Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

CYBER FRIDAY: SECURING THE SUPPLY CHAIN – "NO MAN IS AN ISLAND"

Cyber Friday Webinar

December 4, 2020




ABOUT WPI
SUPPORTING THE MISSION

Celebrating 32 Years of serving Wisconsin Business!

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

Assist businesses in creating, developing and growing their sales, revenue and jobs through Federal, State and Local Government contracts.

- **INDIVIDUAL COUNSELING – At our offices, at client's facility or via telephone/GoToWebinar**
- **SMALL GROUP TRAINING – Workshops and webinars**
- **CONFERENCES to include one on one or roundtable sessions**

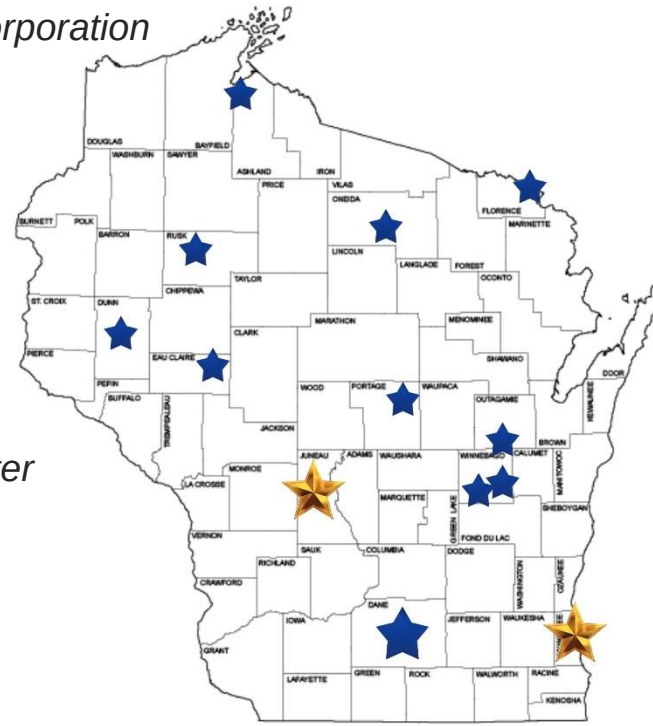
Last year WPI provided training at over 100 events and provided service to over 1,200 companies

WPI is a Procurement Technical Assistance Center (PTAC) funded in part by the Defense Logistics Agency (DLA), WEDC and other funding sources.

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

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)*
- **STEVENS POINT**
  - *IDEA Center*
- **APPLETON**
  - *Fox Valley Technical College*
- **FLORENCE**
  - *Florence County Economic Development*
- **OSHKOSH**
  - *Fox Valley Technical College*
  - *Greater Oshkosh Economic Development Corporation*
- **EAU CLAIRE**
  - *Western Dairyland*
- **MENOMONIE**
  - *Dunn County Economic Development Corporation*
- **LADYSMITH**
  - *Indianhead Community Action Agency*
- **RHINELANDER**
  - *Nicolet Area Technical College*
- **GREEN BAY**
  - *Advance Business & Manufacturing Center*
- **ASHLAND**
  - *Ashland Area Development Corporation*



12/04/20

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)


Search ...
BLOG
SERVICES
ABOUT
CLIENT PORTAL
SPONSORSHIP
CONTACT
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
GRANTS
SUCCESS & AWARDS
FAQS
CURRENT EDITION OF THE WPI NEWSLETTER
UPCOMING EVENTS
WED 21
Acquisition Hour: Government Property Management for Federal Contractors and Subcontractors
August 21 @ 12:00 pm - 1:00 pm
THU 22
Advancing Cybersecurity in the Industry, Energy, Water Nexus – Oshkosh, WI
August 22 @ 9:00 am - 3:00 pm
Oshkosh WI
THU 22
NDIA Great Lakes Chapter 10th Anniversary – Milwaukee, WI
August 22 @ 12:30 pm - 7:30 pm
Brookfield Wisconsin
SEP 11
Acquisition Hour: The End of the Fiscal Year is Here – What is Hot and What is Not
September 11 @ 12:00 pm - 1:00 pm
View More...
CURRENT OPPORTUNITIES (1)
www.wispro.org
GET STARTED WITH THE BASICS
Questions & answers on how to get started.
SIGN-UP FOR OUR NEWSLETTER
Stay up-to-date with the latest WPI news.
HAVE A QUESTION? WE'RE HERE TO HELP.
One of our staff of experts is available to answer your questions.

Securing the Supply Chain
"No man is an island"

Marc N. Violante

December 4, 2020

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

- Supply Chains are vital to DOD being able to execute its mission.
- They are often complex, lengthy and involve numerous businesses.
- Understanding what they are, how they are used and what is important to their success can be key to maintaining and/or unlocking business opportunities at either a contract level or at a system level.
- Supply Chain security issues impact where we are today with respect to new requirements.

Being a good contractor

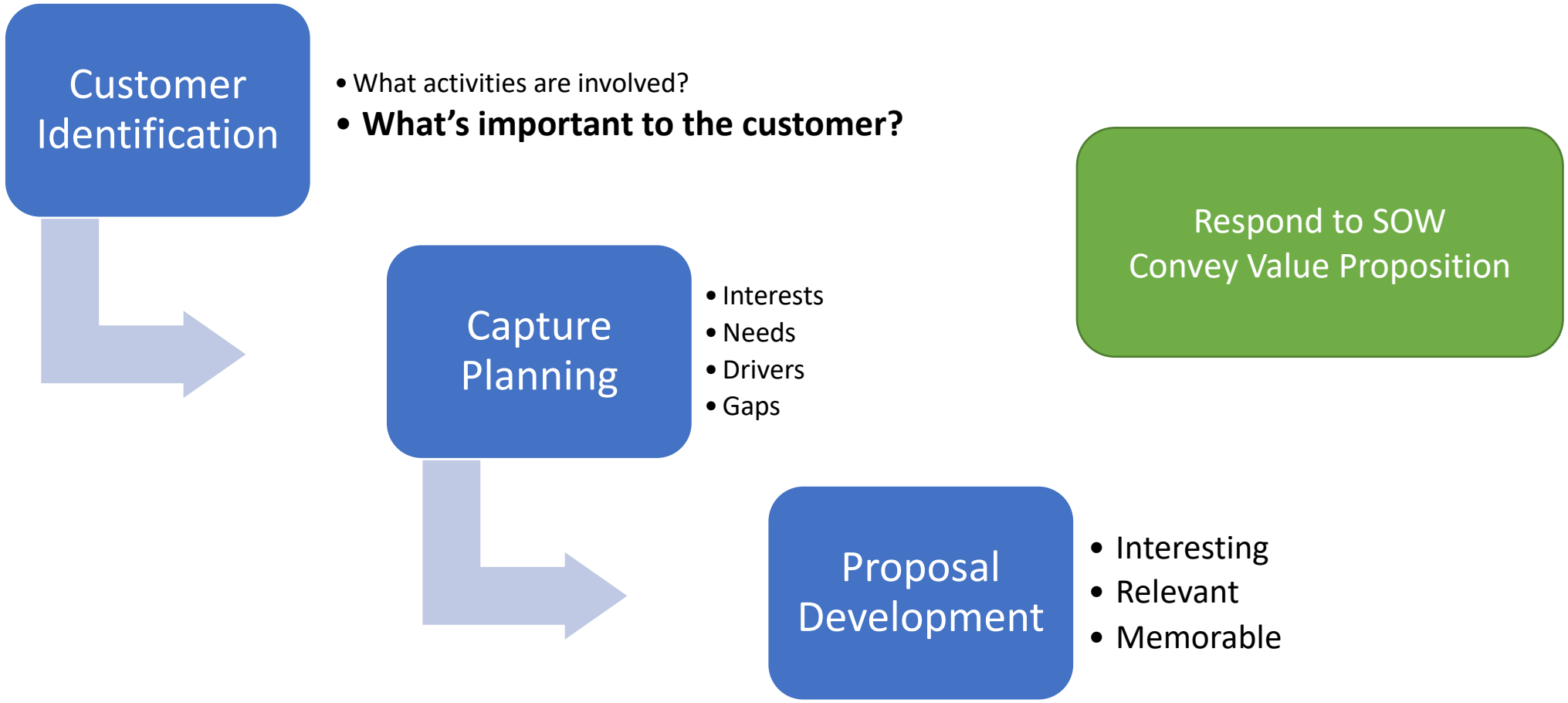
It’s required

Compliance/Responsibility

It’s good for business

Business Development
Capture Planning
Proposal Development

Business Development



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 – 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

DLA - actions

Think DIBBS & enhanced JCP

- strengthens technical data controls across the enterprise
- instituting an enhanced validation procedure for suppliers requiring access to export controlled technical data
- develops the capability to block foreign Internet
- Protocol addresses from accessing export controlled data stored in DLA's data repository.
- This initiative also assigns the highest level of restriction to the data repository for exportable data that includes a TDP and minimizes the amount of time a TDP is made available in the repository.

