Wisconsin Procurement Institute

An APEX Accelerator

Emerging Issues:

Vetting and securing your supply chain

June 20 | 11:00 am - Noon

Presented by:

Marc Violante, Wisconsin Procurement Institute

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

Webinar Etiquette

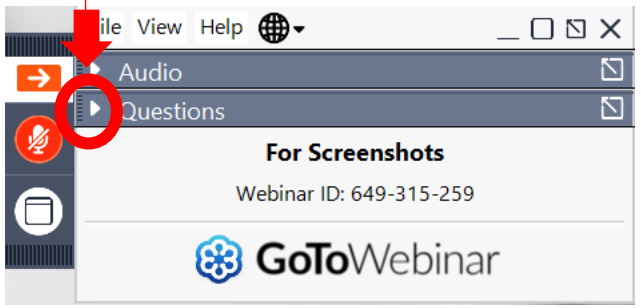
PLEASE

- 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!

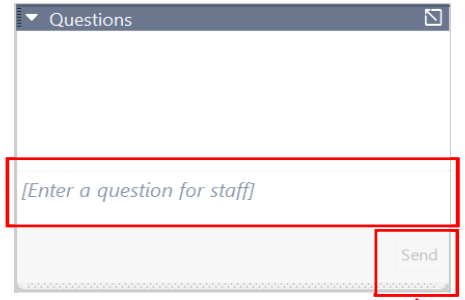
OPENING THE QUESTIONS BOX

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

An APEX Accelerator

Assisting Wisconsin businesses compete in the government marketplace.

WPI is Wisconsin's APEX ACCELERATOR

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.

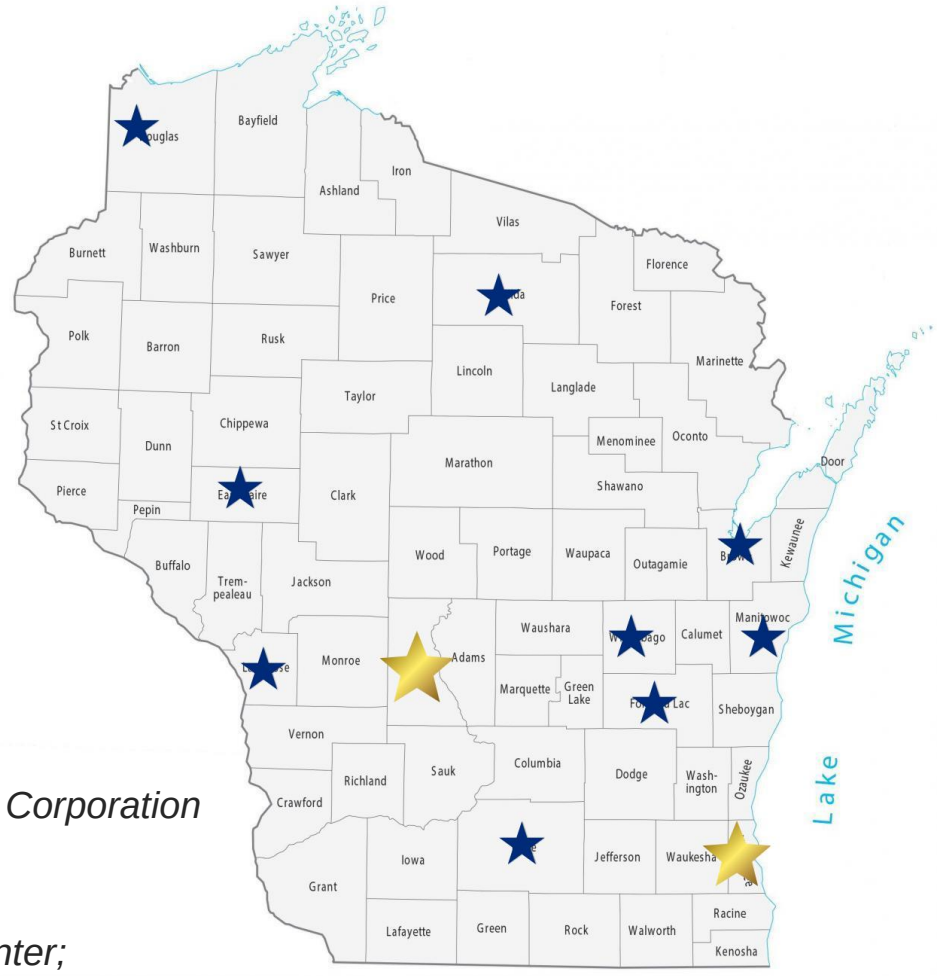
WPI provides services to all of Wisconsin's 72 counties

