Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

Cyber Friday

Vetting and Creating Agreements with Subcontractors and 3rd Party Service Providers

October 21, 2022




Webinar Etiquette

PLEASE

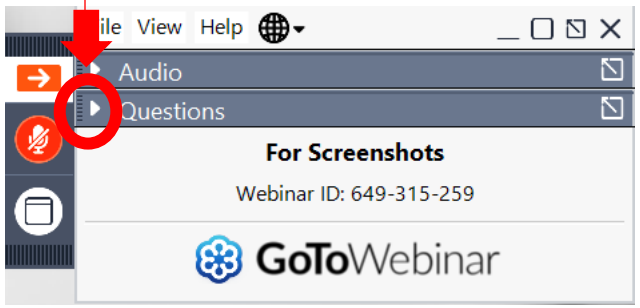
- Log into the GoToWebinar session with the name that you registered with online
- Place your phone or computer on MUTE
- Use the QUESTIONS option to ask your question(s).
  - We will share the questions with our guest speaker who will respond to the group

THANK YOU!

QUESTIONS?

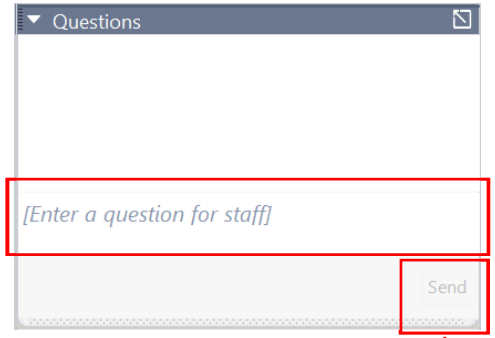
OPENING THE QUESTIONS BOX

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

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
Cyber Friday

ABOUT WPI
Supporting the mission

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
Cyber Friday

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/GoToMeeting**
- **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

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
Cyber Friday

WPI is a Procurement Technical Assistance Center (PTAC) funded in part by the Department of Defense (DOD), WEDC and other funding sources.

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

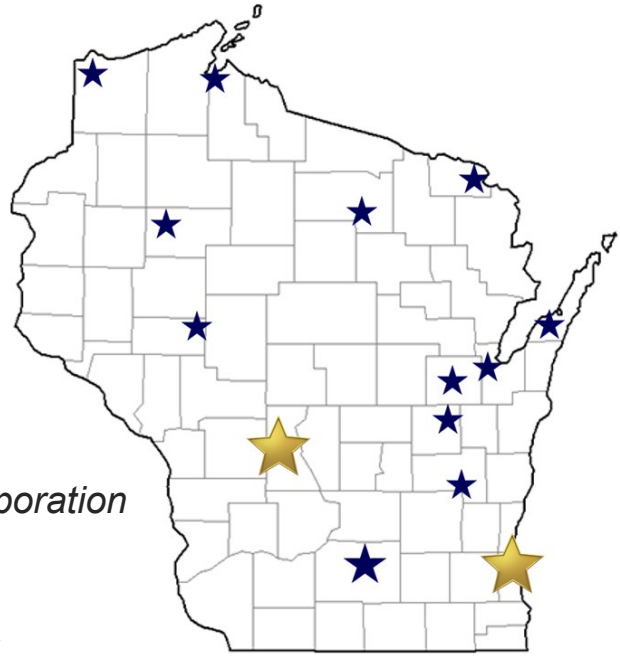
Sign-up for our Newsletter

Stay up-to-date with the latest WPI news and events.