Defense Logistics Agency Supply Chain Security Strategy, page 7

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

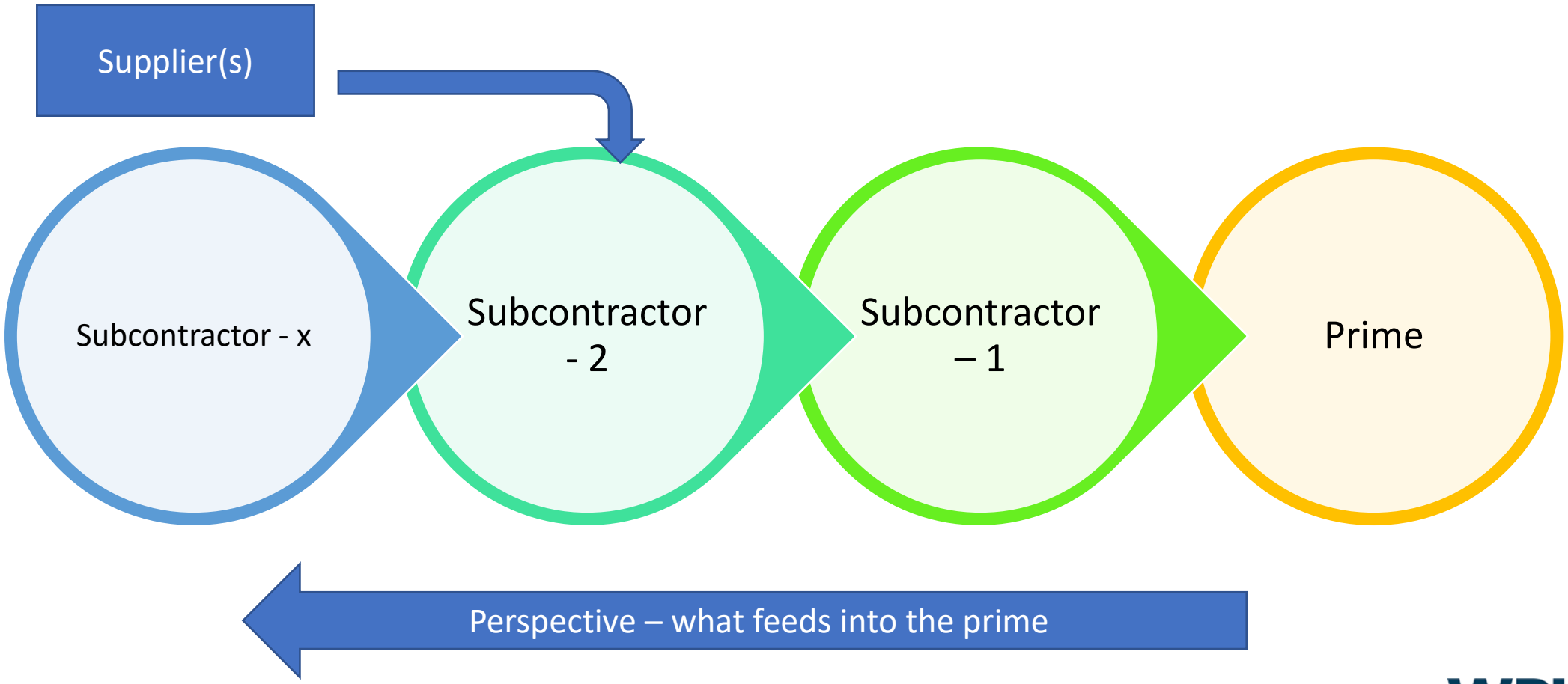
Supply Chain – matters! - opportunities

- Unawarded Solicitation Opportunities - This list includes open unawarded solicitations that do not have a qualified quote for DLA Aviation. You can browse the spreadsheet for solicitations by NSN or nomenclature. If interested in a particular solicitation, the DIBBS link can be opened to view the solicitation.
- Prime Strategic Contracting Opportunities - This spreadsheet details small business strategic solicitations for DLA Aviation. You can filter by type of set-aside, National Stock Number (NSN) and nomenclature. If interested in a particular solicitation, copy and past the DIBBS link provided into your web browser to see the solicitation. It is suggested that if you are interested in the solicitation on DIBBS that you also sign up in DIBBS to receive an email alert to for amendments to the solicitation.
- Strategic Subcontracting Opportunities - This spreadsheet provides points-of-contact for the major Original Equipment Manufacturers (OEM) that support DLA Aviation's strategic contracts. You can use the information in the sheet if you are interested in exploring subcontracting opportunities with the OEMs.
- No Bid Solicitation List - Most of these items can be found at DIBBS. You can search the National Stock Number (FSC+NIIN, i.e. 5962011231234) and find open solicitations, a point of contact, and complete data, if available. Contact the DLA Land & Maritime Business Counseling Center for assistance by email: Small Business Office.
- Replenishment Parts Purchase or Borrow (RPPOB) Program - Aviation's reverse engineering opportunities through the RPPOB Program
  - RPPOB Parts Online Catalog
  - Parts Catalogue Spreadsheet - the link to the spreadsheet is located in the middle of the page
- Land and Maritime Value Management & Engineering (VE) Programs - View Land & Maritime's VE Programs webpage for various opportunities to include the RPPOB Program

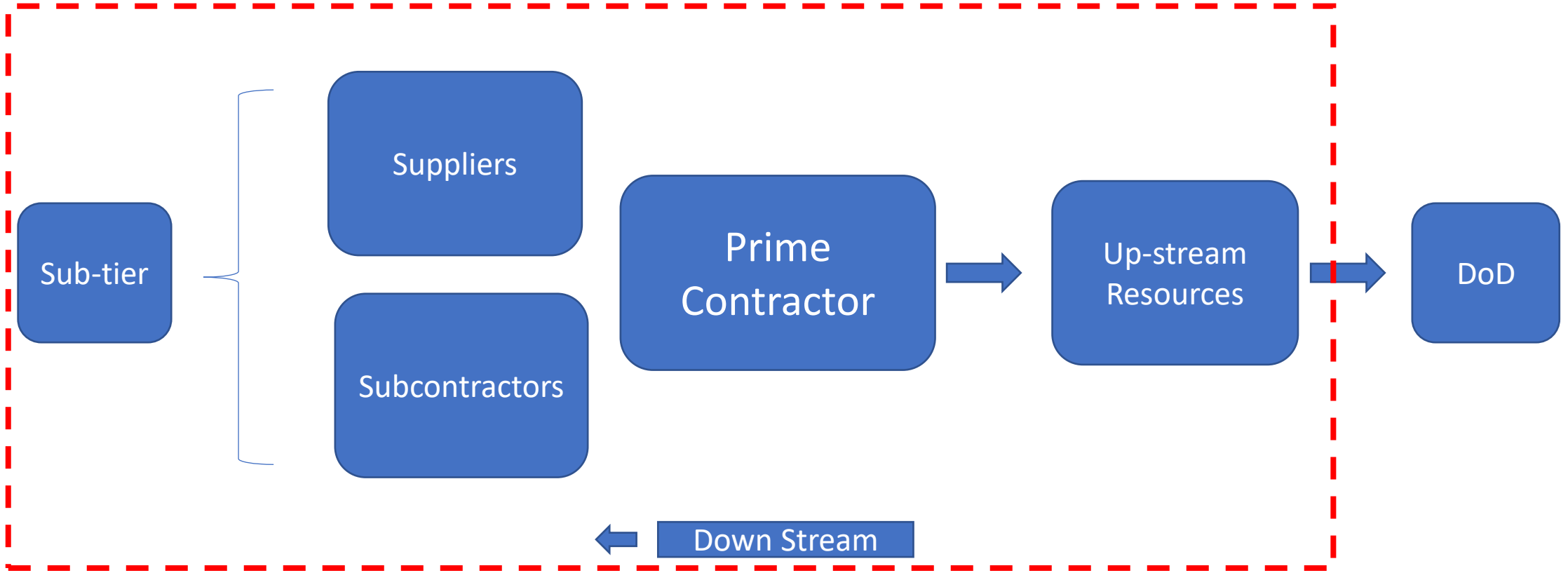
Land: 2,175
Maritime: 3,580

https://www.dla.mil/SmallBusiness/VendorOpportunities/

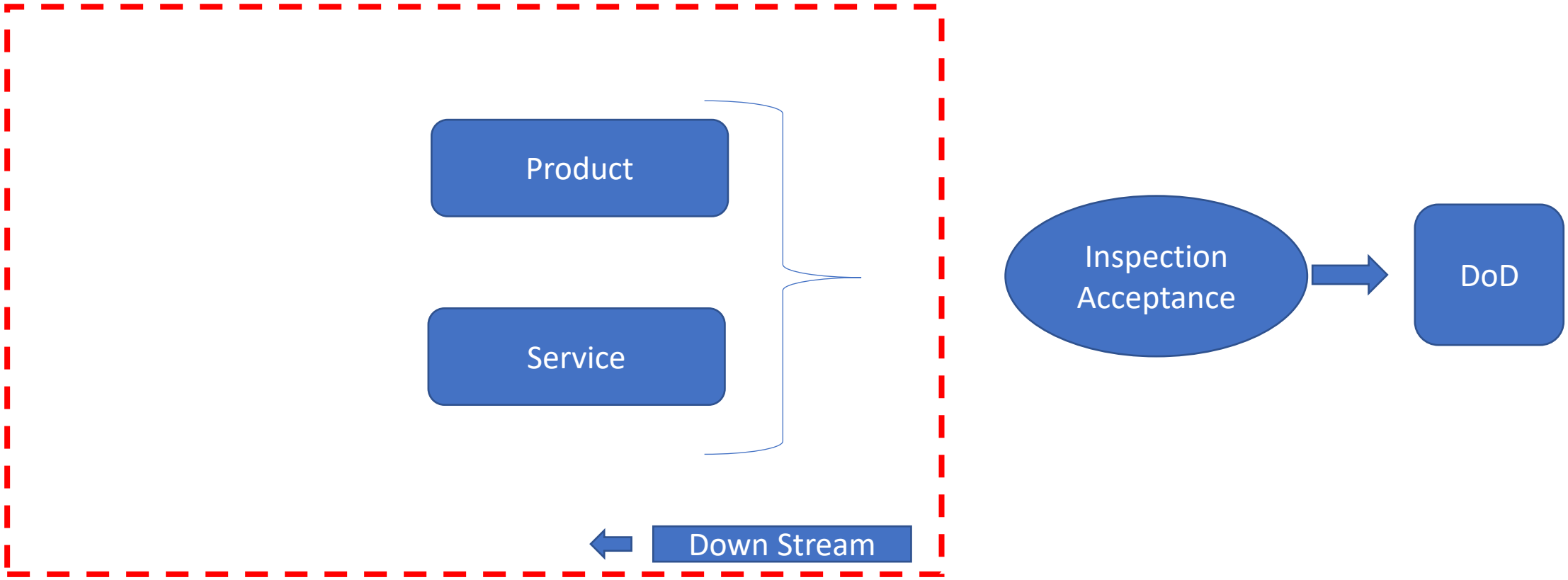
Supply Chain – As seen by a DoD contractor



