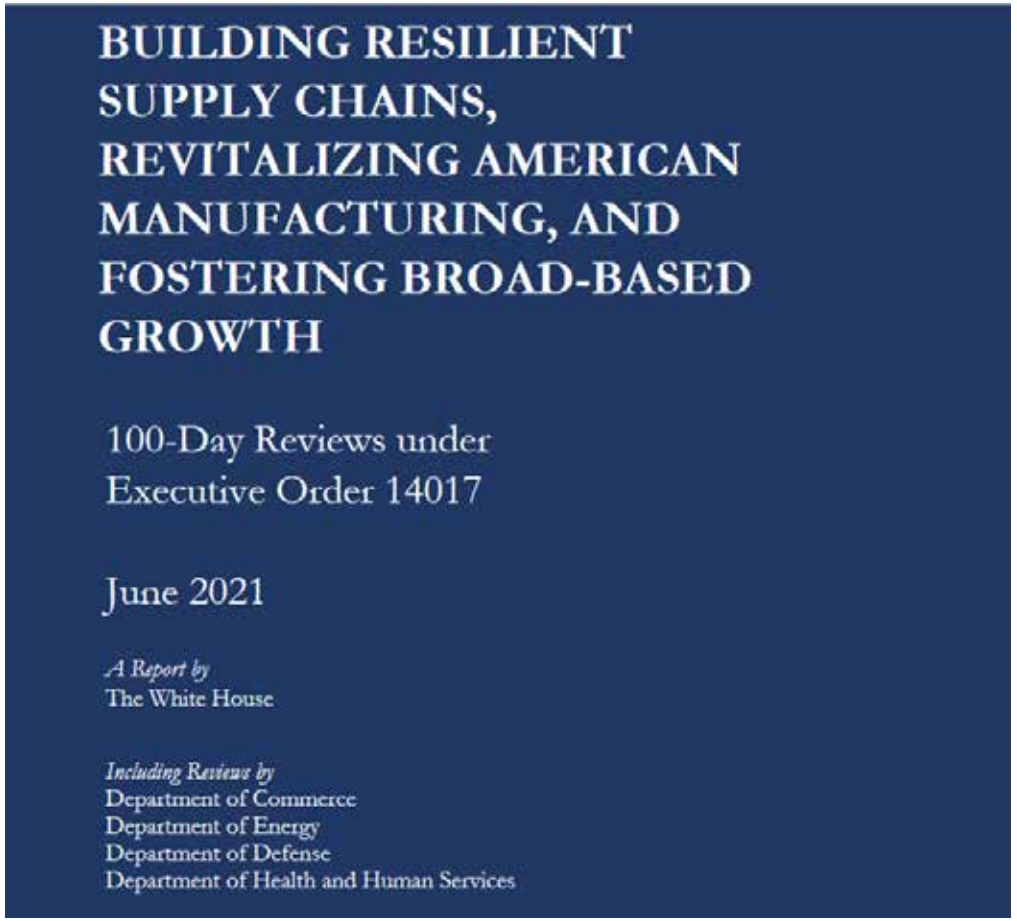
ISO 73: Risk Management Vocabulary

AS 9100: Quality Systems - Aerospace - Model for Quality Assurance in Design, Development, Production, Installation and Servicing

Importance of Risk Categories



Resilient Supply Chains



https://www.bis.doc.gov/index.php/documents/technology-evaluation/2958-100-day-supply-chain-review-report/file

Proposed definitions

Supply Chain Resilience (SCR)	The capability of supply chains to respond quickly, so as to ensure continuity of operations after a disruption, and to quickly adapt to change. Resilience is the expected outcome of proactive Supply Chain Risk Management and Supply Chain Security.
Supply Chain Risk Management (SCRM)	The process of proactively identifying supply chain vulnerabilities, threats, and potential disruptions and implementing mitigation strategies to ensure the security, integrity, and uninterrupted flow of materials, products, and services as risks are found or disruptions occur.
Supply Chain Security (SCS)	The application of policies, procedures, processes, and technologies to ensure the security, integrity, and uninterrupted flow of products while moving through the supply chain. Examples include the ability to protect supply chains from cyber infiltrations and the introduction of counterfeit material.

DoD - Supply Chain Risk Management Framework – page C-2

Risk Categories

- Foreign Ownership Control or Influence (FOCI)
- Political and Regulatory
- Economic
- Environment
- Product Quality and Design
- Manufacturing and Supply
- Transportation and Distribution
- Financial
- Compliance
- Technology and Cybersecurity
- Human Capital
- Infrastructure

DoD - Supply Chain Risk Management Framework – page C-2

Sub-Categories

MANUFACTURING & SUPPLY	Inventory Stockout/Material Shortages
MANUFACTURING & SUPPLY	Inventory or Capacity Incidents
MANUFACTURING & SUPPLY	Industrial Capacity
MANUFACTURING & SUPPLY	Industrial Capability
MANUFACTURING & SUPPLY	Extended Lead Times
MANUFACTURING & SUPPLY	Equipment Down Time
MANUFACTURING & SUPPLY	Obsolescence/DMSMS

112 Sub-categories

DoD - Supply Chain Risk Management Framework – Appendix C

Sub-Category: Compliance - Fraud

COMPLIANCE	Fraud (Procurement and Government)	Fraudulent activities by Federal or State employees, contractors, subcontractors, or any other participants on government contracts. Suspected fraudulent activities include, but are not limited to: • falsifying information on contract proposals • using Federal funds to purchase items that are not for Government use • billing more than one contract for the same work • billing for expenses not incurred as part of the contract • billing for work that was never performed, falsifying data • substituting approved materials with unauthorized products • misrepresenting a project's status to continue receiving Government funds • charging higher rates than those stated or negotiated for in the bid or contract • influencing government employees to award a grant or contract to a particular company, family member, or friend.