- 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……

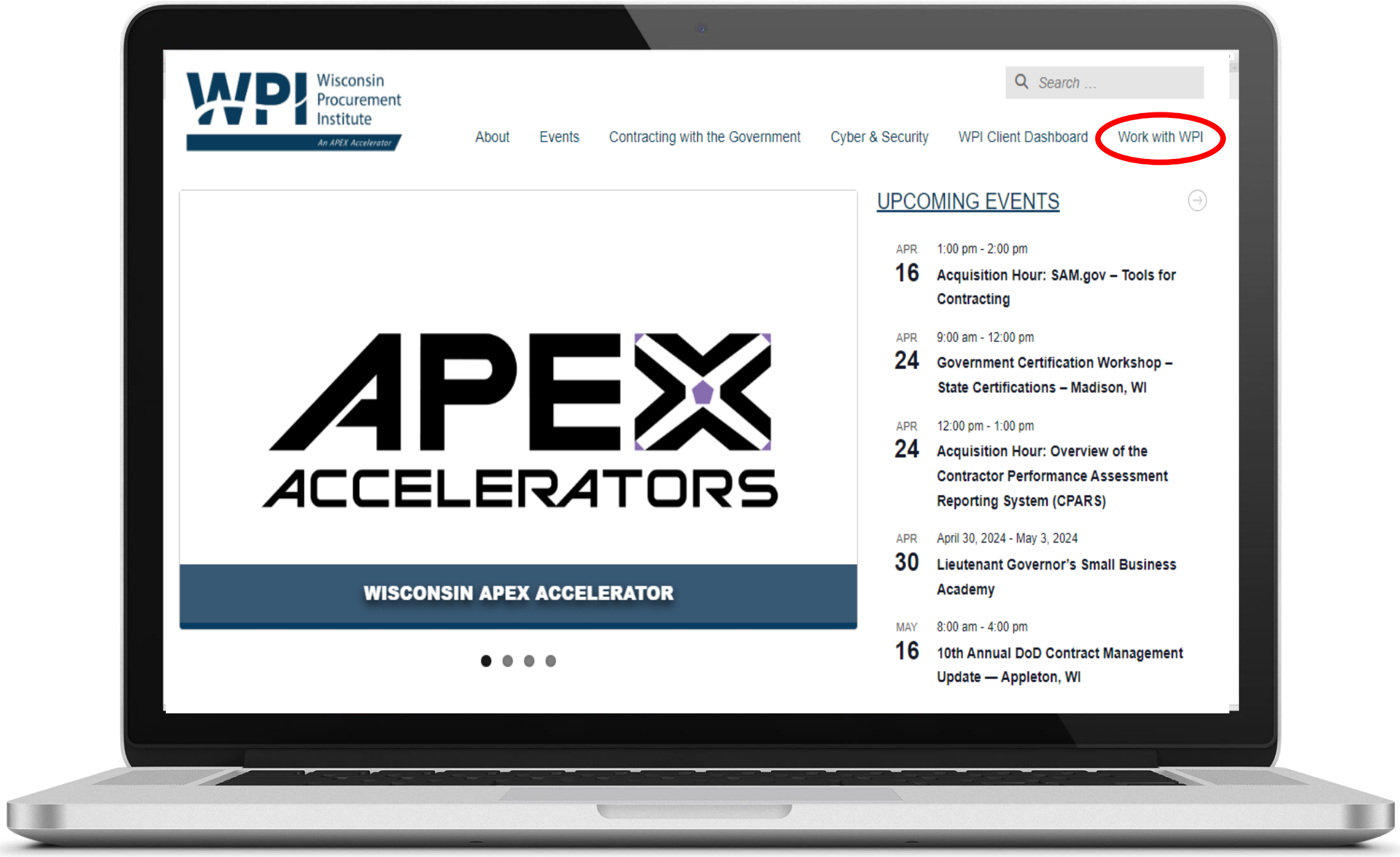
www.wispro.org

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)*
- **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*
- **SUPERIOR**
  - *Small Business Dev Center; UW Superior*



Wisconsin Procurement Institute
An APEX Accelerator


WPI Wisconsin Procurement Institute
An APEX Accelerator
Search ...
About
Events
Contracting with the Government
Cyber & Security
WPI Client Dashboard
Work with WPI
APEX ACCELERATORS
WISCONSIN APEX ACCELERATOR
UPCOMING EVENTS
APR 16 1:00 pm - 2:00 pm
Acquisition Hour: SAM.gov – Tools for Contracting
APR 24 9:00 am - 12:00 pm
Government Certification Workshop – State Certifications – Madison, WI
APR 24 12:00 pm - 1:00 pm
Acquisition Hour: Overview of the Contractor Performance Assessment Reporting System (CPARS)
APR 30 April 30, 2024 - May 3, 2024
Lieutenant Governor's Small Business Academy
MAY 16 8:00 am - 4:00 pm
10th Annual DoD Contract Management Update — Appleton, WI