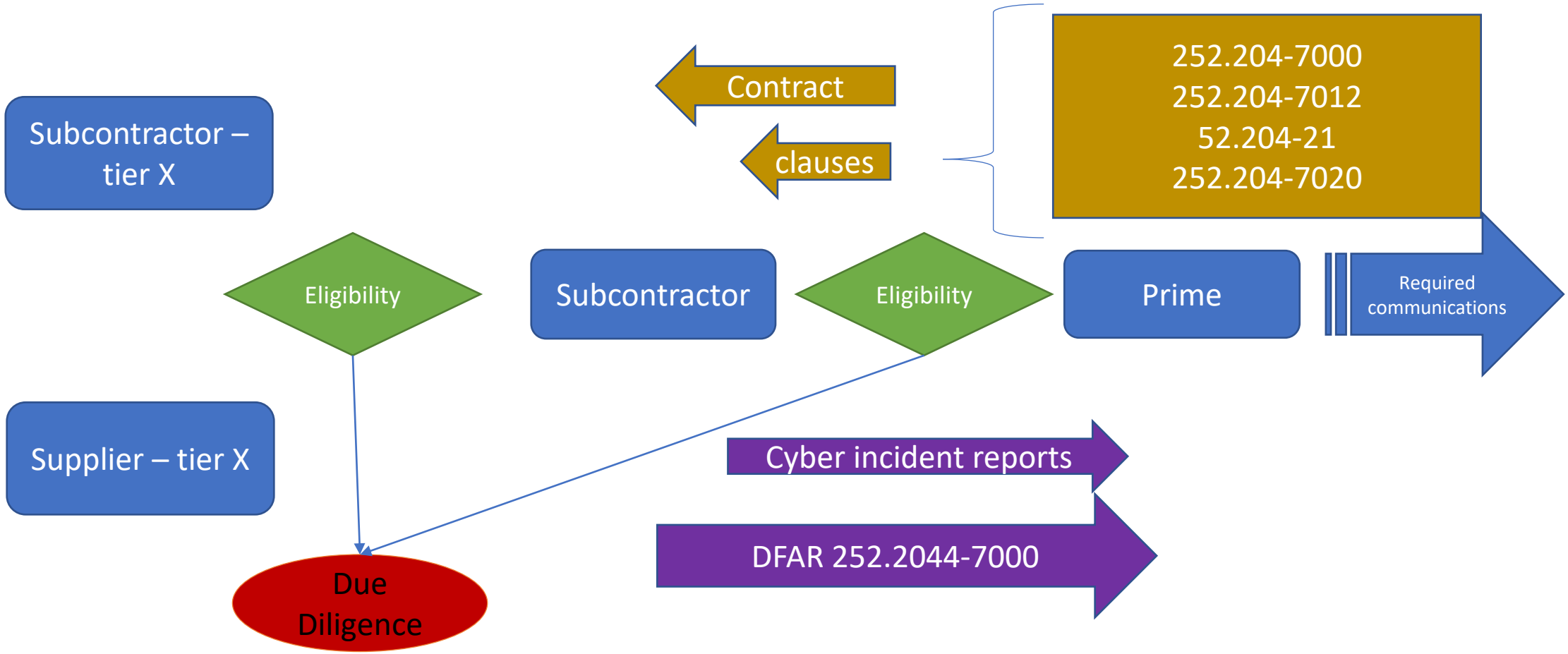
Performance Chain



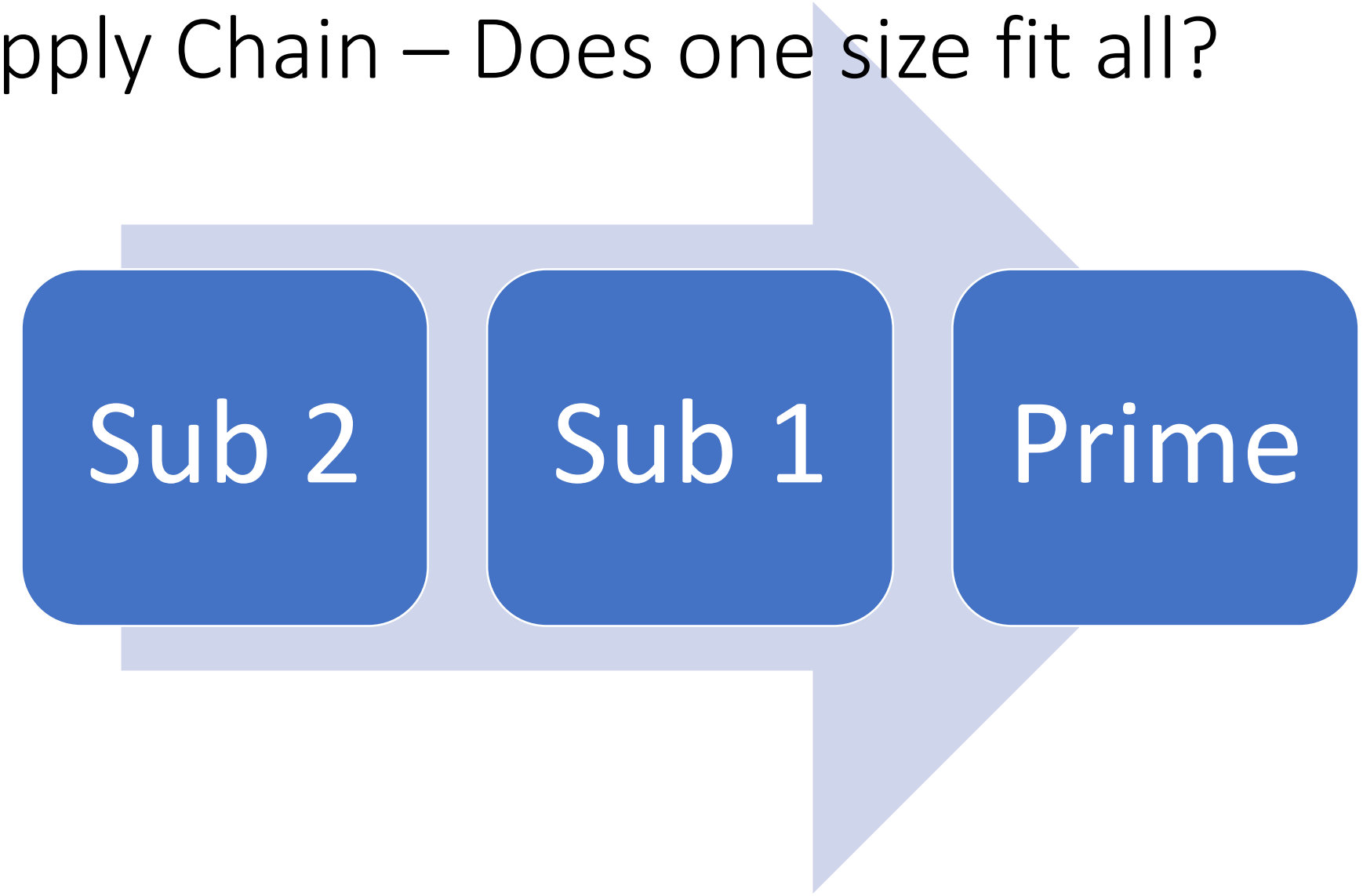
Performance Chain – focus points



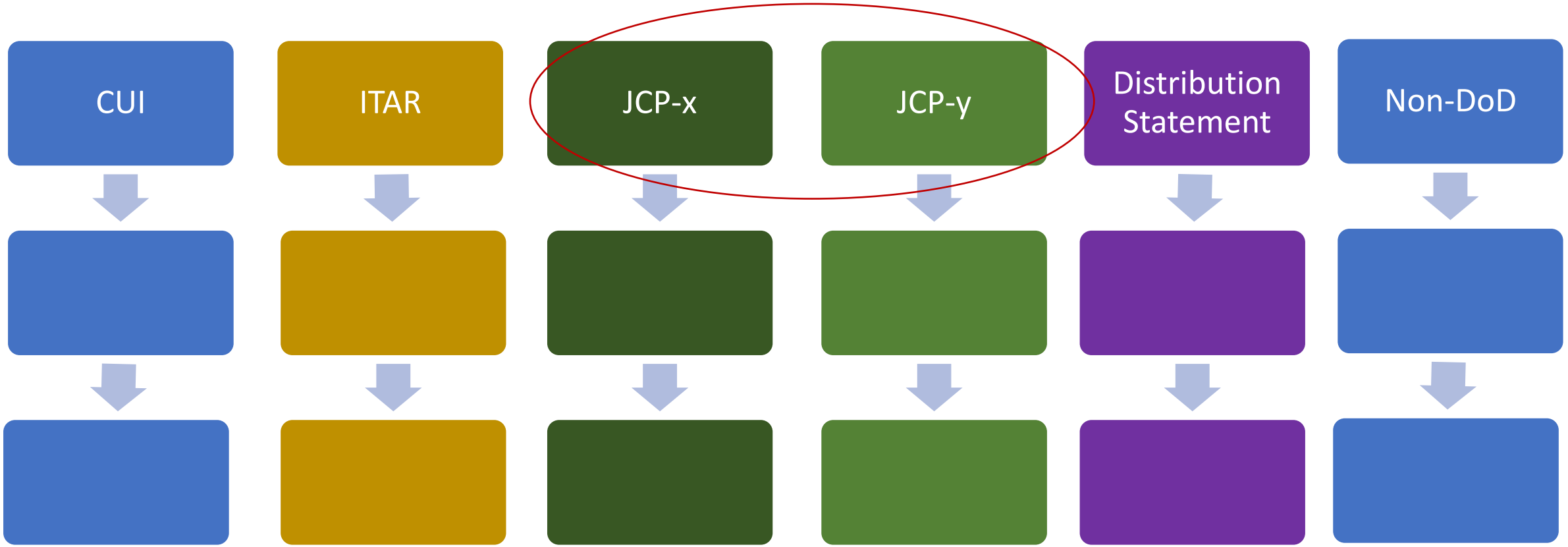
Identifying and managing Information Flows



Supply Chain – Does one size fit all?



Supply Chain – information category driven



JCP – X | JCP - Y

- 3.2.4. The U.S. contractor also agrees that, unless dissemination is permitted by paragraph 5.8., below, it will not provide access to export-controlled technical data subject to this Directive to persons other than its employees or persons acting on its behalf, without the permission of the DoD Component that provided the technical data.

- 5.4.2. The requested data are judged to be unrelated to the purpose for which the qualified U.S. contractor is certified. When release of technical data is denied in accordance with this paragraph, the controlling DoD office shall request additional information sufficient to explain the intended use of the requested data and, if appropriate, request a new certification (see paragraph 3.2., above) describing the intended use of the requested data; or

DoDD NUMBER 5230.25 November 6, 1984 ; Incorporating Change 2, October 15, 2018

Supply Chain - definition

- The linked activities associated with providing materiel to end users for consumption. Those activities include supply activities (such as organic and commercial ICPs and retail supply activities), maintenance activities (such as organic and commercial depot level maintenance facilities and intermediate repair activities), and distribution activities (such as distribution depots and other storage locations, container consolidation points, ports of embarkation and debarkation, and ground, air, and ocean transporters).

DoDI 4140.01, March 6, 2019 ; Glossary

Supply Chain – As seen by DLA

Classes of Supply	Supply Chains	DLA Major Subordinate Command	Support Contracts
Class 1	Subsistence (Food and Drinking)	DLA Troop Support	Global Contract Support (EA for Subsistence)
Class 2	Clothing & Equipment	DLA Troop Support (Clothing and Textiles)	Contract Support (Management)
Class 3	Petroleum, Oil & Lubricants	DLA Energy	Global Contract Support (EA for Bulk Petroleum)
Class 4	Construction Materiel	DLA Troop Support	Global Contract Support (EA for Construction & Barrier Materiel)
Class 5	Ammunitions	Military Departments	
Class 6	Personal Demand Items	DLA Troop Support	
Class 7	Major End Items	Military Departments	
Class 8	Medical Materiel	DLA Troop Support	Global Contract Support (EA for Medical Materiel)
Class 9	Repair Parts	DLA Land & Maritime DLA Aviation	Contract Support (Common Use Items)
Service	Disposal / Salvage	DLA Disposition Services	Deployable Support
Service	Warehouse / Distribution	DLA Distribution	Deployable Services
Service	National Defense Stockpile	DLA Acquisition (J7) Strategic Materials	
Service	DLA Document Services	DLA Information Operations (J6)	
Service	DLA Transaction Services	DLA Information Operations (J6)	
Service	DLA Logistics Information Services	DLA Information Operations (J6)	Global Support (EA for Logistics Management Standards)

Contact Information: DLA HQ Battle Captain (571)767-2711 **Email:** cat.HQC@dla.mil