https://www.wispro.org/newsletter-signup/

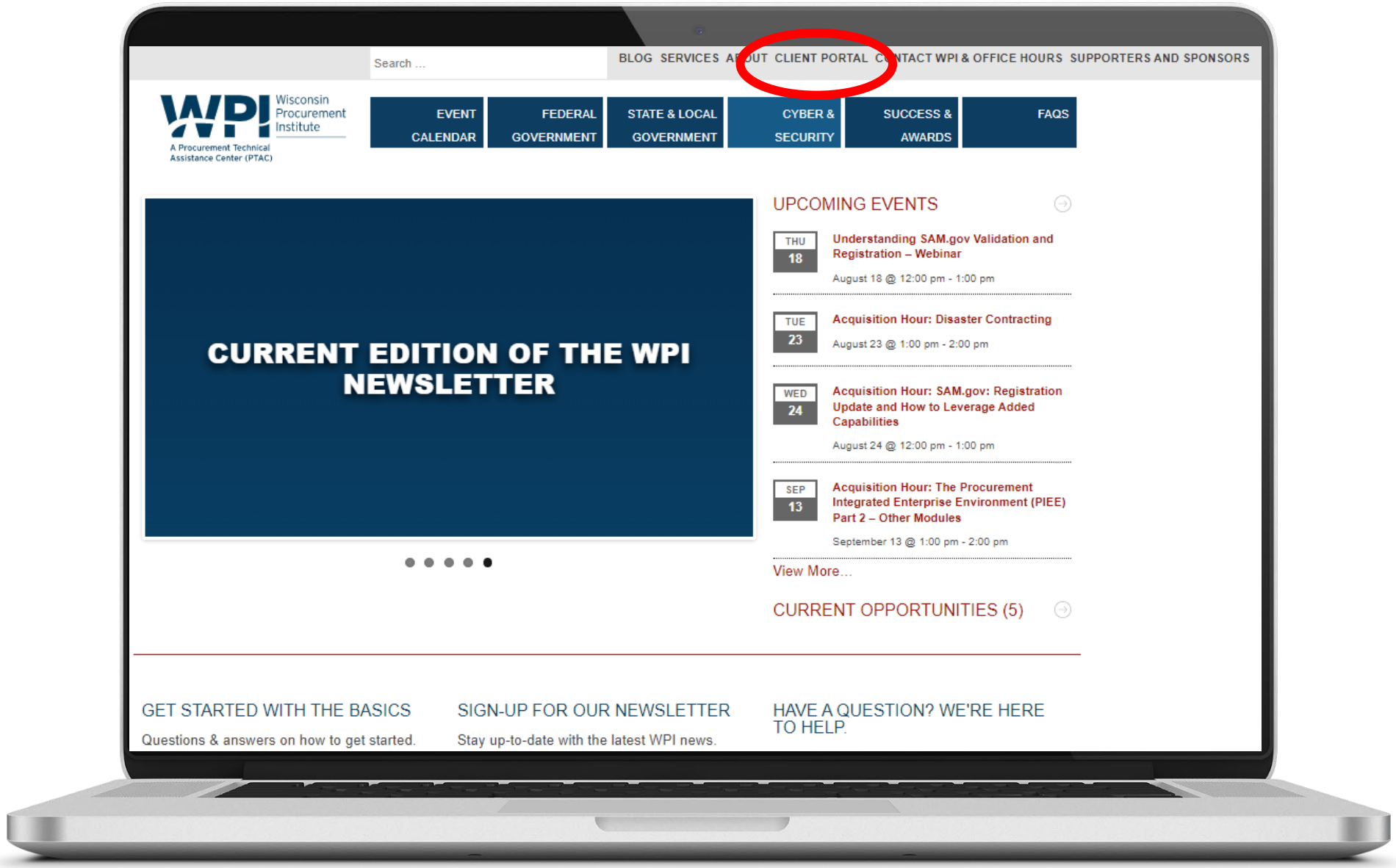
WPI OFFICE LOCATIONS

- **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)*
- **FOND DU LAC**
  - *Envision Greater Fond du Lac*
- **GREEN BAY**
  - *NWTC Startup Hub*
- **APPLETON**
  - *Fox Valley Technical College*
- **OSHKOSH**
  - *Fox Valley Technical College*
  - *Greater Oshkosh Economic Development Corporation*
- **EAU CLAIRE**
  - *Western Dairyland*
- **LADYSMITH**
  - *Indianhead Community Action Agency*
- **RHINELANDER**
  - *Nicolet Area Technical College*
- **ASHLAND**
  - *Ashland Area Development Corporation*
- **FLORENCE**
  - *Florence County Economic Development*
- **DOOR COUNTY**
  - *NE WI Technical College*
  - *Door County Economic Development Corporation*
- **SUPERIOR**
  - *Small Business Dev Center; UW Superior*



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

Cyber Friday


Search ...
BLOG SERVICES ABOUT CLIENT PORTAL CONTACT WPI & OFFICE HOURS SUPPORTERS AND SPONSORS
WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
CYBER & SECURITY
SUCCESS & AWARDS
FAQS
CURRENT EDITION OF THE WPI NEWSLETTER
UPCOMING EVENTS
THU 18
Understanding SAM.gov Validation and Registration – Webinar
August 18 @ 12:00 pm - 1:00 pm
TUE 23
Acquisition Hour: Disaster Contracting
August 23 @ 1:00 pm - 2:00 pm
WED 24
Acquisition Hour: SAM.gov: Registration Update and How to Leverage Added Capabilities
August 24 @ 12:00 pm - 1:00 pm
SEP 13
Acquisition Hour: The Procurement Integrated Enterprise Environment (PIEE) Part 2 – Other Modules
September 13 @ 1:00 pm - 2:00 pm
View More...
CURRENT OPPORTUNITIES (5)
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.

Vetting and Creating Agreements with Subcontractors and 3rd Party Service Providers

Marc N. Violante

Wisconsin Procurement Institute

October 21, 2021

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

Companies are not at liberty to select just any subcontractor or third-party service provider without ensuring that those companies are eligible to receive and use the information being provided. Additionally, relying upon a past review may not be sufficient since staff and/or company ownership can change, and eligibility requirements such as SAM, JSP, ITAR, and/or SPRS can expire. Each contract has requirements that define eligibility and qualifications necessary for the types of information involved. Therefore, it is important for both contract compliance and information security perspectives that companies be aware of these requirements and develop a system that provides current information both for new and existing supply chain members.

This webinar will review a variety of scenarios, regulations, requirements, and analysis required. Additionally, suggestions will be provided with respect to best practices and documentation that should be used for contract compliance.

- Requirements
- Status
- Vendor – supply chain
- Changes
- Internal issues
- External issues

Current requirements

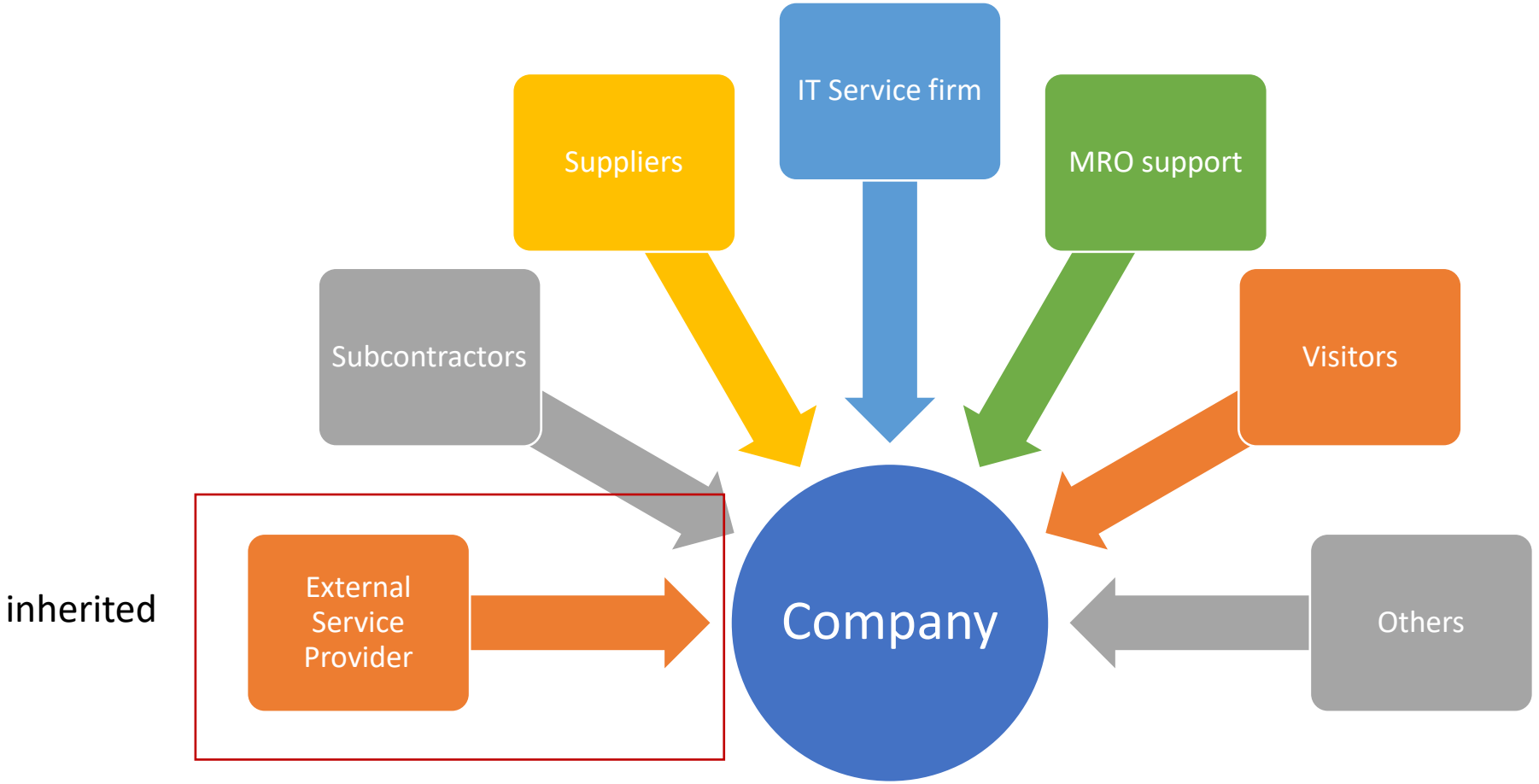
- Federal –
  - 52.204-21 -- Basic Safeguarding of Covered Contractor Information Systems (Jun 2016)
- DoD –
  - 252.204-7012 --SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2019)
  - 252.204-7019 -- NOTICE OF NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS (NOV 2020)
  - 252.204-7020 -- **NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS** (NOV 2020)
    - DoD Basic Assessment Methodology
      - CAGE, Date Assessment Performed, SSP name (if more than one), Brief Architecture Description, Summary Score, Date a score of 110 will be achieved – upload to SPRS
      - Flow down – assessment can be performed and emailed to webptsmh@navy.mil for posting to SPRS.
- Other requirements listed in solicitation/contract* -- RFQ's