Vetting and Securing Your Supply Chain

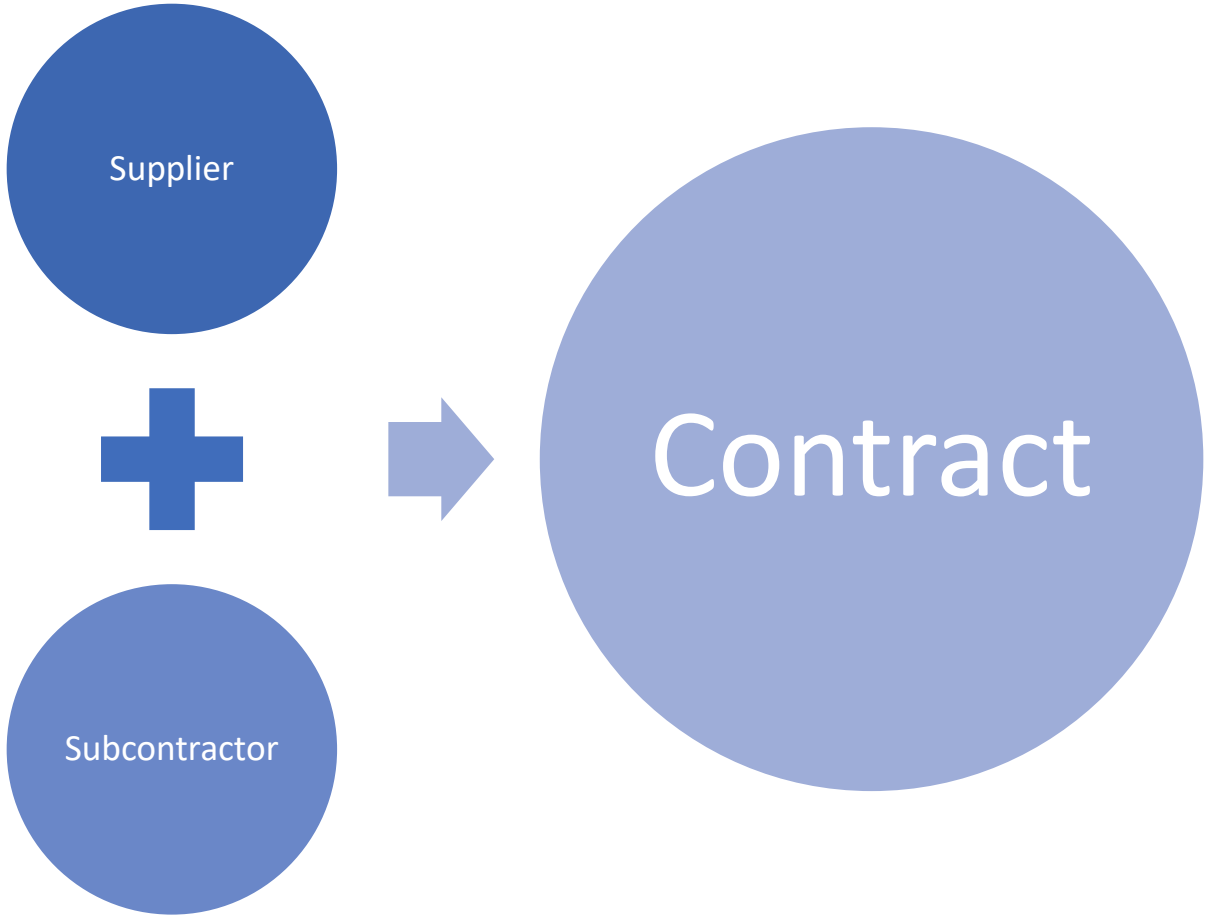
Marc N. Violante

Wisconsin Procurement Institute

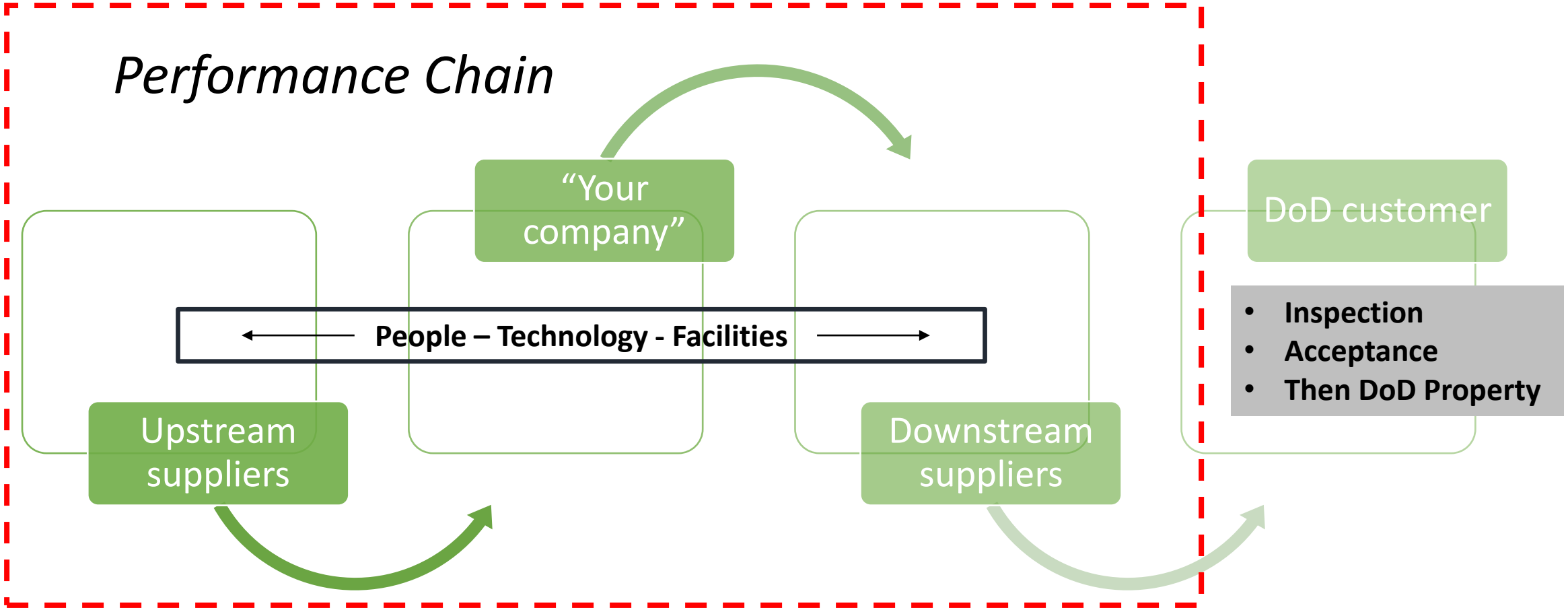
June 20, 2024

Wisconsin Procurement Institute
An APEX Accelerator

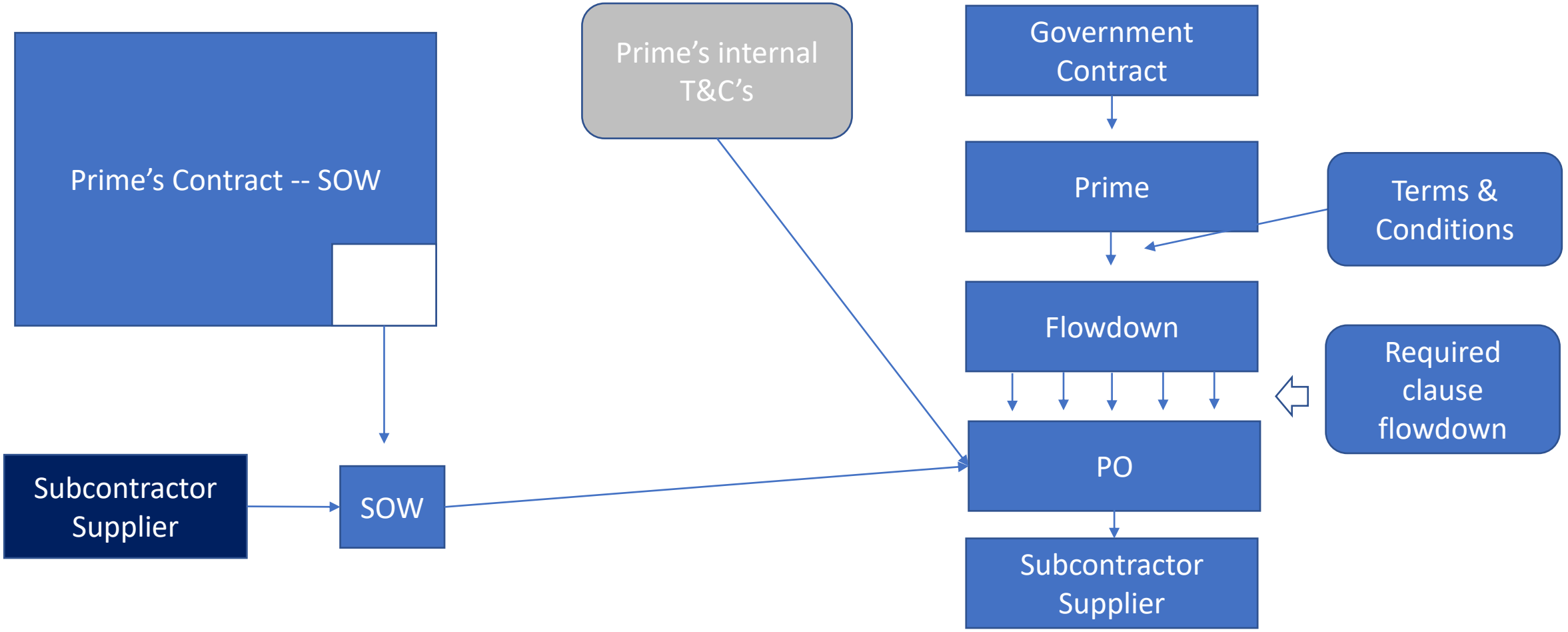
Don’t oversimplify the supply chain



Define – Understand the totality of your chain



Functions of a Subcontracting agreement



Supply Chain Elements

Figure 5. Supply Chain Elements

Defense Logistics Agency Supply Chain Security Strategy, page 7

Supply Chain Interdependencies & Threats

Supply Chain Risks - Macro

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

Risk Categories

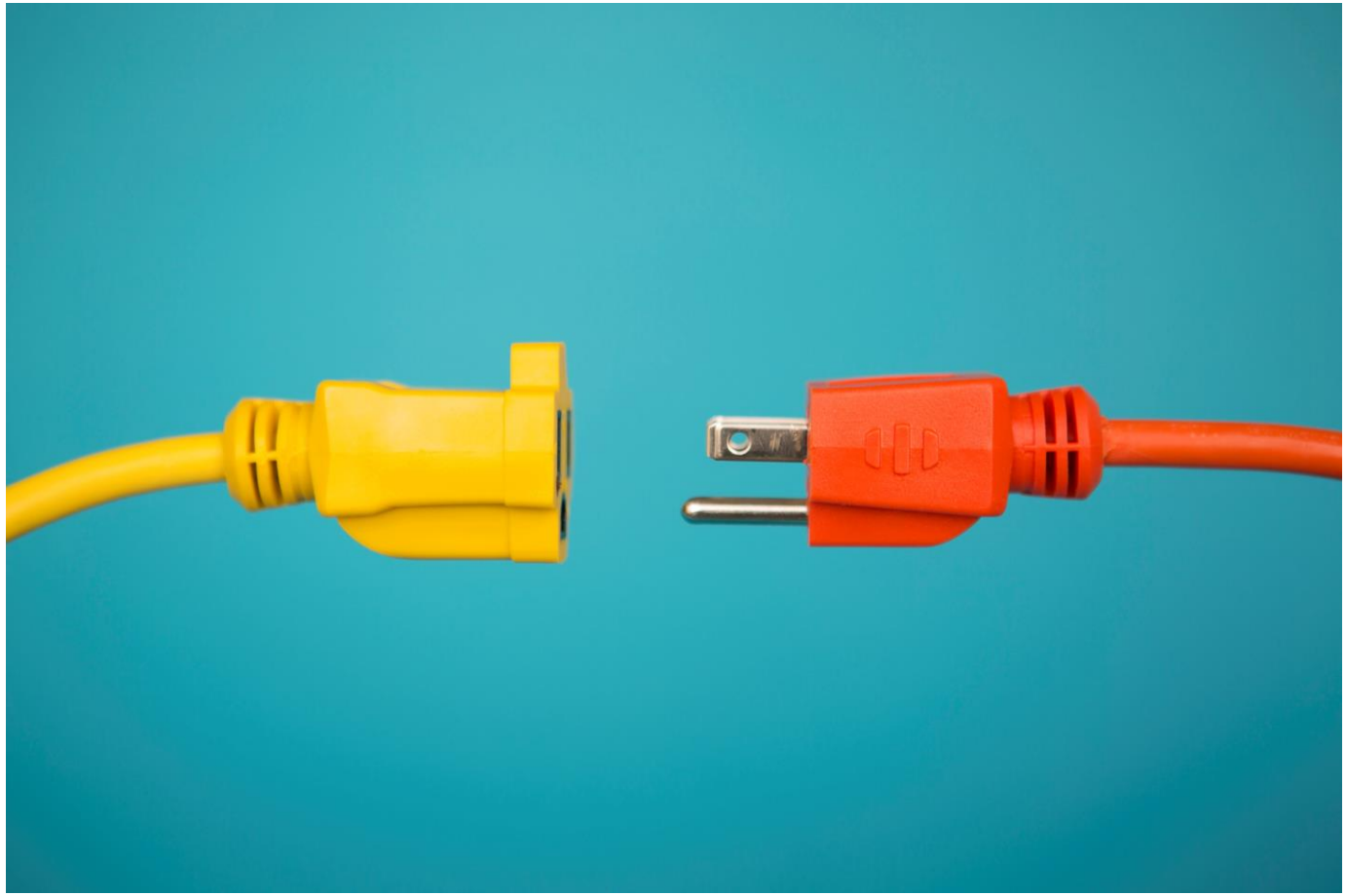
- Foreign Ownership Control or Influence (FOCI)
- Political and Regulatory
- Economic
- Environment
- Product Quality and Design
- Manufacturing and Supply
- Transportation and Distribution
- Financial
- Compliance
- Technology and Cybersecurity
- Human Capital
- Infrastructure

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

Identify Supply Chain Risks - specific

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

Knowledge of Vulnerabilities & Risks



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

Awareness - the first requirement

- Quality, price, and on-time performance remain important factors to consider when identifying and selecting subcontractors and suppliers.
- Changes to cybersecurity requirements have established new regulations and, consequently, concerns that must be addressed.
- Companies need to know about these requirements. Then conversations need to be open, frank and recurring with subcontractors and suppliers.
- Vetting needs to include all of the information, processes and procedures used to get to know members of your supply chain and to ensure that they are eligible from a regulatory standpoint.
- These efforts should include a thorough review of first tier supply chain members but also to understanding how mandatory requirements will be “flowed down,” managed and tracked at sub-recipient levels.

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

The character of war is changing.