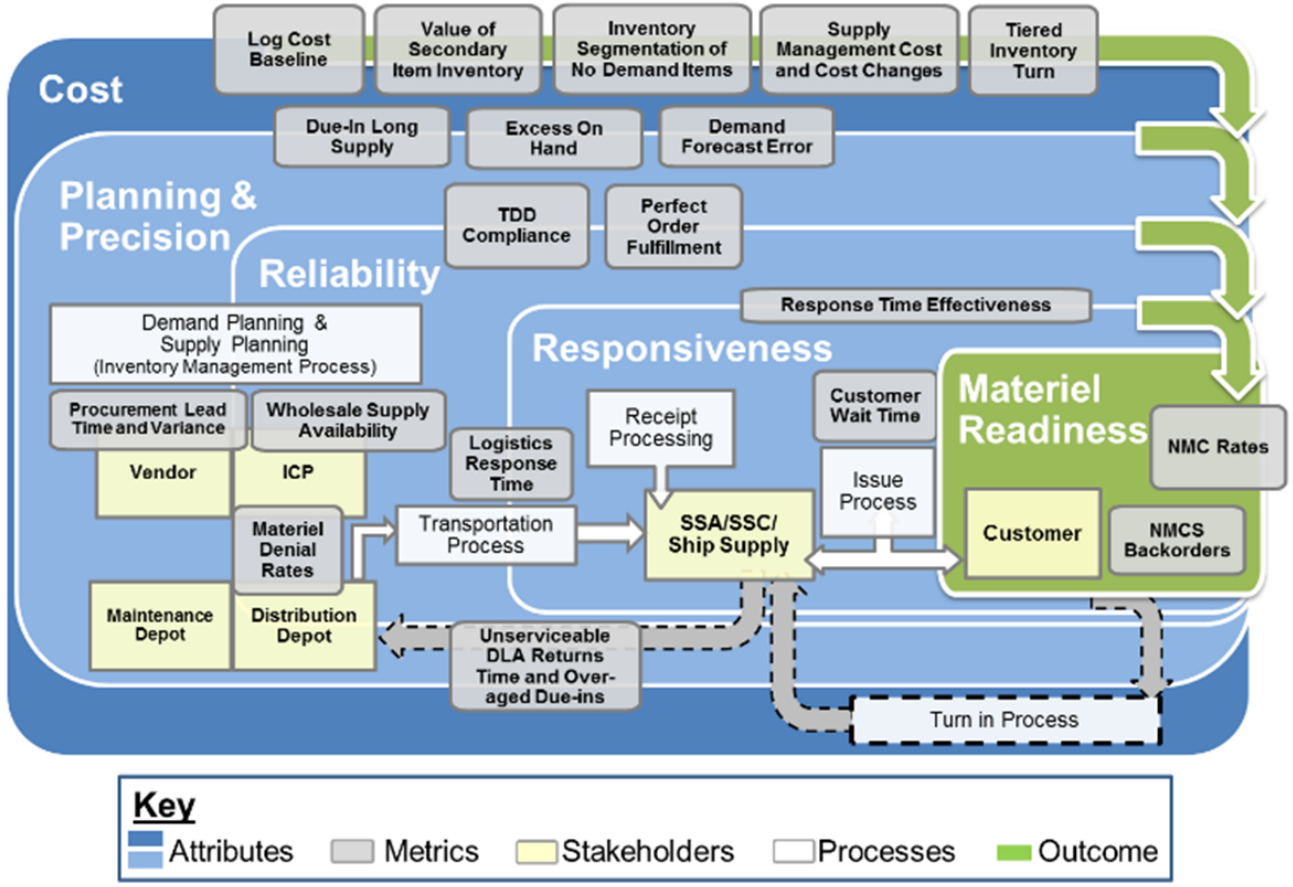
https://www.dla.mil/HQ/Acquisition/

Supply Chain – elements - complexity

Figure 5. Supply Chain Elements

Defense Logistics Agency Supply Chain Security Strategy, page 7

Supply Chain – As seen by DoD

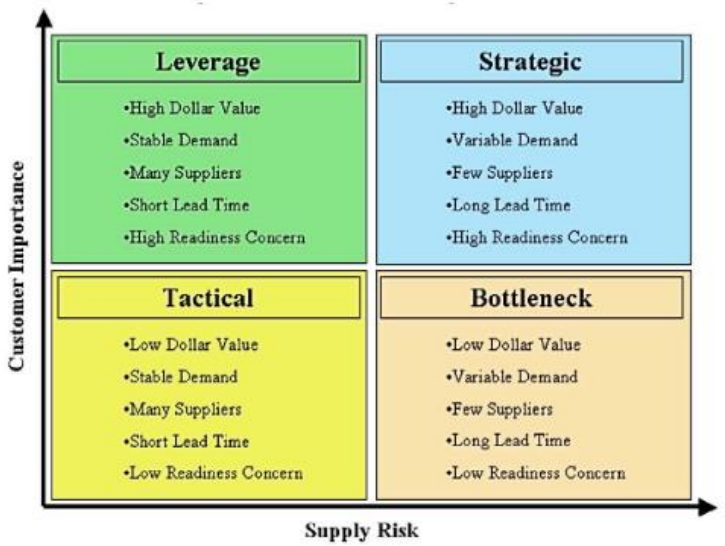


https://www.acq.osd.mil/log/SCI/.policy_vault.html/Supply_Chain_Metrics_Guide_signed_3Mar2016.pdf; page 4

Supply Chain – As seen by DLA

- For leading firms, understanding and managing supply chain risk is an essential first step in designing and implementing a successful strategic sourcing and supplier relationship management strategy.
- Supply chain risk is a measure of the effect of uncertainty along any point in the end-to-end supply chain and its objectives.

Figure 1.2. DLA Supplier Segmentation Matrix



SOURCE: Report to Office of Management and Budget: Department of Defense Strategic Sourcing Initiatives FY 2008 Update.

RAND_RR902.pdf page 4

Supply Chain – Details considered

VendorFailRisk = (StatusRisk + RevenuePercentFall + RevenuePercentFallToAllVendors
+ RevenuePercentSAM + IsContractExpired
+ Floodrisk + TornadoRisk + HurricaneRisk + QuakeRisk + ForeignRisk)/9.

SystemImpactRisk = (1/7)*(isNonreparable + Solesource + DACrisk + ,Factor
+ SystemCountRisk + EDA_demands_factor + EDA_ratio_factor).

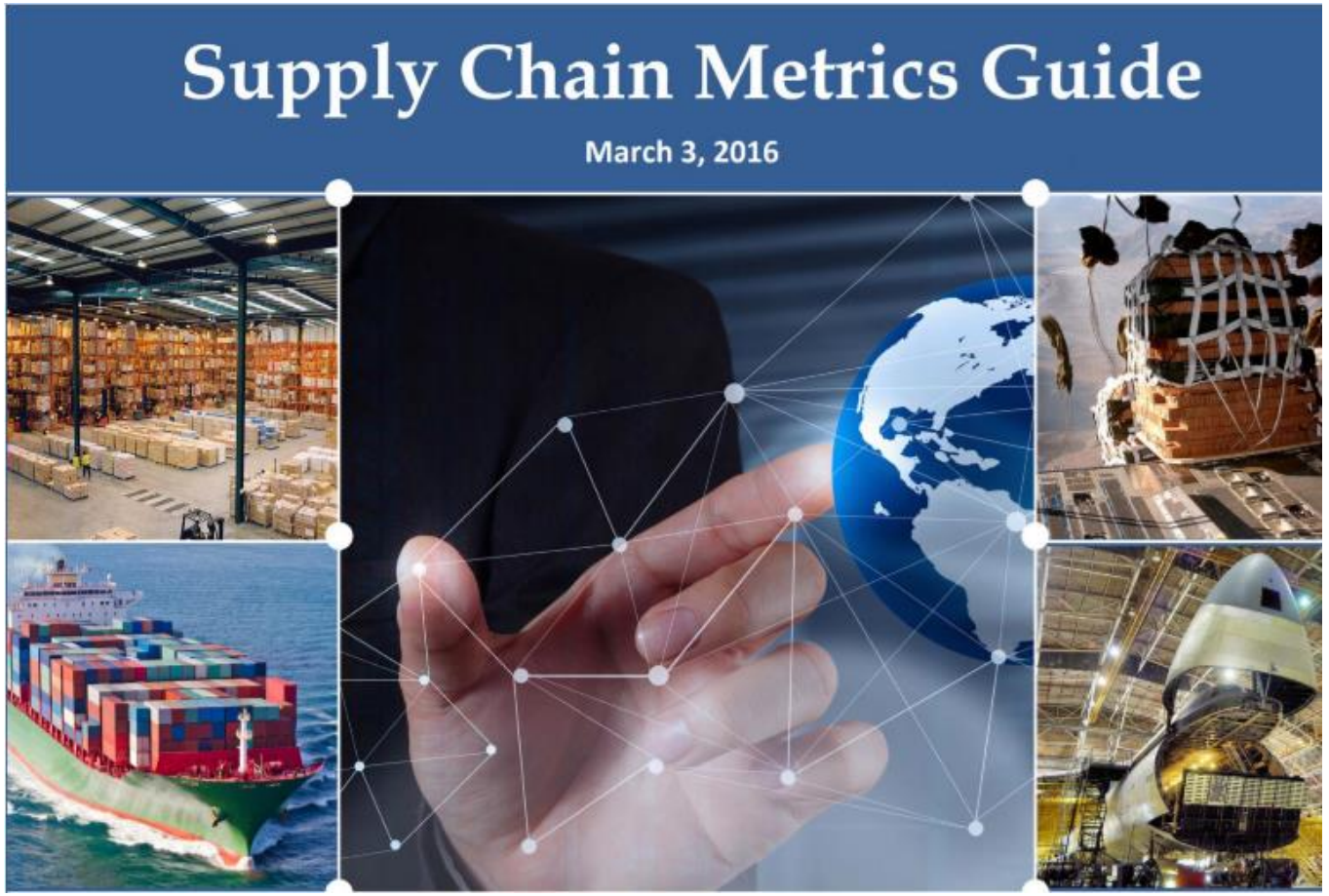
NIIN risk = VendorFailRisk*SystemImpactRisk/(DaysToRunOut/365 + 1).

Final calculation. If the NIIN was reparable, we calculated days to run-out as the days to contract run-out, plus 365 times the quantity on hand, divided by [annual issues times the wash-out rate]. (With 48 parts on hand, demand of 30, and a 40 percent washout rate, we would predict about 48/(30*0.4) = 48/12 = 4 years on hand.)

RAND_RR902.pdf pages 19-21

“You get what you measure”

The Guide provides a description of each metric and how it is used to assess supply chain performance throughout the DoD enterprise. The metrics in this guide include enterprise level metrics that cross supply chain functions to describe the overall effectiveness of the supply chain.



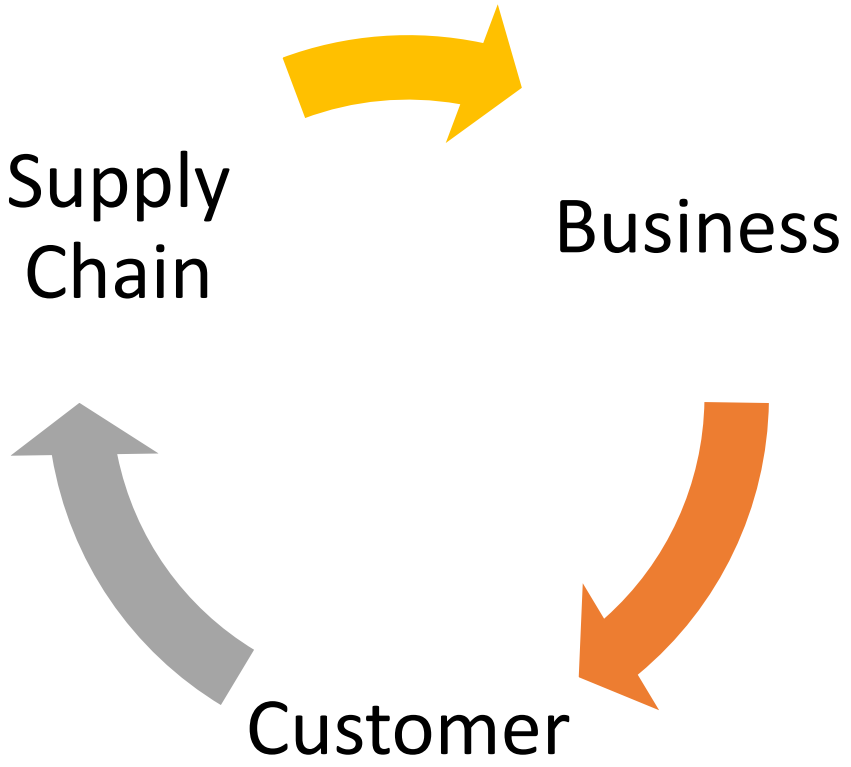
Out of the Crises, Deming
https://www.acq.osd.mil/log/SCI/.policy_vault.html/Supply_Chain_Metrics_Guide_signed_3Mar2016.pdf