- 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.

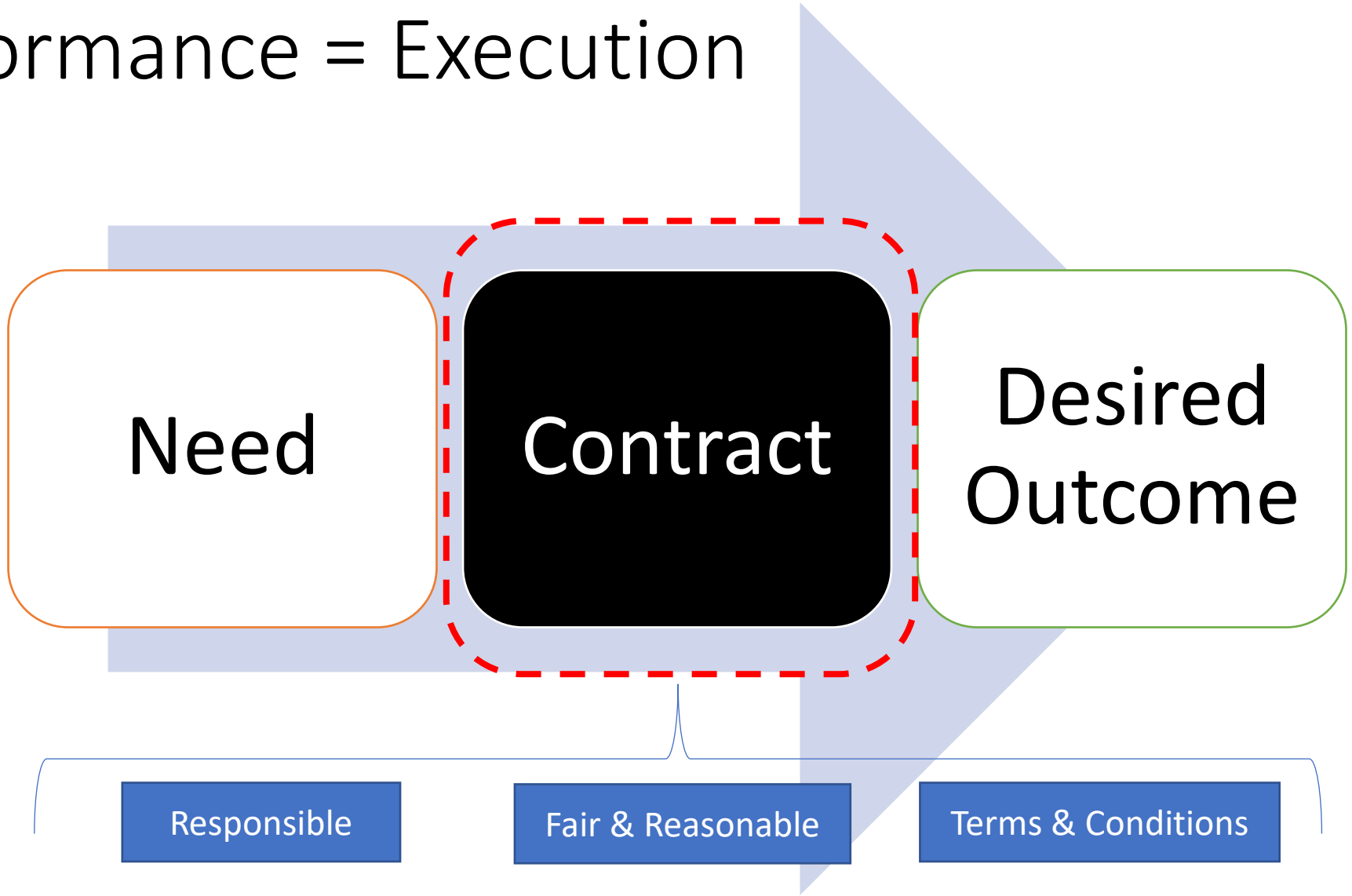
Significant questions

- How do you know?
- Can you show?
- Do you have documentation?
- What triggers an update?
- Are violations tracked?
- Do you have policies and procedures?
- How are staff members informed?
- What type of training is conducted?
- How is network traffic monitored?
- Does the company have cyber insurance?
  - What kind(s)?