- Our adversaries no longer have to engage the United States kinetically. They have shifted their strategy to engage our nation *asymmetrically*, exploiting the seams of our democracy, authorities, and even our morals. They can respond to a kinetic action non-kinetically and often in misattributed ways through *blended operations* that take place through the supply chain, cyber domain, and human elements. They can render our national capability to project power—hard or soft—non-mission ready and collapse and collapse and even reverse the decision cycle.

https://ciri.illinois.edu/events/supply-chain-security-asymmetric-era

Deliver Uncompromised

- "Today our adversaries may have a better understanding of our strategic vulnerabilities than do we. This includes vulnerabilities introduced via networks or through the supply chain. This is because of poor/inadequate intelligence on such threats, excessive compartmentation that precludes effective sharing of such threat information, lack of prioritization, and widespread availability of information in the public domain."

- MITRE Report, 8 Aug 2018, Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War

DLA's Strategic Focus

This document carves a path forward for the Agency to follow in pursuit of strengthening operational resiliency across the enterprise. The strategy within it anchors to the fundamental elements of Supply Chain Risk Management (SCRM) and Mission Assurance. I need every DLA member to understand this strategy and to support it wherever you may fit in because supply chain disruption is not an option for the Warfighter. With each of us synchronized on supply chain security, together we can thwart disruption by strengthening operational resiliency.

https://www.dla.mil/Portals/104/Documents/Headquarters/StrategicPlan/SupplyChainSecurityStrategy.pdf

DLA – “risk management”

- A third initiative within this Strategic Focus Area optimizes the use of cybersecurity as a discriminator in source selections and awards to ensure DLA conducts business with vendors who take appropriate action to protect DoD sensitive data and information.
- PARTNER WITH VALID, REPUTABLE VENDORS WHO PRODUCE QUALITY SUPPLIES & SERVICES
- DLA uses a decision support tool called Business Decision Analytics (BDA) to analyze nearly 1 million bids a day to help mitigate procurement risk. BDA is part of a suite of tools that use machine learning, predictive variables, multiple data sources and advanced analytics to help make informed material and purchasing decisions by evaluating supplier, solicitation, price and item risk. BDA helps DLA mitigate risk when making material and purchasing decisions.

https://www.dla.mil/Portals/104/Documents/Headquarters/StrategicPlan/SupplyChainSecurityStrategy.pdf, page 7

DLA – partner actions/concerns

- The purpose of the third Strategic Focus Area is to ensure that the vendors DLA partners with produce high-quality materiel for the Warfighter.
- The accompanying initiatives are heavily focused on **preventing counterfeit and non-conforming parts from entering** into DLA's Global Supply Chain.
- With well established processes in-place to ensure DLA partners **with valid and reputable vendors**, fraudulent exploitation still exists given the sheer volume of purchases, business transactions and the automation required to support them.
- Further complicating this is the complexity of **sub-vendor relationships** that support DLA's primary vendor base.
- **DLA has limited insight into these relationships** which often times have several upstream providers, foreign dependencies and a multitude of potential entry points for counterfeit and non-conforming parts to enter into DLA's Global Supply Chain.

Defense Logistics Agency Supply Chain Security Strategy, page 6

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/

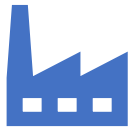
Awareness & Compliance – all levels

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.

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

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

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

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

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.

- 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.

How much do you really know about your supply chain?

- What information do you have?
- What information do you want but lack?
- What questions do you ask?
- How frequently do you contact supply chain members?
- Are members identified with respect to information & importance?
- Are supply chain members casual, tactical or strategic?
- What information is required to be shared?
- Are there any types of agreements? – data sharing, etc?

The “handshake” informal business dealings

- Issues: may be overlooked, not considered
  - Ownership
  - Knowledge of requirements
  - Appropriate cybersecurity
  - Data (information) security
  - Compliance

Defining awareness …

- Kindred spirit to Awareness is –
  - Thoughtfully and completing reviewing requirements
  - Digesting – understanding the requirements
  - Assembling references
  - Reviewing references and identifying applicable sections
  - Comparing requirements with internal processes and procedures
  - Identifying gaps
  - Specifying resource requirements
  - Prioritizing actions
  - Gaining formal corporate “buy-in” and support
  - Initiation
  - Feedback
  - Establishing processes and procedures
  - Records and training – internal/external

Beware of Confirmation Bias

- What is better?
  - To seek “Yes” and overlook what’s missing
  - To find “No’s” correct those discrepancies and develop a system that creates a strong “Yes?

Example: A prime is looking to subcontract to a small machine shop for work related to a DoD contract. The prime searches SAM and doesn’t find a registration. The prime knows that it cannot require the small business to register in SAM as a requirement to receive the subcontract (FAR 19.703 (a)(2)(iii)).

Question: Is the lack of being registered in SAM a problem and why?

All the blocks are checked – now what?

- ✓SAM
- ✓JCP
- ✓ITAR
- ✓DoD Basic Assessment

Is the compliance

- Mechanical
- Checkmark
- Spirit and Intent

Does it matter?

How do you differentiate?

FOCI

INFORMATION HANDLING

CYBERSECURITY

SOFTWARE

MANAGING UPDATES

QUALITY, PRICE, DELIVERY

CONTRACT COMPLIANCE

Determine scope and applicable criteria

- Does one size fit all?
- The goal should be to limit data shared to the minimum
- The recipient should endeavor to minimize the “spread” of the data once received
- Data (information) should not be shared on “the hope of safe-guarding”
- Determine if the data will need to be shared downstream.
- Understand the subcontractor’s data sharing policies and philosophies