Operations Security

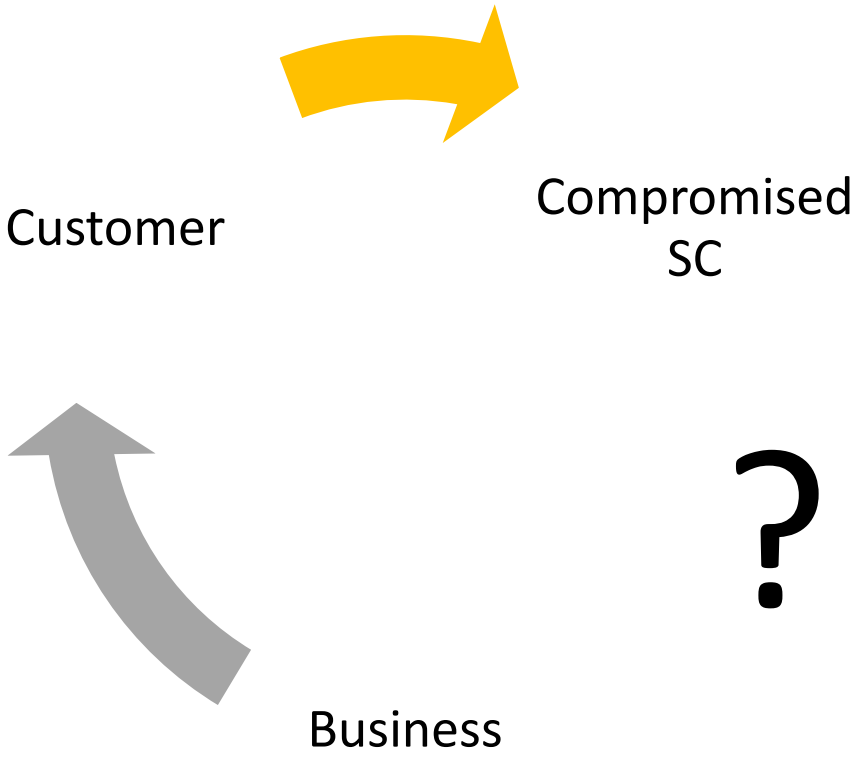
- Operations Security (OPSEC) is a systematic process to preserve friendly essential secrecy by identifying, controlling and protecting critical information and indicators that would allow adversaries or potential adversaries to identify and exploit friendly vulnerabilities. DLA must be ever vigilant 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

Generalized Business Cycle



Corrupted Business Cycle

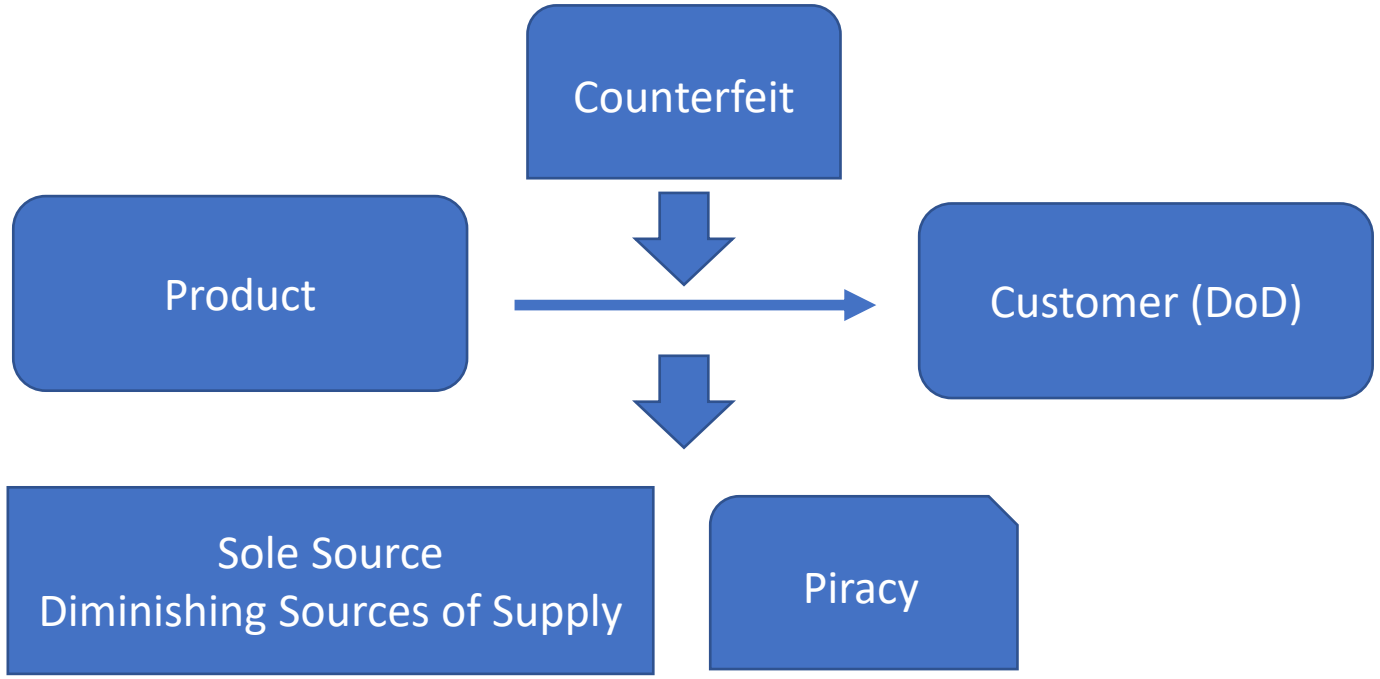


Supply Chain Risks

Geopolitical	Cyber	Nefarious actors
Natural Disasters	Diminishing Manufacturers	Sole Source

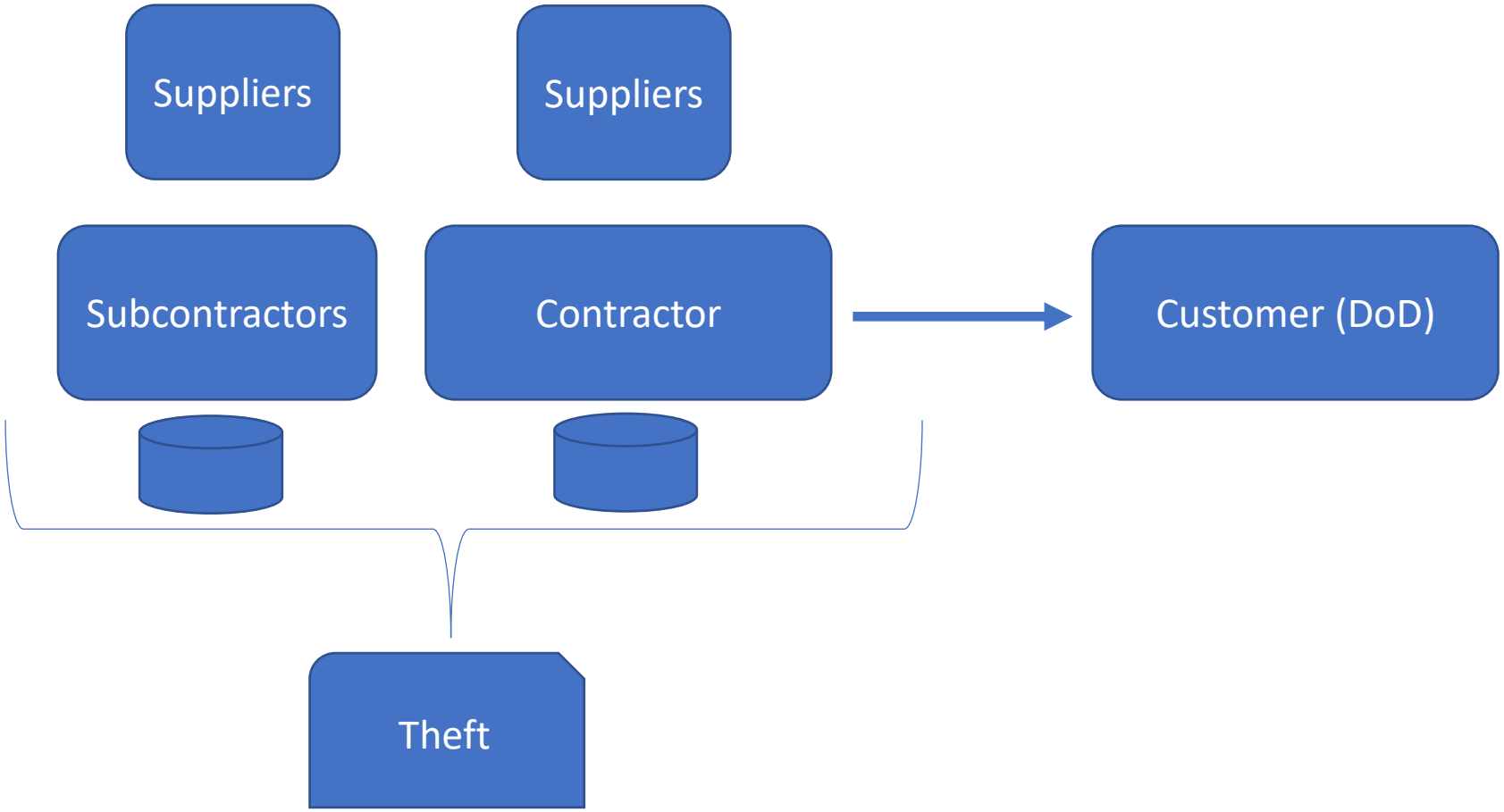
SUPPLY CHAIN SECURITY STRATEGY Strengthening Operational Resiliency - Appendix 1 to DLA's 2018 - 2026 Strategic Plan; Introduction

Type 1 threats (product)



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

Type 2 threats (information)



Key Practices in Cyber Supply Chain Risk Management: Observations from Industry

- Reducing the cybersecurity risk to one of the most vulnerable aspects of commerce — global supply chains — is the goal of a new publication by the National Institute of Standards and Technology (NIST), whose computer security experts have distilled a set of effective risk management techniques into a draft guidebook for businesses. NIST is seeking public comment on the draft for the next 30 days.
- *Key Practices in Cyber Supply Chain Risk Management* (Draft NISTIR 8276) provides a set of strategies to help businesses address the cybersecurity issues posed by modern information and communications technology products, which are commonly built using components and services supplied by third-party organizations. The composed nature of these devices and systems makes them difficult to secure effectively against malware and other threats, placing manufacturers, service providers and end users at risk.

https://www.nist.gov/news-events/news/2020/02/nist-offers-strategies-help-businesses-secure-their-cyber-supply-chains

Cyber Supply Chain Risk Management (C-SCRM) program

Key Practices

1. Integrate C-SCRM across the organization
2. Establish a formal program
3. Know and manage your critical suppliers
4. Understand your supply chain
5. Closely collaborate with your key suppliers
6. Include key suppliers in your resilience and improvement activities
7. Assess and monitor throughout supplier relationship
8. Plan for the full lifecycle

https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8276-draft.pdf

Cyber Supply Chain Risk Management (C-SCRM) program

Selected Key Recommendations

- Create explicit collaborative roles, structures, and processes for supply chain, cybersecurity, product security, and physical security (and other relevant) functions.
- Integrate cybersecurity considerations into the system and product lifecycle.
- Determine supplier criticality by using industry standards and best practices.
- Mentor and coach suppliers to improve their cybersecurity practices.
- Include key suppliers in contingency planning, incident response, and disaster recovery planning and testing.
- Use third-party assessments, site visits, and formal certification to assess critical suppliers.

https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8276-draft.pdf

Cyber Supply Chain Risk Management (C-SCRM) program

Recommendations – selected items

- Propagate security requirements to suppliers' sub-suppliers
- Train key stakeholders in your organization and within the supplier's organization
- Terminate supplier relationships with security in mind
- Use the Criticality Analysis Process Model or BIA to determine supplier criticality
- Establish visibility into your suppliers' production processes (e.g., capture defect rates, causes of failure, and testing)
- Know if your data and infrastructure are accessible to suppliers' sub-suppliers
- Mentor and coach suppliers to improve their cybersecurity practices
- Require the use of the same standards within both acquirer and supplier organizations
- Use acquirer assessment questionnaires to influence acquirer's cybersecurity requirements