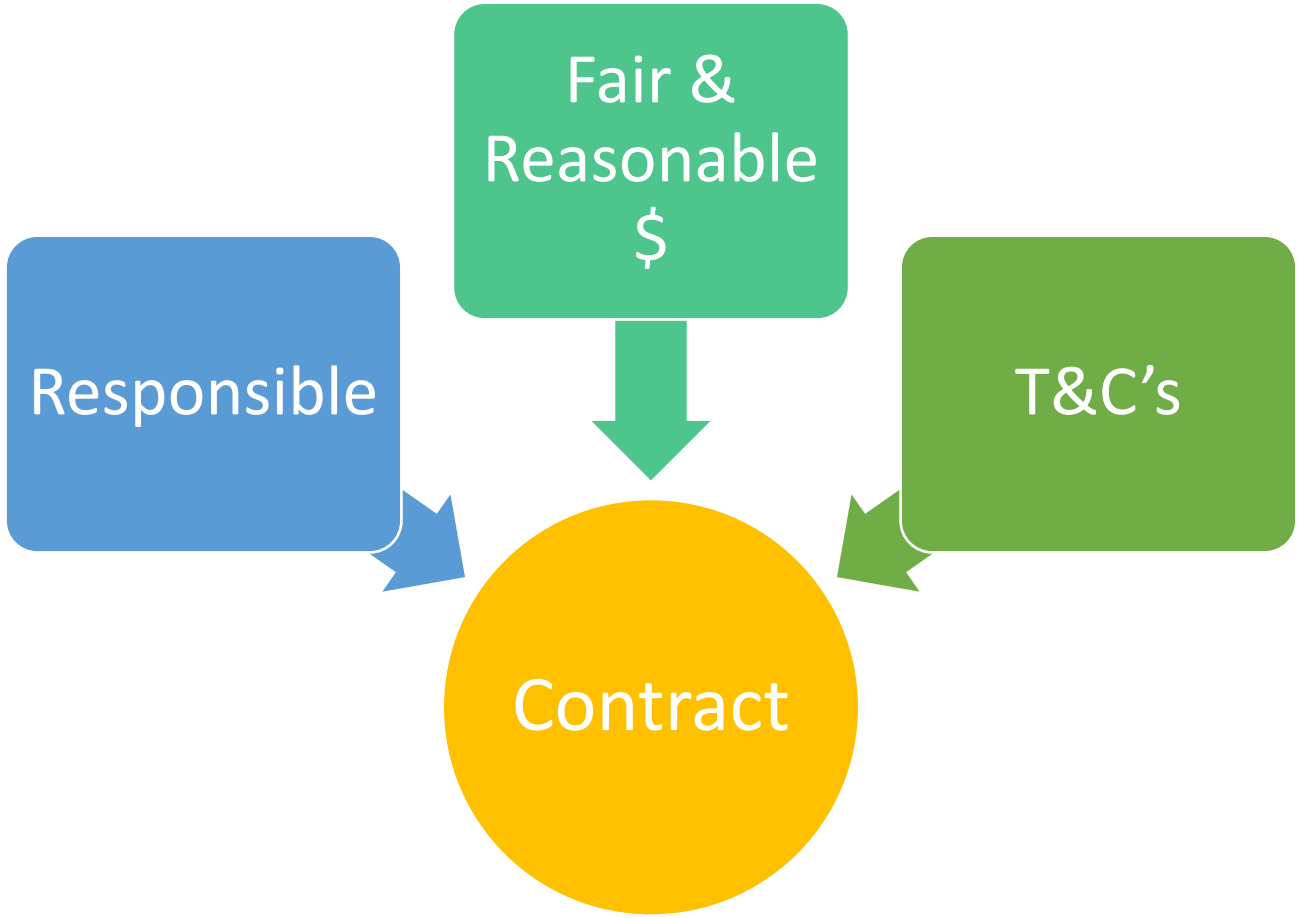
Managing Relationships and Information Security/flow