Information Sharing – just one consideration

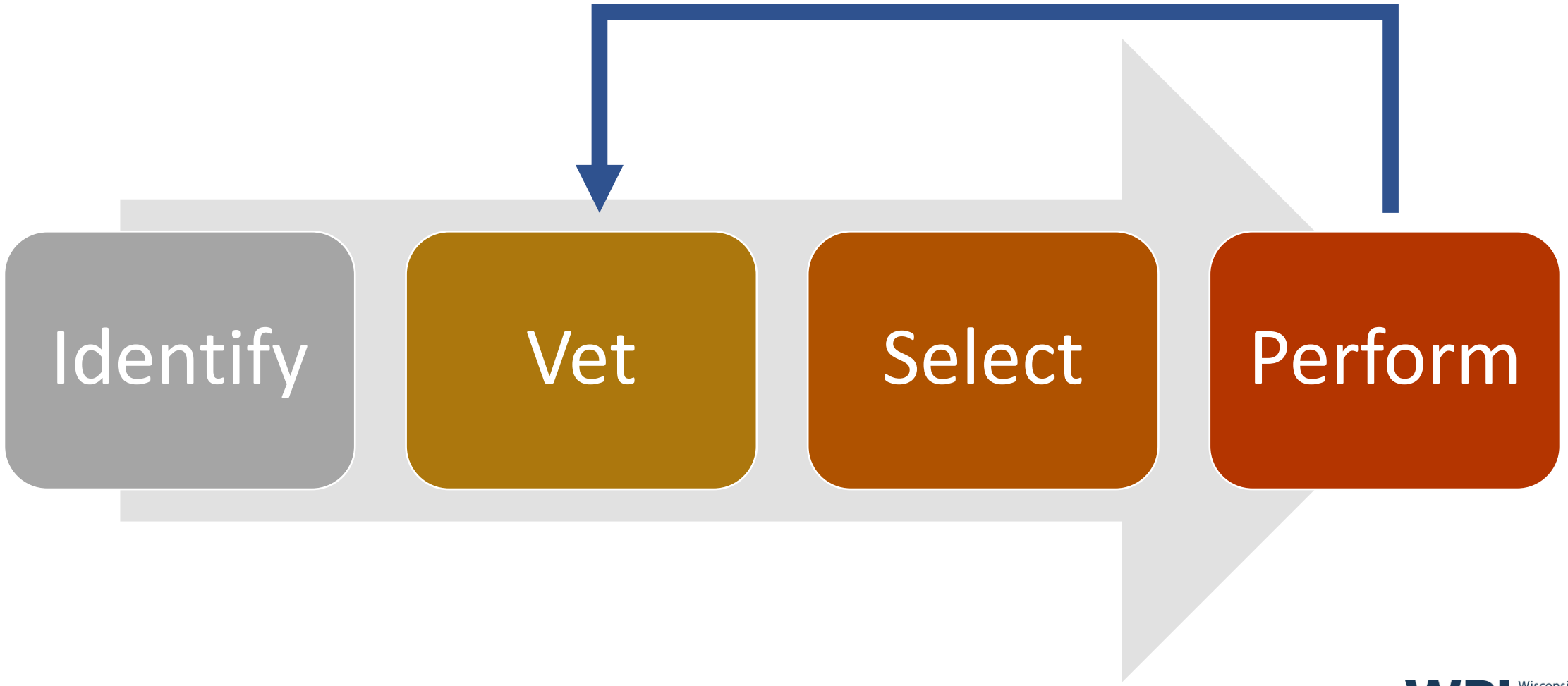
- Contractor Support Agreements
- Subcontractor/Supplier Information Sharing Agreement
  - Validate NIST Basic Assessment/JCP/CUI
  - Periodic drills
  - Inspections
  - Scans
  - Exercises
- Communication is required within/among supply chain members
  - discuss information security, sharing, reporting and incident response

DAU Webinar, September 22, 2020; Request for Information/ Proposal (RFI/RFP) Contract Strategy Considerations to Implement the CMMC, slide 4 & comments