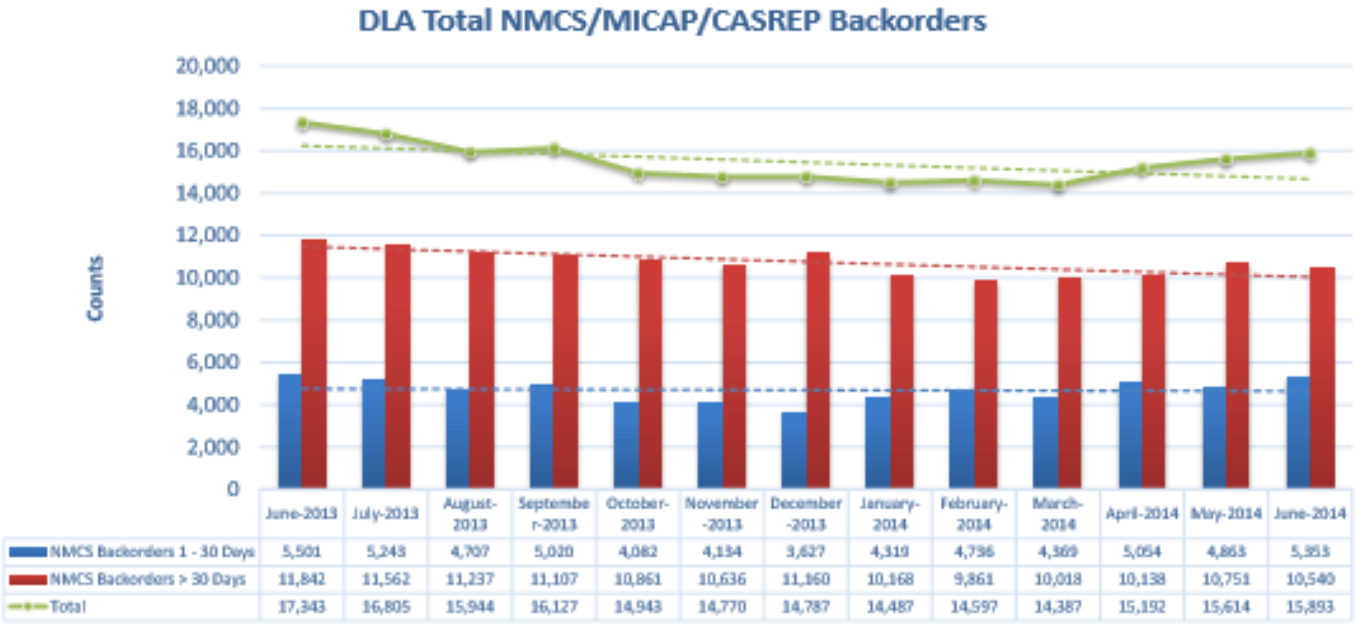
https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8276-draft.pdf

Criticality Analysis Process Model – see: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8179.pdf -- Business Impact Analysis - https://www.ready.gov/business-impact-analysis

Why? – Insight into key ideas – drivers

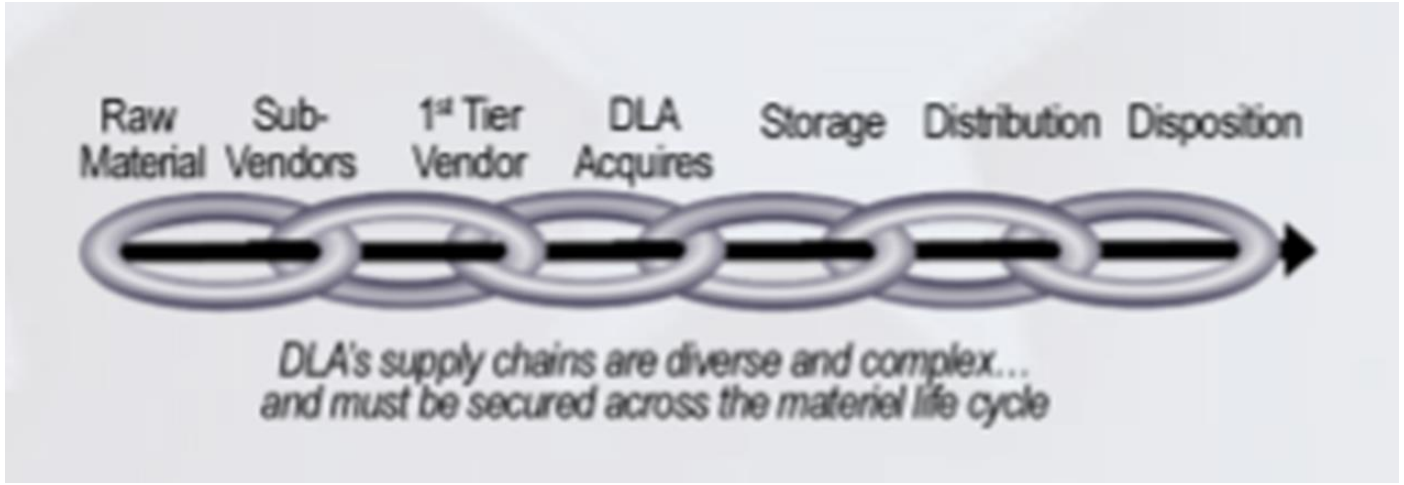
Growth in the backorder counts above can be an indication of future readiness problems. As the number of backorders greater than 30 days increases, the probability increases that NMC rates will rise

Figure 8. Not Mission Capable Supply Backorders



	June-2013	July-2013	August-2013	September-2013	October-2013	November-2013	December-2013	January-2014	February-2014	March-2014	April-2014	May-2014	June-2014
NMCS Backorders 1 - 30 Days	5,501	5,243	4,707	5,020	4,082	4,134	3,627	4,319	4,736	4,369	5,054	4,863	5,353
NMCS Backorders > 30 Days	11,842	11,562	11,237	11,107	10,861	10,636	11,160	10,168	9,861	10,018	10,138	10,751	10,540
Total	17,343	16,805	15,944	16,127	14,943	14,770	14,787	14,487	14,597	14,387	15,192	15,614	15,893

DoD Supply Chain Metrics Guide, March 3, 2016; page 13



Why is understanding DoD's Supply Chain important to your business?

Awareness of programs and emphasis

- Issue: DFARS 252.2304-7012 “Does not provide for verification of a DIB contractor’s implementation of the security requirements specified in NIST SP 800-171 prior to contract award. – self-attest
- CMMC is designed to provide increased assurance to the Department that a DIB contractor can adequately protect sensitive unclassified information such as FCI and CUI at a level commensurate with the risk accounting for information flow down to its subcontractors in a multi-tier supply chain.
- The CMMC implementation will provide the Department with an ability to illuminate the supply chain, for the first time, at a scale across the entire DIB sector.

Interim Rule: FR - Vol 85, No 189 page 61505; 615059

252.204-7000 Disclosure of Information.

(a) The Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract, unless—

(1) The Contracting Officer has given prior written approval;

(2) The information is otherwise in the public domain before the date of release; or

(3) The information results from or arises during the performance of a project that involves no covered defense information (as defined in the clause at DFARS 252.204-7012) and has been scoped and negotiated by the contracting activity with the contractor and research performer and determined in writing by the contracting officer to be fundamental research (which by definition cannot involve any covered defense information), in accordance with National Security Decision Directive 189, National Policy on the Transfer of Scientific, Technical and Engineering Information, in effect on the date of contract award and the Under Secretary of Defense (Acquisition, Technology, and Logistics) memoranda on Fundamental Research, dated May 24, 2010, and on Contracted Fundamental Research, dated June 26, 2008 (available at DFARS PGI 204.4).

(b) Requests for approval under paragraph (a)(1) shall identify the specific information to be released, the medium to be used, and the purpose for the release. The Contractor shall submit its request to the Contracting Officer at least 10 business days before the proposed date for release.

(c) The Contractor agrees to include a similar requirement, including this paragraph (c), in each subcontract under this contract. Subcontractors shall submit requests for authorization to release through the prime contractor to the Contracting Officer.

Future emphasis

3. Securing supply chains: The incoming administration could require device makers to label their products with alerts about potential insecurities, particularly in Internet of Things devices.

- It could also fund "critical technology testing centers" where the private sector could check for security flaws. And it could help support more open-source software, which would open technology to more security scrutiny.

4. Measuring cybersecurity: Biden could, among other initiatives, establish a "Bureau of Cyber Statistics" to track and provide statistical data to policymakers and the public, as well as have the Department of Homeland Security form a working group on cyber risk that brings in the insurance industry and modeling experts to better work out potential pricing schemes for cyber insurance.

- The report says that “today, the federal government lacks the most basic, reliable data” on a wide range of critical issues like cyberattacks.

Zach Dorfman of the Aspen Institute zach.dorfman@axios.com, Axios Codebook: Biden’s cybersecurity agenda — Hacking law goes to SCOTUS — Krebs speaks on threats; Wed 12/2/2020 11:35 AM

Supply Chains – current v. future

- Vendors are being asked to bring ideas for the following technologies and processes related to digital engineering: “virtual work environments, rapid prototyping and demonstration, infrastructure operability, big data management, analysis, and visualization, linking disparate data sources and systems, digital thread and digital twin, 3D printing/additive manufacturing, advanced architecture tools, **advanced logistics tools**, 2D to 3D conversion/validation, augmented/virtual reality, cyber security, decision analysis, model based systems engineering, model based engineering, software visualization, and cloud/high performance computing (HPC) cost effective infrastructure.”

https://breakingdefense.com/2020/12/air-force-plans-first-digital-engineering-pitch-day/

Dell Announces New Supply Chain Security Offerings

- Dell Technologies on Thursday announced new security offerings designed to address threats targeting the supply chain, a device's boot process, and sensitive data.

- For supply chain security, Dell unveiled SafeSupply Chain solutions. This includes SafeSupply Chain Tamper Evident Services, which involves adding tamper-evident seals to ensure a device has not been modified during transport — for extra security customers can also request pallet seals. The offering also includes SafeSupply Chain Data Sanitization Services, which enables organizations to perform a hard drive wipe before deploying their own images to ensure that there is no spyware or other malware on the device.