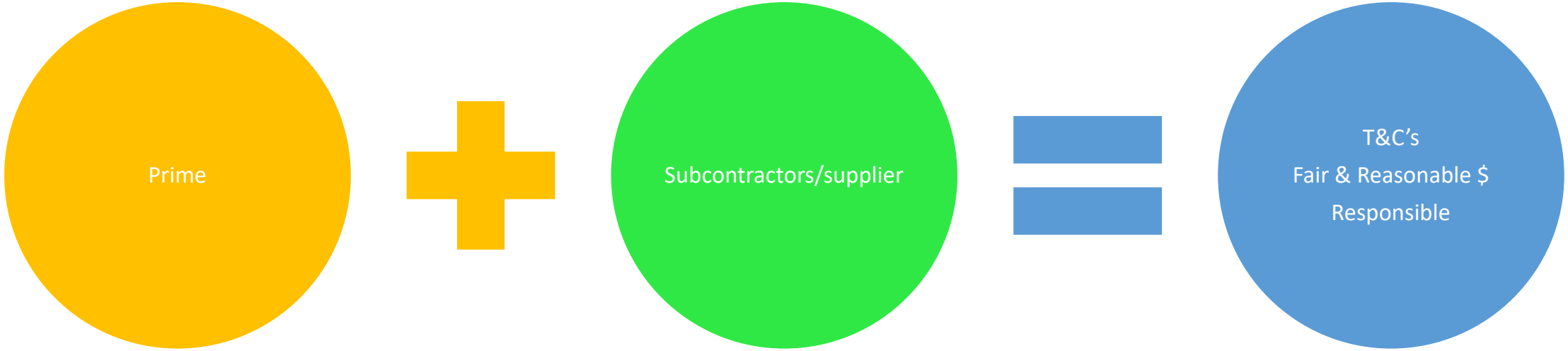
Performance = Execution



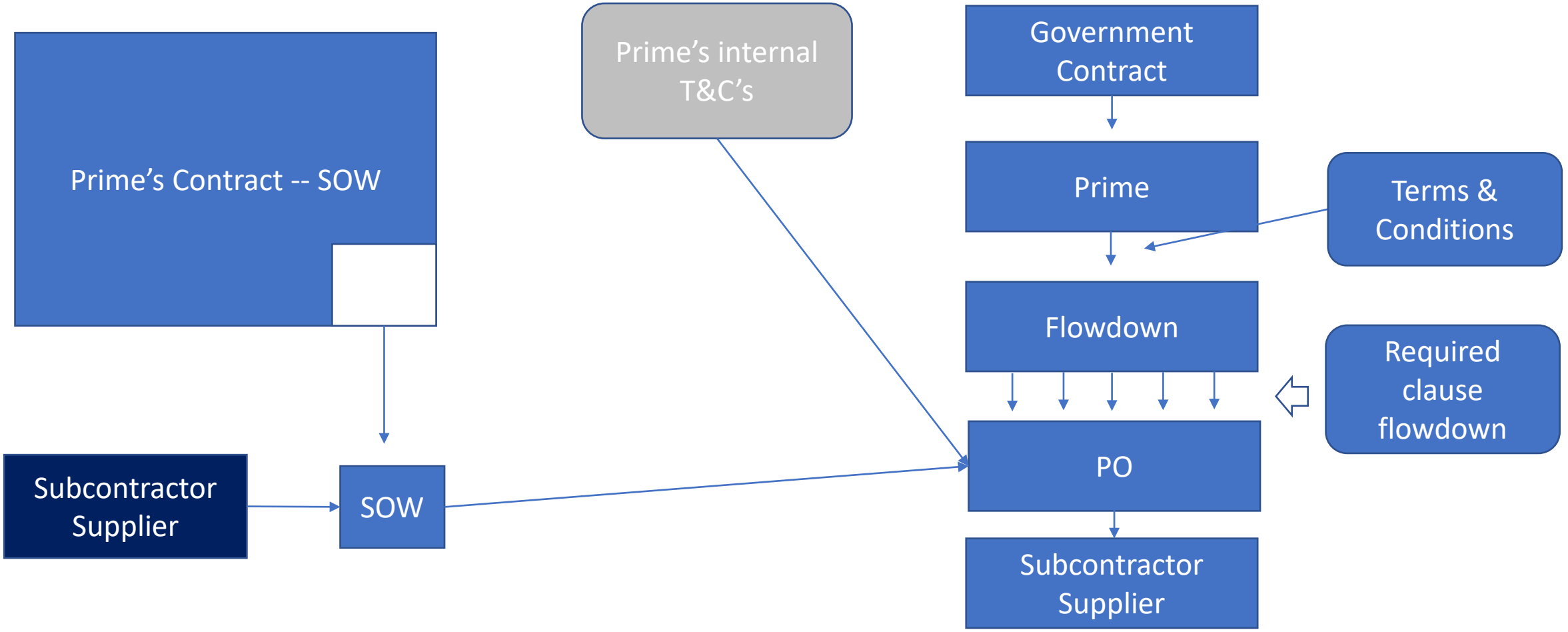
Contracting Triangle



Contracting Equation



Functions of a Subcontracting agreement



Subcontracting Agreement – don’ts

- Flowdown all T&C’s – you, the prime are not the federal government
  - T&C’s such as Termination for Convenience are federal authority but not in general automatic on a B2B level
- All T&C’s in the prime’s contact
  - To do so would require the prime to attach – make available it’s contract and typically a prime will not do so. As a result, the sub cannot see the requirements.
- Wording – from the Prime and acceptance by the sub – if the prime states, this agreement can be cancelled at any time – is there an enforceable contract? If the prime’s has language that “over-reaches” or other requirements – be aware, consult an attorney.

Responsible

(a) Purchases shall be made from, and contracts shall be awarded to, *responsible prospective contractors* only.

(b) No purchase or award shall be made unless the contracting officer makes an affirmative determination of responsibility. In the absence of information clearly indicating that the prospective contractor is responsible, the contracting officer shall make a determination of nonresponsibility. If the prospective contractor is a small business concern, the contracting officer shall comply with subpart 19.6, Certificates of Competency and Determinations of Responsibility. (If Section 8(a) of the Small Business Act (15 U.S.C.637) applies, see subpart 19.8.)

(c) The award of a contract to a supplier based on lowest evaluated price alone can be false economy if there is subsequent default, late deliveries, or other unsatisfactory performance resulting in additional contractual or administrative costs. While it is important that Government purchases be made at the lowest price, this does not require an award to a supplier solely because that supplier submits the lowest offer. A prospective contractor must affirmatively demonstrate its responsibility, including, when necessary, the responsibility of its proposed subcontractors.

FAR 9.103 - Responsible

Subcontractor Responsibility

- (a) Generally, prospective prime contractors are responsible for determining the responsibility of their prospective subcontractors (but see 9.405 and 9.405-2 regarding debarred, ineligible, or suspended firms). Determinations of prospective subcontractor responsibility may affect the Government's determination of the prospective prime contractor's responsibility. A prospective contractor may be required to provide written evidence of a proposed subcontractor's responsibility.

FAR 9.104-4 Subcontractor responsibility.

Responsible – General Standards

To be determined responsible, a prospective contractor must-

(a) Have adequate financial resources to perform the contract, or the ability to obtain them (see 9.104-3(a));

(b) Be able to comply with the required or proposed delivery or performance schedule, taking into consideration all existing commercial and governmental business commitments;

(c) Have a satisfactory performance record (see 9.104-3 (b) and subpart 42.15). A prospective contractor shall not be determined responsible or nonresponsible solely on the basis of a lack of relevant performance history, except as provided in 9.104-2;

(d) Have a satisfactory record of integrity and business ethics (for example, see subpart 42.15);

(e) Have the necessary organization, experience, accounting and operational controls, and technical skills, or the ability to obtain them (including, as appropriate, such elements as production control procedures, property control systems, quality assurance measures, and safety programs applicable to materials to be produced or services to be performed by the prospective contractor and subcontractors). (See 9.104-3(a).)

(f) Have the necessary production, construction, and technical equipment and facilities, or the ability to obtain them (see 9.104-3(a)); and

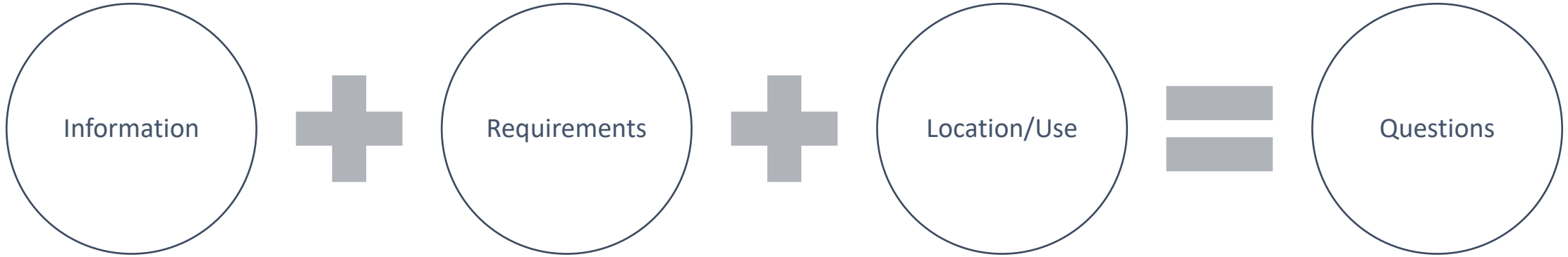
(g) Be otherwise qualified and eligible to receive an award under applicable laws and regulations (see also inverted domestic corporation prohibition at 9.108).