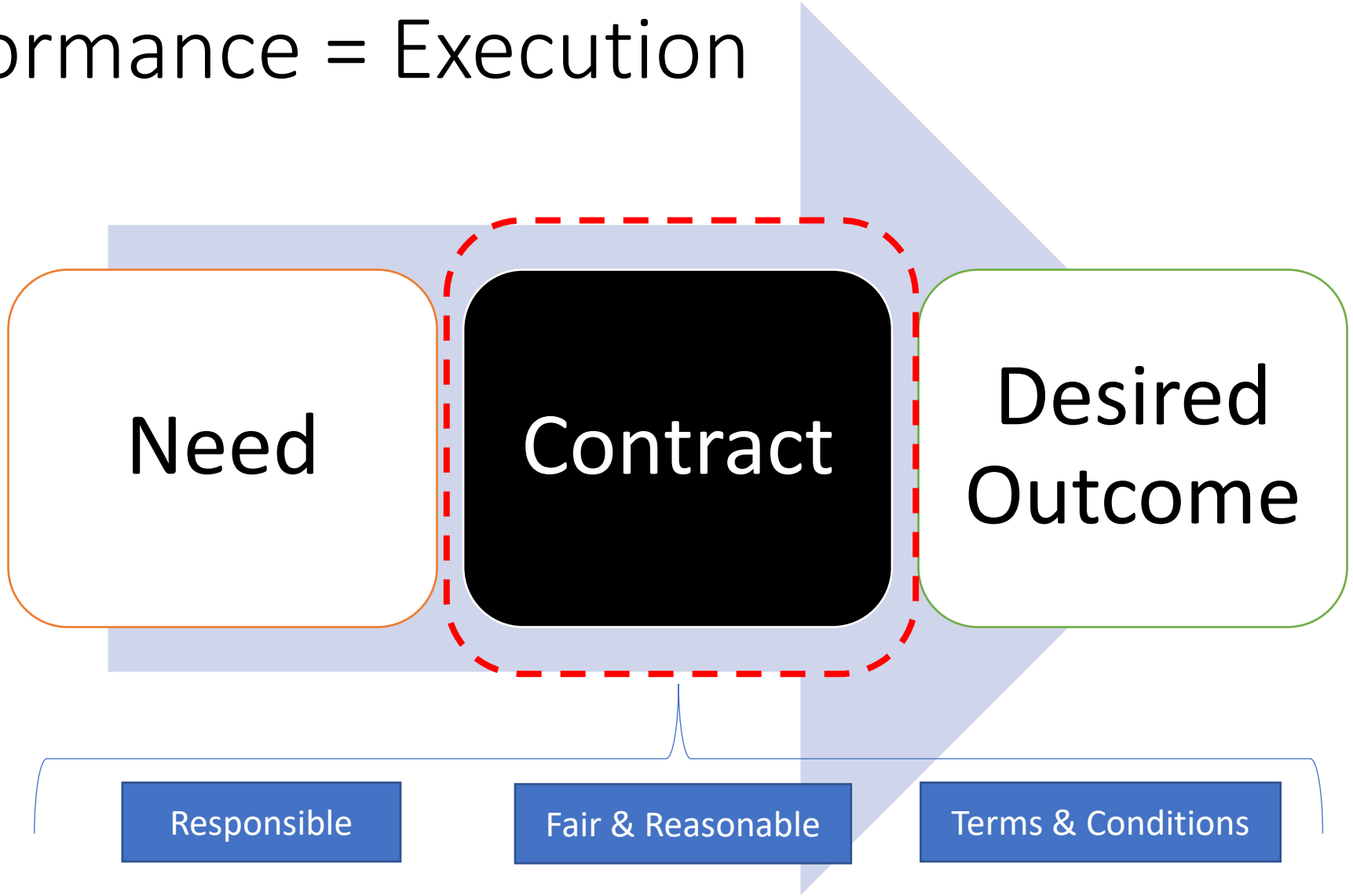
Partners – Knowing & Communicating

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

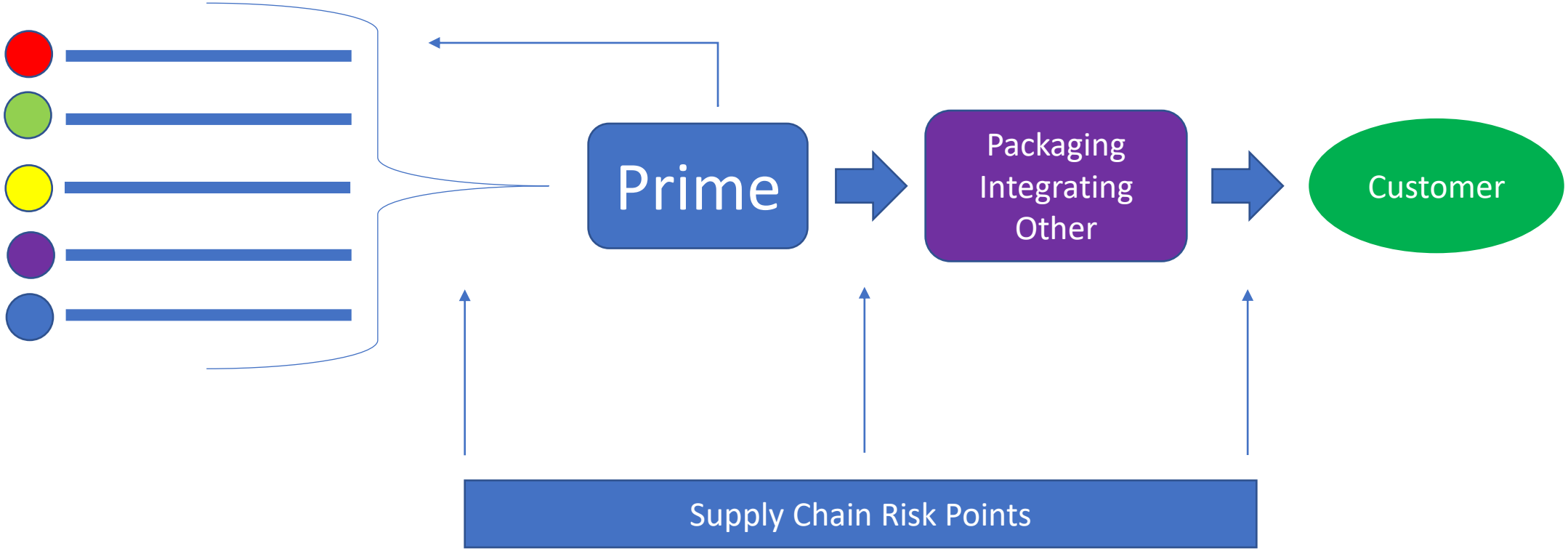
Business partner vetting



Performance = Execution



Resource Selection



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

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 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

Evaluation - strategies

- Who will conduct?
- Consistency
- Questionnaire
- Site Visit
- Interviews
- Attend training
- Evaluate – assess the next tier
- As an alternative
  - Ask about their supply chain
  - How do they identify subcontractors/suppliers?
  - How do they vet these companies?

Identify general Risk Vectors

- Facility
- Network
- Policies
- Staff
- Subcontractors
- Suppliers
- Vendors
- Visitors

Determine – “who are you doing business with?”

- Current security philosophy/posture – Basic (required) or better* (enhanced)
- Designation of Company Information Security Officer or equivalent
- Ownership, Control, Foreign Investors
- Keeping current
- References use – maintained
- Determination of Governmental Purpose
- Minimizing access
- Handling of Export-Controlled information
- Awareness and Management of CTI
- Understanding of requirements – details
- Storage capability
- Ability to decontrol – destroy various information types (disposition)
- Publication requirements/procedures

Develop a Risk Profile

- Information type
  - JCP | ITAR | CUI | Other
- Review of company web site
- Review of select policies
- Performance metrics – quality / on-time
- Leadership involvement
- Responsiveness
- Training documentation
- Turn-over key positions

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

Supplier agreements – presence & use of

- What notification requirements should be required?
  - Key staff –
    - Move/departure/hires
  - Interest in purchase/investing
  - Unusual requests for information – external – non-federal
  - Changes in key supplier/subcontractor
  - Changes in cyber-security status – supplier/subcontractor
  - Requirement for periodic testing of cyber-incident response plan
  - Maintenance of an active DoD Medium Assurance Certificate
  - Acknowledgement of the ability to capture a forensic network image IAW DFARS 252.204-7012

Formally adopt plans & policies

- Board approval
- CEO/President date, signature, revision
- Establish controls
  - Change
  - Version
  - Distribution
  - Responsibility
  - Edits/corrections/updates
  - Test – it sounds good; does it work?
  - List of effect pages - LOEP

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.

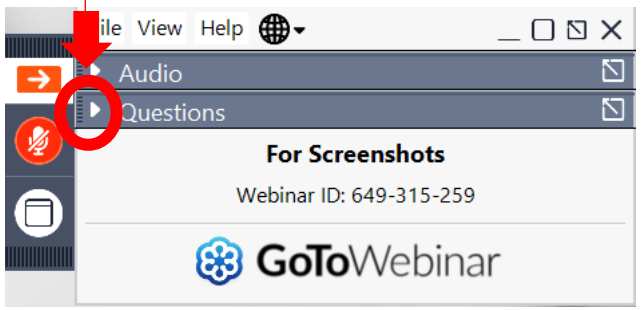
- There are multiple tier 1's contracting to the same tier 2 - which creates a diamond shaped supply chain. This creates huge concentrations at the tier 2 level no matter how much companies try to prevent it; they cannot mask it and it is possible to learn something from the near misses.