DoD - Supply Chain Risk Management Framework – Appendix C

Manufacturing & Supply -- examples

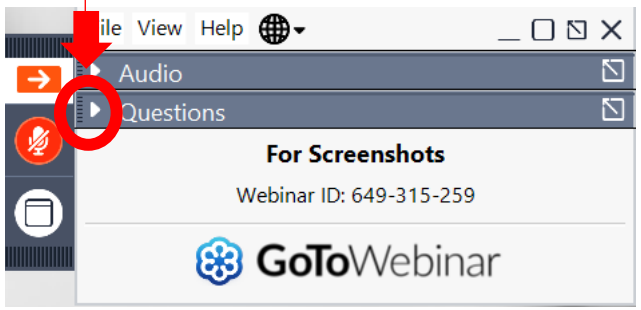
MANUFACTURING & SUPPLY	Sole Source Dependency	Only one supplier for the required item is available.
MANUFACTURING & SUPPLY	Single Source	A particular supplier is purposefully chosen by the buying organization, even when other suppliers are available
MANUFACTURING & SUPPLY	Reseller/3rd Party Vendor/Middleman	A person or company that sells something they have bought from someone else.
MANUFACTURING & SUPPLY	Reclamation/Utilization	Process to reclaim whole or essential components and materials for manufacturing either the same or alternate products. Reutilization is using components and materials for the same, similar, or differing purpose (e.g., using ships again in different missions or sinking to build reefs)
MANUFACTURING & SUPPLY	Parts/Spares Inventory Shortages	Inadequate supplies of spare parts on hand for maintenance and repairs.

DoD - Supply Chain Risk Management Framework – Appendix C

QUESTIONS?

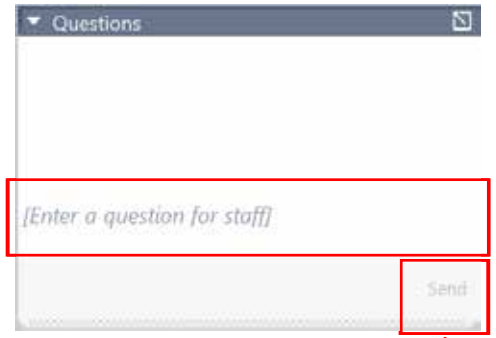
OPENING THE QUESTIONS BOX

Click here to access within the Control Panel



USING THE QUESTIONS BOX

Type questions here at any time during a presentation



Click Send when ready to submit a question

UPCOMING TRAINING - EVENTS

ACQUISITION HOUR LIVE WEBINAR SERIES

- November 8
  Preparing for One-on-One Buyer Meetings
- November 15
  Preparing a Winning Government Proposal
- November 29
  Service Contracts with Federal Agencies
- December 12
  The HUBZone Program – Certification Benefits and Regulations

…More information and registrations at wispro.org/events

GOVERNMENT CERTIFICATION WORKSHOPS

- ~~October 12~~
  ~~Federal Certifications~~
- ~~October 26~~
  ~~Local Certifications~~
- November 30
  State Certifications

MADISON AREA TECHNICAL COLLEGE

MATC Goodman-South Campus
2429 Perry Street, Madison, WI 53713

…More information and registrations at wispro.org/events

CYBER FRIDAY LIVE WEBINAR SERIES

- ~~October 27~~
  ~~NIST SP 800.171 – 3.9 Personnel Security and 3.10 Physical Protection~~

- November 3
  NIST SP 800.171 – 3.11 Risk Assessment and 3.12 Security Assessment

- November 9 (Thursday)
  NIST SP 800.171 – 3.13 System and Communications Protection and 3.14 System and Information Integrity

PRESENTED BY

WPI Wisconsin Procurement Institute
APEX Accelerators
Cyber Friday

TECHNOLOGY INNOVATION CENTER at Research Park

NCMA National Contract Management Association
WISCONSIN

Registration Now Open

The Contracting Academy

Developing and Growing Government Contractors

December 5-7, 2023

MarketplaceWisconsin.com

November 2, 2023

SURVEY

Wisconsin Procurement Institute

November 2, 2023

NCMA WISCONSIN

CONTINUING PROFESSIONAL EDUCATION

This webinar is eligible for 1 CPE credit.
For a certificate of this credit please contact:

Jack Laufenberg
jackl@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)
www.wispro.org

Marc Violante

Wisconsin Procurement Institute

marcv@wispro.org | 920-456-9990

10437 Innovation Drive Suite 320
Milwaukee WI 53226