Key Assessment Areas

- ***Invoicing/Cost Control.*** Is the contractor effective in forecasting, managing, and controlling contract/order cost and keep within the total estimated cost? Were billings current, accurate and complete?
- ***Timeliness (schedule/delivery).*** Is the contractor on schedule to meet contractual requirements? Did the contractor meet the contractual delivery requirements? Does the contract include a reward for early delivery, or a penalty for late delivery?
- ***Quality of performance and deliverables.*** Do the supplies or services meet the requirements? Do they conform to the contract specifications, standards, PWS/SOW/SOO, and quality assurance plan?
- ***Business relations.*** Is the contractor responsive, professional, and courteous?
- ***Management of key personnel.*** Are technical experts highly qualified and effective in performing the required services? Do they meet the skill level stated in the contract? Are an appropriate number of personnel assigned to the project? Do delivered supplies reflect the skill and standardization required by the user?
- ***Customer satisfaction.*** Will the requiring activity be satisfied in terms of cost, quality, and timeliness of the delivered supplies or services? What percentage of the deliverable meets the user's expectations? How long has the contractor taken to address any user complaints? How many user complaints have there been?
- ***Compliance.*** Has the contractor complied with, for example, Occupational Safety and Health Administration, Environmental Protection Agency, and Department of Labor regulations or local standards?

https://www.acq.osd.mil/dpap/policy/policyvault/USA001435-22-DPC.pdf; DoD Contracting Officer Representatives Guidebook; § 7.5

Key Considerations



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

Know who you are working with - Login.gov

1. Your State-Issued ID. You can upload a photo by phone or by computer.
   Don't have a state issued ID?
2. A phone or computer with a camera to take a photo of yourself (This feature is not currently enabled or required.)
3. Social Security Number
4. A phone number on a phone plan that is in your name.
   - If you do not have a phone plan that is in your name, we can send you the verification code by mail which takes approximately 3-5 days.

If you are missing any of this information, please contact the government agency you are trying to access.

https://login.gov/help/verify-your-identity/how-to-verify-your-identity/

Identity Verification Requirements

List A: IDs to Confirm Identity and Citizenship

- U.S. passport
- U.S. certificate of naturalization
- Certificate of citizenship issued by USCIS
- Passport issued by country of citizenship

List B: Government-issued Photo ID to Confirm Identity

- Federal-issued driver's license
- State-issued driver's license or state ID card
- U.S. federal government employee ID
- DoD Common Access Card (CAC) with photo

List C: U.S. Citizens Only, to Confirm Identity and Citizenship

- Certification of Report of Birth (DoS form DS-1350)
- Consular Report of Birth Abroad (DoS form FS-240)
- Certified birth certificate issued by city, county or state of birth in the U.S.

https://www.identrust.com/sites/default/files/resources/identrust-dod-med-assur-cert-ds-en_1.pdf & DFARS 252.204-7012

Confirm Details

- POINT OF CONTACT (POC) VERIFICATION
-
- Is XXXXXXXXXXX an owner, officer, employee or partner of the company/organization? We do NOT accept a Government Business POC listed as the company name, department, division or any federal agency contracting official.
- Please confirm that the email provided, XXXXXXX@hotmail.com, is a valid email related to the business operations of the entity registering and listed specifically to the individual listed as the POC. This should NOT be a generic group email. ***NOTE*** If an email address is found not to be following the domain format listed on the company's website, then DLA CAGE reserves the right to question the validity of the contact information and return the SAM registration without further processing. Private email domains, such as Gmail, Yahoo, Yandex, Protonmail etc are not recommended to be used if your company has its own domain.
- Please confirm that xxx-xxx-xxxx is a valid number related to the business operations of the entity registering and reaches specifically the individual listed as the POC. This should NOT be a generic sales/marketing number without at least listing the phone extension to the individual listed. ***NOTE*** If DLA CAGE calls the phone number listed and finds that it is disconnected or invalid, we reserve the right to not process the SAM registration. If the phone number is listed to someone other than the POC listed, then DLA CAGE reserves the right to question the validity of the contact information and return the SAM registration without further processing.

Selected text from DLA email to a business

DLA EXPORT CONTROL TECHNICAL DATA MANAGEMENT QUESTIONNAIRE

- (5) Please provide the physical address of the personal computer or server where the export-controlled data will be stored.
- Also, please provide the Media Access Control (MAC) address of the personal computer or server.
- For American firms, the personal computer or server must be physically located in the United States. Individuals with access to the designated personal computer or server must be United States citizens or lawful permanent residents of the United States. For Canadian firms, the personal computer or server must be physically located in Canada. Individuals with access to the designated personal computer or server must be Canadian citizens or lawful permanent residents of Canada.

(m) Subcontracts. The Contractor shall—

- (1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties.

The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

252.204-7020 Paragraph (g) Subcontracts

(1) The Contractor shall insert the substance of this clause, including this paragraph (g), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items (excluding COTS items).

(2) The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800-171 security requirements, in accordance with DFARS clause 252.204-7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment, as described in https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html, for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government.

Flowdowns besides Cyber

(g) The Contractor agrees to include the substance of this clause, appropriately modified to reflect the identity and relationship of the parties, in all first-tier subcontracts exceeding the simplified acquisition threshold in Part 2 of the Federal Acquisition Regulation, except those for commercial items or components.