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

QUESTIONS?

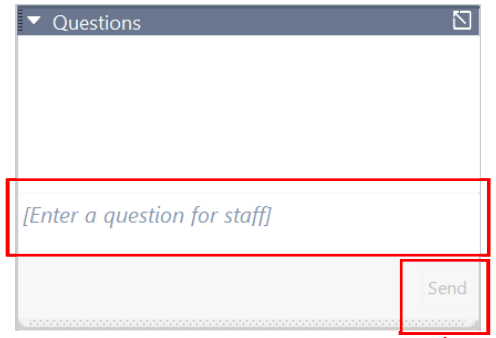
OPENING THE QUESTIONS BOX

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

Wisconsin Procurement Institute
An APEX Accelerator

June 20, 2024

NCMA
NATIONAL CONTRACT MANAGEMENT ASSOCIATION
WISCONSIN

CYBER FRIDAY LIVE WEBINAR SERIES

Cyber Friday is a series of one-hour webinars focusing on critical topics for DOD contractors and subcontractors in cyber security, data security, and CMMC. Attendees receive 1 CPE credit for attending.

- **June 21,** 3.1.2 Security Awareness Training, Role-Based Training, and Insider Threat Training
- **July 19,** 3.1.3 Audit and Accountability Policy, Log Review Procedure
- **August 23,** 3.1.4 Configuration Management Policy, Change Request Process, Baseline Configurations
- **September 20,** 3.1.6 Incident Response Policy, Incident Response Plan
- **October 18,** 3.1.7 System Maintenance Policy
- **November 22,** 3.1.8 Media Control Policy, Media Destruction Policy and Personnel Security
- **January 24,** 3.1.11 Risk Assessment Policy, Security Assessment Reports

WPI Wisconsin Procurement Institute
An APEX Accelerator

…More information and registrations at wispro.org/events

EMERGING ISSUES WEBINAR SERIES

This series is intended as an information tool and resource for contract managers and those with a compliance function. Attendees receive 1 CPE credit for attending.

- **June 20** – Vetting and Securing Your Supply Chain
- **July 25** – Beyond contracts: Conducting Business with the Federal Government
- **Aug 22** – Regulation Making – The Process and the Important Role Businesses Play
- **Sep 19** – Industry 4.0 – The Next Generation of the DIB
- **Oct 24** – Innovation – What Does Innovation Look Like from DoD's Perspective?
- **Nov 21** – The Critical Role Your Accounting System Plays in SBIR/STTR Success

WPI Wisconsin Procurement Institute
An APEX Accelerator

…More information and registrations at wispro.org/events

18th Annual Wisconsin Government Opportunities Business Conference (GOBC)

In Partnership with Wisconsin's Military Installations

July 10

Truax Field

GOBC will provide you the opportunity to gain insights into:

- *COFFEE with the COMMANDER*
- Current operations and priorities at Wisconsin's Federal and State government agencies and military facilities
- Connecting with agency and installation leadership, operational staff and buyers
- Locating and bidding on current and future procurement opportunities
- Resources available to assist your business in winning government prime and subcontracts

…More information and registrations at wispro.org/events

WPI Wisconsin Procurement Institute
An APEX Accelerator

NCMA National Contract Management Association
WISCONSIN

- Save the Date -

The Contracting Academy

Developing and Growing Government Contractors

Dec 10

Virtual | 9:00 am - 4:00 pm

The Contracting Academy (TCA) is an opportunity for businesses to grow their technical knowledge of contracting with Federal Government, State/Local Government, and Government Prime Contractors. The series of workshops will benefit established businesses looking to grow and develop their government sales.

…More information and registrations at wispro.org/events

WPI Wisconsin Procurement Institute
An APEX Accelerator

NCMA National Contract Management Association
WISCONSIN

NDIA
Great Lakes

15th NDIA Great Lakes Chapter Annual Meeting

July 24, 2024

10:00 am – 5:00 pm

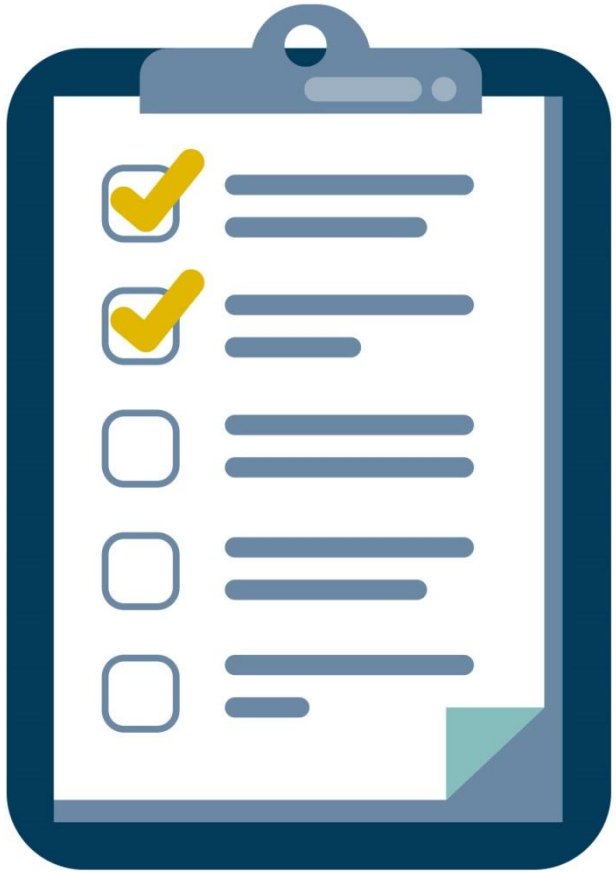
Itasca, IL

Guest Speaker: Matthew Travis, Ceo, Cyber-AB

WPI Wisconsin Procurement Institute
An APEX Accelerator

…More information and registrations at wispro.org/events

SURVEY



Wisconsin Procurement Institute
An APEX Accelerator

June 20, 2024

NCMA
NATIONAL CONTRACT MANAGEMENT ASSOCIATION
WISCONSIN

CONTINUING PROFESSIONAL EDUCATION

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

Neelu Patil
neelagangap@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