- Dell also announced that EMC PowerEdge servers will use Secured Component Verification, which leverages an embedded certificate to cryptographically verify that the hardware has not been tampered with after it left the factory.

https://www.securityweek.com/dell-announces-new-supply-chain-security-offerings

CJCS Milley Predicts DoD Budget 'Bloodletting' To Fund Navy

- WASHINGTON: In a major speech outlining important strategic shifts for the United States, the Chairman of the Joint Chiefs, an Army general, today predicted "a lot of bloodletting" in the Pentagon as the military strives to get the Navy the hundreds of new ships it says it needs to confront China.
- "I would advocate, and bias going forward, heavy investment" in sea, air and space-centric platforms, Milley said. As for the other priorities, he said, "none of it gets cut to zero; this is a matter of balancing things. It's a very, very difficult exercise we're going to have to go through. It's going to be ruthless, there's going to be a lot of bloodletting and a lot of stuff left on the floor. We're gonna have to do that in the coming years — no question about it."

https://breakingdefense.com/2020/12/cjcs-milley-predicts-dod-bloodletting-to-fund-navy-priorities/

Supply Chain – DoD, 1 example

- In the military space, the collaborative construction of the Lockheed Martin F-35 aircraft
- by 10 countries
- and more than 1,500 global suppliers
- suggests the capability of the United States to successfully work together with its allies to develop critical technologies.[45]

Cyberspace Solarium Commission, BUILDING A TRUSTED ICT SUPPLY CHAIN, pg 6,

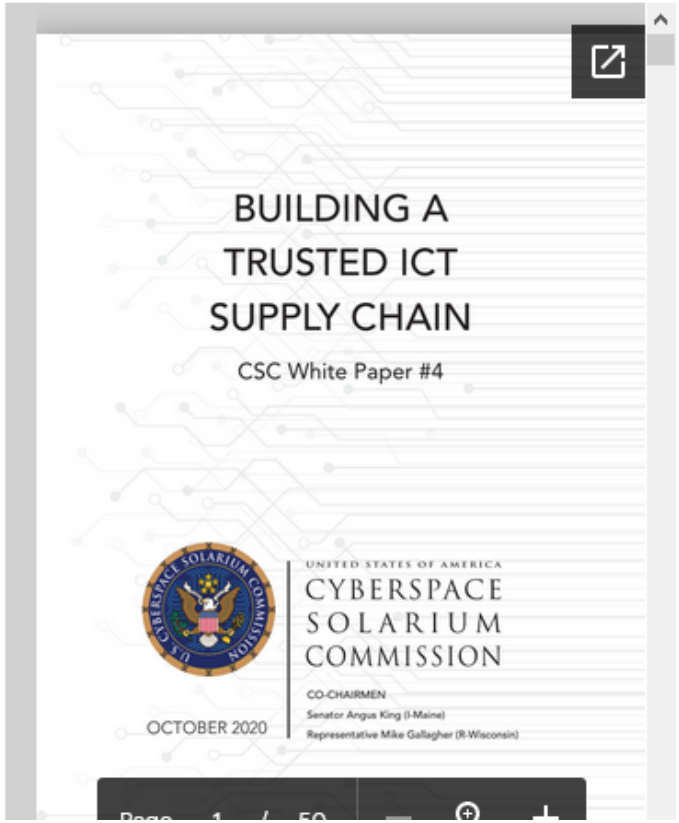
Cyberspace Solarium Commission

Introduction

The Cyberspace Solarium Commission (CSC) was established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." The finished report was presented to the public on March 11, 2020.

https://www.solarium.gov/

CSC White Paper #4: Proposes five-pillar strategy



Dependency on China and other adversary countries for some of our most critical supply chains threatens to undermine the trustworthiness of critical technologies and components that constitute and connect to cyberspace. This dependency also risks impairing the availability of these same critical technologies and components and compromises American and partner competitiveness in global markets in the face of Chinese economic aggression.

To address these challenges, the Commission proposes a five-pillar strategy built on the firm foundation of public-private and international partnerships. Specifically, the Commission provides a roadmap and recommendations focused on:

1. ***Identifying key technologies and equipment*** through government reviews and public-private partnerships to identify risk.
2. ***Ensuring minimum viable manufacturing capacity*** through both strategic investment and the creation of economic clusters.
3. ***Protecting supply chains from compromise*** through better intelligence, information sharing, and product testing.
4. ***Stimulating a domestic market*** through targeted infrastructure investment and ensuring the ability of firms to offer products in the United States similar to those offered in foreign markets.
5. ***Ensuring global competitiveness*** of trusted supply chains, including American and partner companies, in the face of Chinese anti-competitive behavior in global markets.

- Information and Communications Technologies (ICTs).

https://drive.google.com/file/d/1efo96fPx5WkOxTiFFY1r5y3lFqdit00C/view (also available from website link)

CSC White Paper #4 – What is important?

Critical Dependencies

First, critical dependencies pose a threat to the consistent and reliable availability of raw materials, intermediate goods, and finished products that are crucial to the uninterrupted operation of the U.S. military, industrial base, and society. The continued reliance on foreign actors for raw materials and intermediate goods, or components that form the basic building blocks of technology, presents adversaries with points of leverage. In a time of crisis, these adversaries may seek to block access to these critical resources.

The second major risk concerns the trustworthiness of equipment or components the United States receives from overseas. While vulnerabilities are a fact of technology in both hardware and software, vulnerabilities intentionally unaddressed or planted by adversaries in components or finished goods undermine the security and trustworthiness of the critical systems that rely on those products. It is important to acknowledge that building trusted supply chains cannot and should not replace continued efforts to secure infrastructure through design and cybersecurity interventions after products are deployed.

Finally, these critical dependencies threaten to undermine American competitiveness and innovation in an age of global markets and rapid technological transformation, in part through facilitating forced technology transfer and intellectual property theft. Recently, China has placed great strategic emphasis on semiconductor manufacturing supremacy, leading to a sharp increase in production facilities based in China, even though China, which remains several generations behind the state of the art in semiconductor manufacturing, is heavily dependent on foreign semiconductor manufacturing equipment.

Cyberspace Solarium Commission, BUILDING A TRUSTED ICT SUPPLY CHAIN, pg 1

Critical Dependencies

- This strategy is tailored to ICTs, but similar efforts are needed for operational technologies that control power, water, transportation, and other critical infrastructure sectors, as well as unique production areas like medical devices and weapons systems.
- these technologies fall outside of the scope of this white paper, many of their core materials and components, including semiconductors, are integral to critical technologies more broadly. Thus many of the recommendations contained in this paper lay a firm foundation for technologies beyond ICT and will support efforts in those other areas.
- Put bluntly: in the context of our supply chains for ICT, the United States has a China problem. Over the past two decades,China has mobilized state-owned and state-influenced companies to grab a dominant position in markets for several emerging technologies, including the market for telecommunications equipment.2

Cyberspace Solarium Commission, BUILDING A TRUSTED ICT SUPPLY CHAIN, Executive Summary

Current / Evolving Threats

IBM Releases Report on Cyber Actors Targeting the COVID-19 Vaccine Supply Chain

12/03/2020 06:00 AM EST

Original release date: December 3, 2020

IBM X-Force has released a report on malicious cyber actors targeting the COVID-19 cold chain—an integral part of delivering and storing a vaccine at safe temperatures. Impersonating a biomedical company, cyber actors are sending phishing and spearphishing emails to executives and global organizations involved in vaccine storage and transport to harvest account credentials. The emails have been posed as requests for quotations for participation in a vaccine program.

The Cybersecurity and Infrastructure Security Agency (CISA) encourages Operation Warp Speed (OWS) organizations and organizations involved in vaccine storage and transport to review the IBM X-Force report Attackers Are Targeting the COVID-19 Vaccine Cold Chain for more information, including indicators of compromise. For tips on avoiding social engineering and phishing attacks, see CISA Insights: Enhance Email & Web Security.

https://us-cert.cisa.gov/ncas/current-activity/2020/12/03/ibm-releases-report-cyber-actors-targeting-covid-19-vaccine-supply
https://www.fastcompany.com/90582260/hackers-are-now-targeting-the-critical-covid-19-vaccine-cold-supply-chain

Americold

- The attack appears to be a ransomware incident that started on Nov. 16, according to a Bleeping Computer report. The attack affected the company's phone systems, email, inventory management and order fulfilment, according to reports on Twitter. One truck driver on Monday tweeted, "At a Americold [depot] and their systems are down," they noted. "They are unable to assign me to a door. Well let the waiting begin."

https://threatpost.com/food-supply-americold-cyberattack/161402/

Next steps to recovery? – “cold start”

- How to get the back up?
- How is the need communicated?
- Who has access?
- Is there a machine to start with?
- Is the process all digital? – Is there a paper copy?
- Is the back-up current?
- Has the back up been tested?
- Copy of the malware for 252.204-7012 – how?
- Forensic image 252.204-7012 – how?
- 252.204-7012 DIB investigation/cyber report
- Other precautions to prevent reinfection?
- Are there contingency contracts?

Supply Chain knowledge requirements

- Programs / Supply Chain members
  - Information used/handled
  - Handling – sharing requirements
  - Vetting/Knowledge of vendor base
  - Maintaining currency of vendor base
  - Communication coordination
  - Testing compliance – you shared!
  - Cost considerations
  - Performance
  - Downstream impacts – ripple effect

DFARS 252.204-7000

-------- Forwarded Message --------
Subject:FW: 20150206 Signed request for Authorization Re [redacted]
Date: Tue, 31 Mar 2015 16:15:47 +0000
From: Jones, Joanna M DLA CIV AVIATION <joanna.jones@dla.mil>
To:[redacted]
CC:DCMA Chicago (Patricia.Scott@dcma.mil) <Patricia.Scott@dcma.mil>, Jones, Joanna M DLA CIV AVIATION <joanna.jones@dla.mil>, Collier, Kimberley J DLA CIV AVIATION <Kimberley.Collier@dla.mil>

All,

Regarding the subject request, permission is granted to allow your sub to have a copy of the drawings.

Rev A, and MIS-20007, Rev AD, are marked with Distribution Statement D; therefore, the contractor must make sure that

[redacted] Inspection Laboratories holds the proper requirements or clearance to access this level of government drawing.

If so, [redacted] may provide the drawings to them. Thank you!

Joanna Jones
DLA Missiles Contracting Officer
256-842-4456
Joanna.jones@dla.mil

Client email

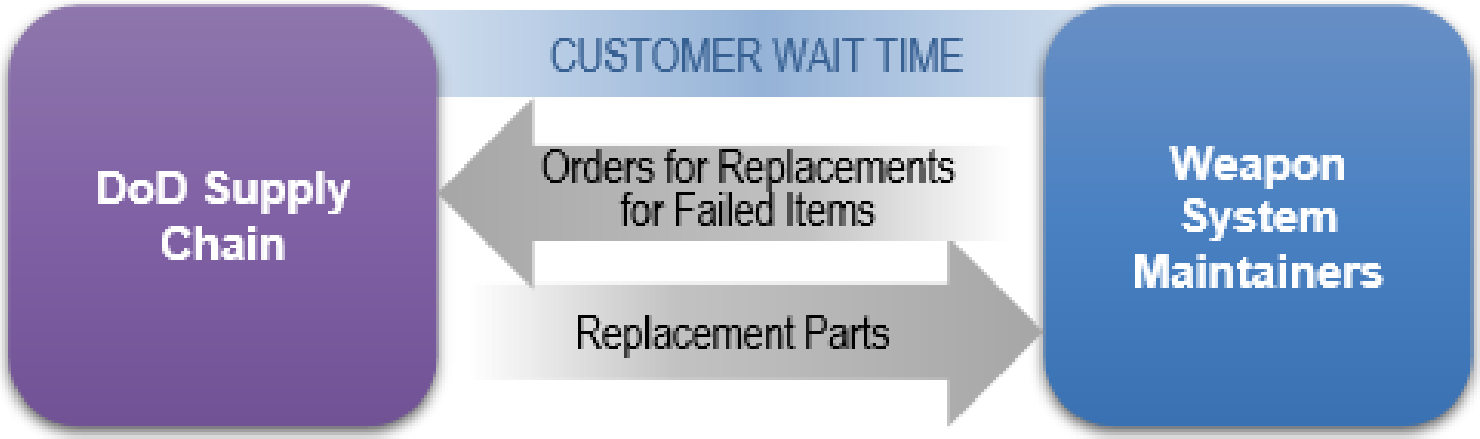
Supply Chain – definition >> activity types

- Supply activities
  - organic and commercial ICPs
  - retail supply activities
  - maintenance activities
    - organic and commercial
      - depot level maintenance facilities
      - intermediate repair activities
  - distribution activities
    - distribution depots
    - other storage locations
    - container consolidation points
    - ports of embarkation and debarkation
    - ground, air, and ocean transporters).

DoDI 4140.01, March 6, 2019 ; Glossary

Why? – Why is understanding the supply chain important?

Figure 5. The Role of the Customer Wait Time



CWT is the key enterprise metric used to evaluate the responsiveness of the supply chain to customers who are maintaining the readiness of weapon systems.

Understand the needs of the customer; ask the right questions; determine the value proposition.