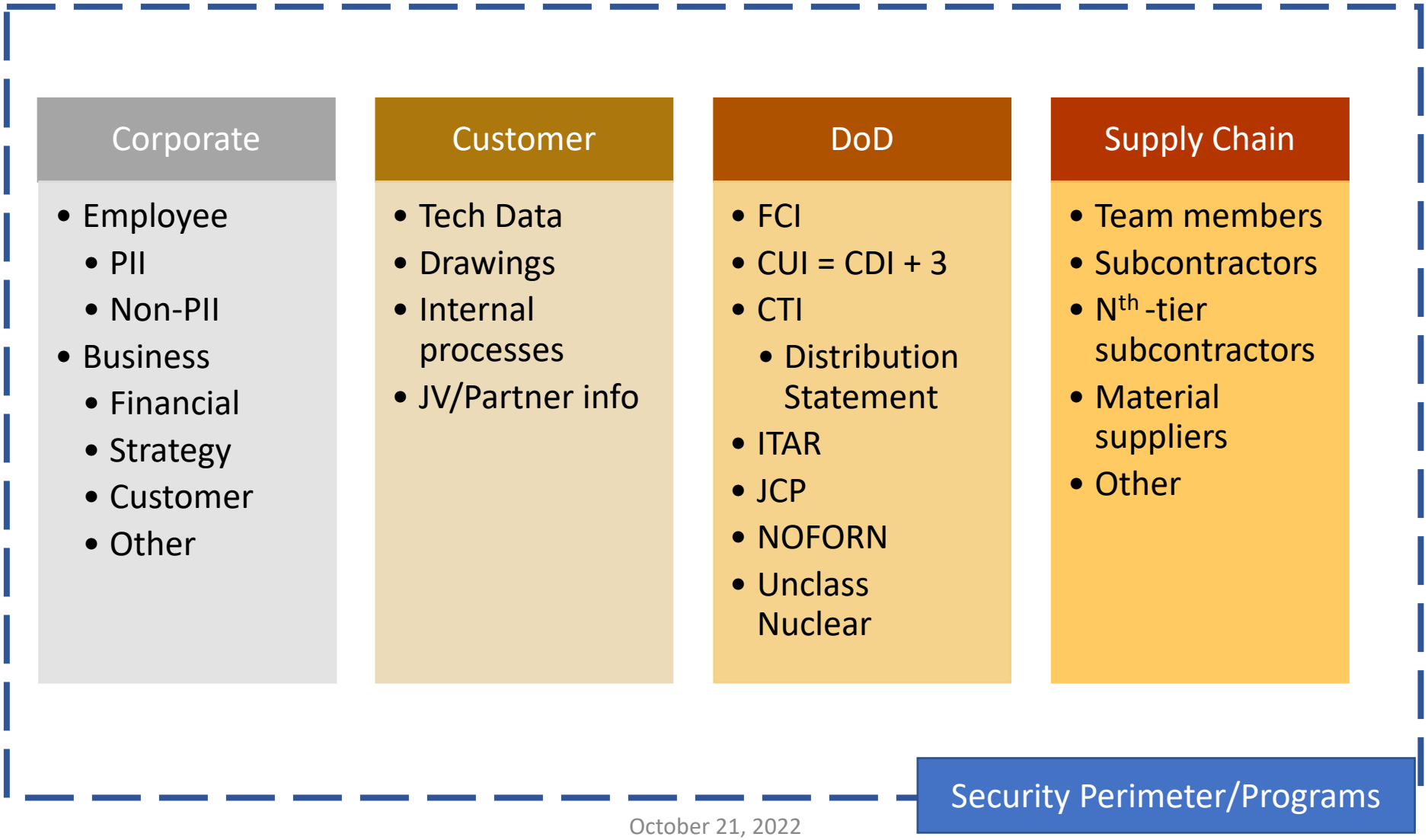
(h) Pursuant to 10 U.S.C. 2408(c), defense contractors and subcontractors may obtain information as to whether a particular person has been convicted of fraud or any other felony arising out of a contract with the DoD by contacting The Office of Justice Programs, The Denial of Federal Benefits Office, U.S. Department of Justice, telephone 301-937-1542; www.ojp.usdoj.gov/BJA /grant/DPFC.html.

252.203-7001 Prohibition on Persons Convicted of Fraud or Other Defense Contract-Related Felonies.

Handle/Share Information with Purpose

- What information do we have?
- What information do we use?
- With whom is information being shared?
- What information is being shared?
- What are the handling requirements?
- Where – how is the information being shared?
- When – normal hours / off hours
- Why is it being shared?
- What systems (software) do we have?
- Other questions ---