DoD Supply Chain Metrics Guide, March 3, 2016; page 11

Defense Logistics Manuals

The DoD Components will comply with DoD supply chain materiel management technical procedures published in the Defense Logistics manuals listed in Table 1 and other applicable publications, such as the Federal Logistics Information System technical procedures.

Table 1

Defense Logistics Manual Number	Defense Logistics Manual Title
Defense Logistics Manual 4000.25	Defense Logistics Management Standards (DLMS)
Volume 1 of Defense Logistics Manual 4000.25	Defense Logistics Management Standards (DLMS): Concept and Procedures
Volume 2 of Defense Logistics Manual 4000.25	Defense Logistics Management Standards (DLMS): Supply Standards and Procedures
Volume 3 of Defense Logistics Manual 4000.25	Defense Logistics Management Standards (DLMS): Transportation
Volume 4 of Defense Logistics Manual 4000.25	Defense Logistics Management Standards (DLMS): Military Standard Billing System (MILSBILLS) - Finance
Volume 6 of Defense Logistics Manual 4000.25	Defense Logistics Management Standards (DLMS): Logistics Systems Interoperability Support Services
Volume 7 of Defense Logistics Manual 4000.25	Defense Logistics Management Standards (DLMS): Contract Administration
Defense Logistics Manual 4000.25-1	Military Standard Requisitioning and Issue Procedures (MILSTRIP)
Defense Logistics Manual 4000.25-2	Military Standard Transaction Reporting and Accountability Procedures (MILSTRAP)
Defense Logistics Manual 4000.25-4	Defense Automatic Addressing System (DAAS)

DoDI 4140.01, March 6, 2019; page 16

SUPPLY CHAIN SECURITY VS. SCRM

- **Supply Chain Security**
  - is DLA's comprehensive approach to protect supply chains, key infrastructure and critical assets in order to assure uninterrupted delivery of proactive global logistics in peace and war.
- **Supply Chain Risk Management (SCRM)**
  - is 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. DODI 4140.01

DoDI 4140.01, March 6, 2019

Supporting Technologies

a. To ensure a high-performing and agile supply chain, DoD materiel managers will:

(1) Leverage modern technologies, such as enterprise resource planning systems, to enhance materiel management processes.

(2) Use modern technologies to automatically identify items in storage and movement that will provide better product support for weapon systems in accordance with the procedures in Volume 7 of DoDM 4140.01.

(3) Implement internal controls on the quality of performance metric generating data used by decision-makers.

(4) Use automatic identification technology to assist in property accountability, effectively manage costs, and implement the DoD policies cited in this issuance.

DoDI 4140.01, March 6, 2019; Section 3.7 – page 12

Threat of Fraudulent Exploitation

- Fraudulent exploitation still exists
  - Sheer volume of purchases
  - business transactions
  - automation required to support them
- Further complicating this
  - 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

Recurring theme

Operational Environment

- Plan and operate as if the environment is –
  - Contested
  - Degraded
- Company's should (align with DLA's view/actions) –
  - Build awareness – threats/activities/indicators/communicate
  - Monitor
  - Establish processes/procedures to –
    - Detect
    - Protect
    - Continue operations

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

DLA's Strategic Focus

- Institutionalize Supply Chain Security across the DLA enterprise
- ★ Maintain integrity and access to key data
- ★ Partner with valid, reputable vendors who produce quality supplies and services
- Strengthen the resiliency of systems, processes, infrastructure and people

DLA Actions - programs

- **DNA Marking of Microelectronics**: To counter the growing sophistication of counterfeiters, DLA launched an anti-counterfeiting program to improve delivery time, reduce costs, strengthen supply chain controls and enhance quality assurance. DNA marking consists of applying a botanical DNA identifier to the surface of a microcircuit to authenticate originality. The DNA mark cannot be replicated and deters counterfeiters. A hand-held scanner for easy identification within the supply chain can detect the DNA mark. The mark can also be used for forensic testing by providing detailed information about the microcircuit, such as supplier, CAGE code, part and lot number.
- **Vendor Network Mapping**: Relationships in DLA supply chains are complex. However, DLA is employing a powerful tool to map vendor networks from Tier 1 through Tier 3 suppliers called Vendor Network Mapping. This capability makes it possible to look upstream in vendor networks to identify risks in areas such as vendor financial position, compliance, legal and foreign relationships.

Controlled Inventory Item (CII)

- CII
  - Those items designated as having characteristics that require that they be identified, accounted for, secured, segregated, handled or transported in a special manner to ensure their integrity and that they are safeguarded. The list of CII codes includes NWRM, CC, non-nuclear missiles and rockets, arms, ammunition and explosives. CII categories in descending order of the degree of control normally exercised are classified items, sensitive items, and pilferable items.

DoDI 4140.01, March 6, 2019; page 19

Critical component

- Critical component
  - A component which is or contains information and communications technology including hardware, software, and firmware, weather custom, commercial, or otherwise developed and delivers or protects mission critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission critical functions of an applicable system as described in DoDI 5200.44.

DoDI 4140.01, March 6, 2019; page 19

Critical Safety Item (CSI)

- CSI
  - A part, assembly, support equipment, installation or production system containing a critical characteristic whose failure, malfunction, or absence may cause a catastrophic or critical failure resulting in loss or serious damage, unacceptable risk of personal injury or loss of life, or an unsafe condition.

DoDI 4140.01, March 6, 2019; page 19

What does it mean to know your vendors

- It depends on the sensitivity (program relationship) of the information
  - Joint Certification Program
  - Export Controlled – ITAR
  - Covered Defense Information (includes CUI)
  - Federal Contract Information
- Solicitation/contract requirements
- Supply Chain Support Agreement

Situational Awareness

- Target fixation – tunnel vision approach to
- Simpler/overlooked threats
  - Mishandling of data
  - Blind business relationships
  - Business first approach – if it “ain’t broke; don’t fix it”
  - Rigorous identification/marking program
  - No/weak/”punch the ticket” training

Threats

- Over-reliance
- Lack of duplication
- Disruption
- Cyber
- Confidentiality
- Integrity
- Availability
- Counter-feit
- Piracy

Looking beyond the first tier

- Programs
- Identifying program relationships
- Marking and marking requirements
- Requirements
- Managing relationships
- Determining who is eligible
- Identifying what is required transfer information

Flow-down clauses

- Active involvement
- Identify
- Inform – discuss
- Know – research
- Can’t be a “and dump” – hidden in documents
- Vague reference to
- Partner – a resource

Knowing your suppliers

- Vetting
- Communications
- Active involvement

Measuring and Managing Army Supply Chain Risk

Table of Contents

Research/Resources

- Defense Supply Chain Security: Current State and Opportunities for Improvement –
  - http://www.cpppe.umd.edu/publications/defense-supply-chain-security-current-stateand-opportunities-improvement
- A Quantitative Approach by Item Number and Commercial Entity Code
  - **https://www.rand.org/pubs/research_reports/RR902.html**
- U.S. Drug Supply Chain Security Act
- Supply Chain Risk Management Practices for Federal Information Systems and Organizations
  - NIST Special Publication 800-161

UPCOMING TRAINING - EVENTS

CYBER FRIDAY LIVE WEBINAR SERIES

Sept 11, 2020	A Deep Dive into DFARS 252.204-7012 - Looking beyond NIST 800-171 r1
Sept 25, 2020	Information Security - An overview of programs, general requirements and resources
Oct 9, 2020	Economic Espionage - You have what they want.
Oct 23, 2020	Guarding and Securing Intangibles - Protecting what you cannot see and touch
Nov 6, 2020	Tools, practices and resources for your cyber-security toolbox
Nov 20, 2020	An overview of cyber-threats - What you can't see - can put you out of business!
Dec 4, 2020	Securing the Supply Chain - "No man is an island"
Dec 18, 2020	Developing and implementing practices, policies and procedures using CMMC reference documents
Jan 8, 2021	The other side of CMMC
Jan 22, 2021	Overview of CMMC Level 1
Feb 5, 2021	Embarking on the path to CMMC Level 3
Feb 19, 2021	Preparing for a CMMC Certification assessment
Mar 5, 2021	CMMC Level 3 - Completing the steps needed to protect Controlled Unclassified Information.

PRESENTED BY

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

TECHNOLOGY INNOVATION CENTER at Research Park

NCMA National Contract Management Association
WISCONSIN

12/04/20

ACQUISITION HOUR LIVE WEBINAR SERIES

- January 20, 2021

  Acquisition Hour: beta.SAM.gov - An Update and Overview
  CLICK HERE for additional information
  Presented by Kim Garber, Wisconsin Procurement Institute

- February 17, 2021

  Acquisition Hour: Market Research – Successful Contractors Do Their Homework
  CLICK HERE for additional information
  Presented by Kim Garber, Wisconsin Procurement Institute

- February 23, 2021

  Acquisition Hour: Update on Federal Wage-Hour Laws
  CLICK HERE for additional information
  Presented by Corey Walton, U.S. Department of Labor

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

…More at wispro.org/events

- SAVE THE DATE-

MARKETPLACE WISCONSIN

December 8-10, 2020

The first virtual marketplace will connect statewide business owners looking to do business with state, federal and local governments, as well as the private sector, in a virtual format over the course of a week.

More info at https://www.wispro.org/event/marketplace-2020-virtual/

TCA The Contracting Academy

Developing and Growing Government Contractors

December 8-10, 2020

The Contracting Academy is an opportunity for businesses to grow their technical knowledge of contracting with the State of Wisconsin, Federal Government and Government Prime contractors. This series of workshops will benefit established businesses looking to grow and develop their government sales.

More info at https://www.wispro.org/event/the-contracting-academy-virtual/

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

- SAVE THE DATE-

January 28, 2021

Join Wisconsin's Federal contractors and subcontractors for this annual event. Keep up to date with this series of briefings focusing on changes and challenges in DOD/ Federal contracting.

Program: 8am – 3pm

Networking Hour with Guest Speaker: 3pm – 4pm

More info at https://www.wispro.org/event/13th-annual-end-of-year-federal-contractor-update-virtual/

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

CYBERSECURITY – UPDATE – DECEMBER 2020

- CMMC -
  - Implementation continues
  - Pathfinder contracts to be announced soon – article, Dec 1, 2020
    - CMMC requirements will be included
  - Full implementation expected by Oct 2025
- New clauses and requirements –
  - DFARS 252.204-7019
  - DFARS 252.204-7020 – applies to contracts subject to 252.204-7012
    - With few exceptions, these requirements apply to all Primes and Subcontractors
    - Consistent with philosophy shift of self-attest to verifiable
    - Three levels – Base – self-performed , Medium & High - DCMA

252.204-7020 – BASIC ASSESSMENT

- Requires
  - System Security Plan(SSP)
  - Plan of Action – with dates for outstanding items
  - Basic Assessment
- Six elements uploaded to Supplier Performance Risk System (SPRS)
  1. System Security Plan name (if more than one system is involved)
  2. Brief description of Plan Architecture
  3. CAGE code associated with SSP
  4. Date Assessment performed
  5. Summary Score
  6. Date a score of 110 to be achieved

CURRENT CYBER REQUIREMENTS

- FAR 52.204-21 – Federal Contract Information
- DFARS 252.204-7012
- Requirements cited in solicitation/contract

Need assistance – please contact Marc Violante from WPI at marcv@wispro.org or 920-456-9990

CONTINUING PROFESSIONAL EDUCATION

CPE Certificate available, please contact:

Benjamin Blanc

benjaminb@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)
www.wispro.org

Marc Violante
Wisconsin Procurement Institute (WPI)
marcv@wispro.org | 920-456-9990

10437 Innovation Drive, Suite 320
Milwaukee, WI 53226