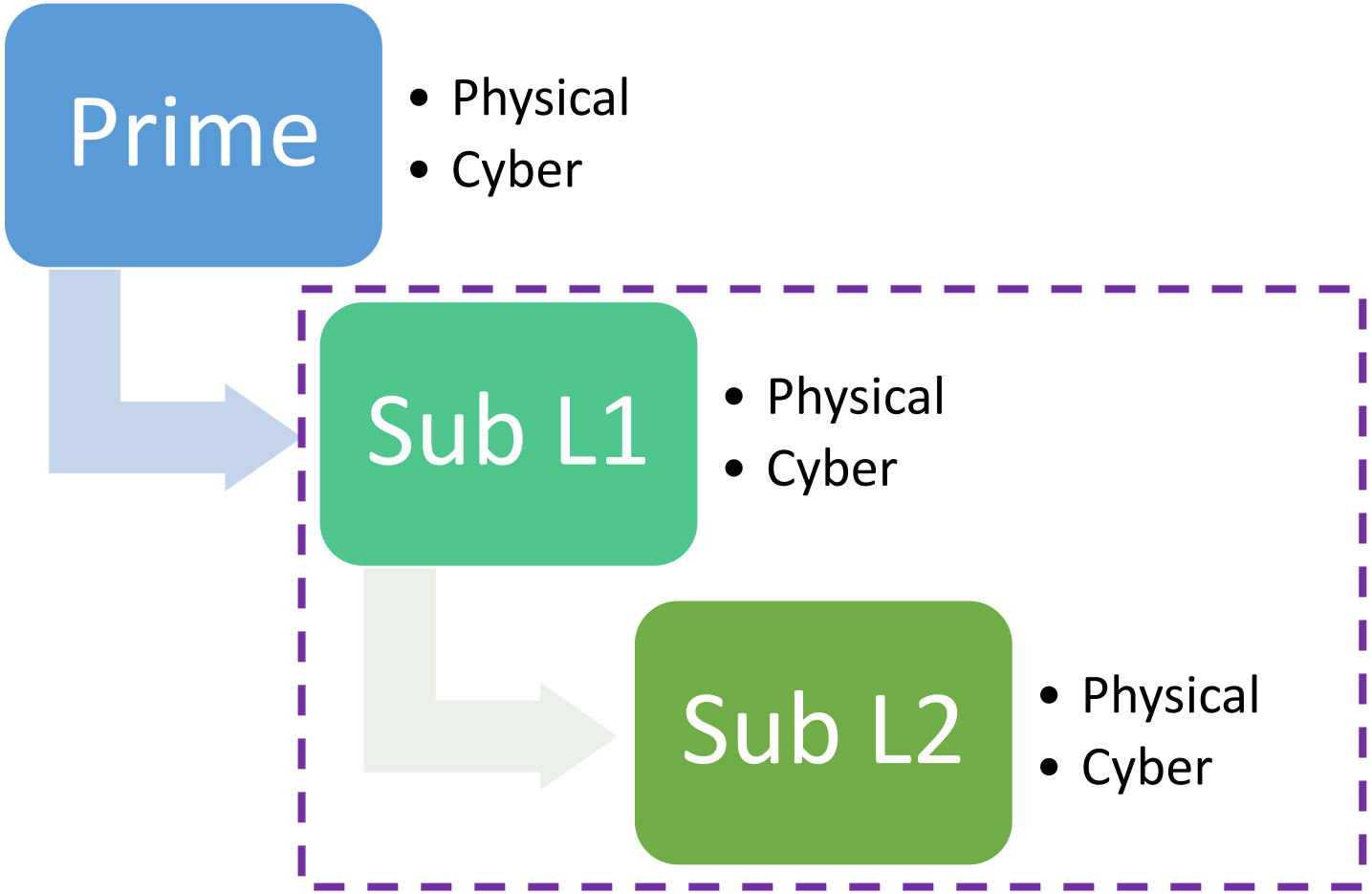
General Information Sources



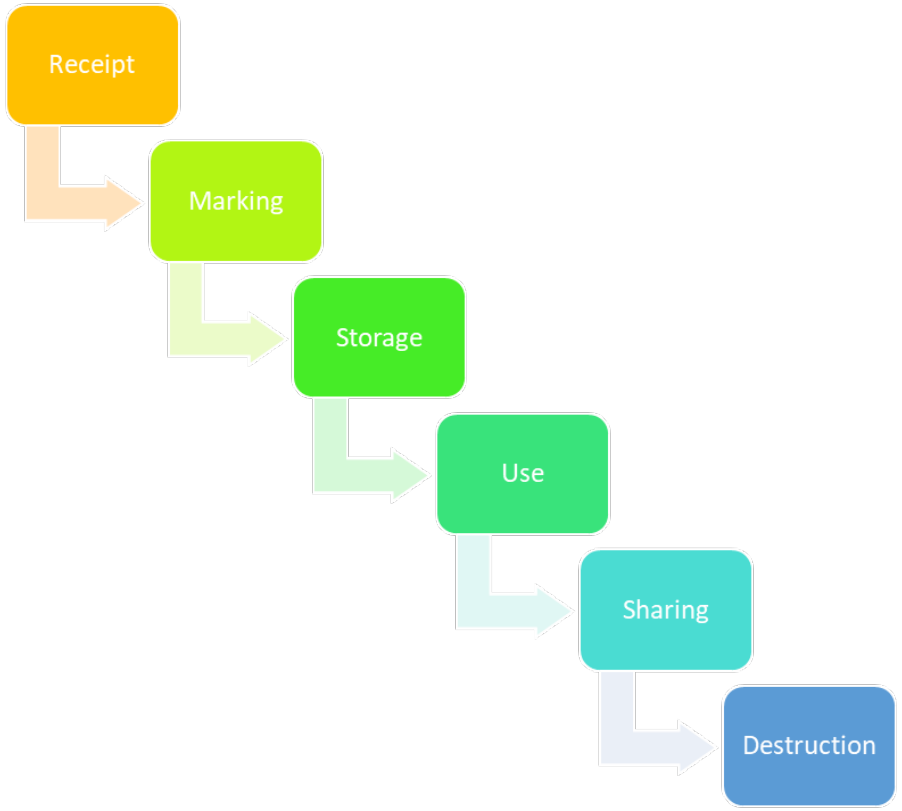
Determine scope and applicable criteria

- 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

Map & Understand Supply Chain



Where v. How drives the questions, evidence



- Auditing
- Awareness
- Controls
- Deliverables
- Information – source(s)
- Monitor – test
- Questions to KO, other
- Training
- Transmittal registry
- Update procedures

M.N. Violante, WPI – Nov 2017

Risk Management

a. Cybersecurity Risk Management. Managing cybersecurity risks is a complex, multifaceted undertaking that requires the involvement of the entire organization, from senior leaders planning and managing DoD operations, to individuals developing, implementing, and operating the IT supporting those operations. Cybersecurity risk management is a subset of the overall risk management process for all DoD acquisitions as defined in Reference (at), which includes cost, performance, and schedule risk associated with the execution of all programs of record, and all other acquisitions of DoD. The risk assessment process extends to the logistics support of fielded equipment and the need to maintain the integrity of supply sources.

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf

Identify key elements- what is needed?

Business Culture & Risk Management

- Ensure that senior leaders/executives recognize the importance of managing information security risk and establish appropriate *governance* structures for managing such risk;
- Ensure that the organization's risk management process is being effectively conducted across the three tiers of organization, mission/business processes, and information systems;
- Foster an organizational climate where information security risk is considered within the context of the design of mission/business processes, the definition of an overarching enterprise architecture, and system development life cycle processes; and
- Help individuals with responsibilities for information system implementation or operation better understand how information security risk associated with their systems translates into organization-wide risk that may ultimately affect the mission/business success.

NIST Special Publication 800-39 Managing Information Security Risk Organization, Mission, and Information System View, pg. 1

5 Questions CEOs Should Ask About Cyber Risks

1) How Is Our Executive Leadership Informed About the Current Level and Business Impact of Cyber Risks to Our Company?
2) What Is the Current Level and Business Impact of Cyber Risks to Our Company? What Is Our Plan to Address Identified Risks?
3) How Does Our Cybersecurity Program Apply Industry Standards and Best Practices?
4) How Many and What Types of Cyber Incidents Do We Detect In a Normal Week? What is the Threshold for Notifying Our Executive Leadership?
5) How Comprehensive Is Our Cyber Incident Response Plan? How Often Is It Tested?

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?

Define 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

Ask the right questions?

- **Do you have a driver's license?**

- How long have you had a license?
- How frequently do you drive? – city or rural
- Have you had any accidents?
- Have you had any tickets?

Export your internal review process

- Apply your company’s internal review framework

Assess corporate culture & philosophy

- Leadership – engaged, interested
- Memberships – ISAC, other industry group
- Efforts mechanical?
- Assess strengths – weaknesses
- Internal business communications
- Logging, logs, analysis, investigation, internal reporting

Evaluation - strategies

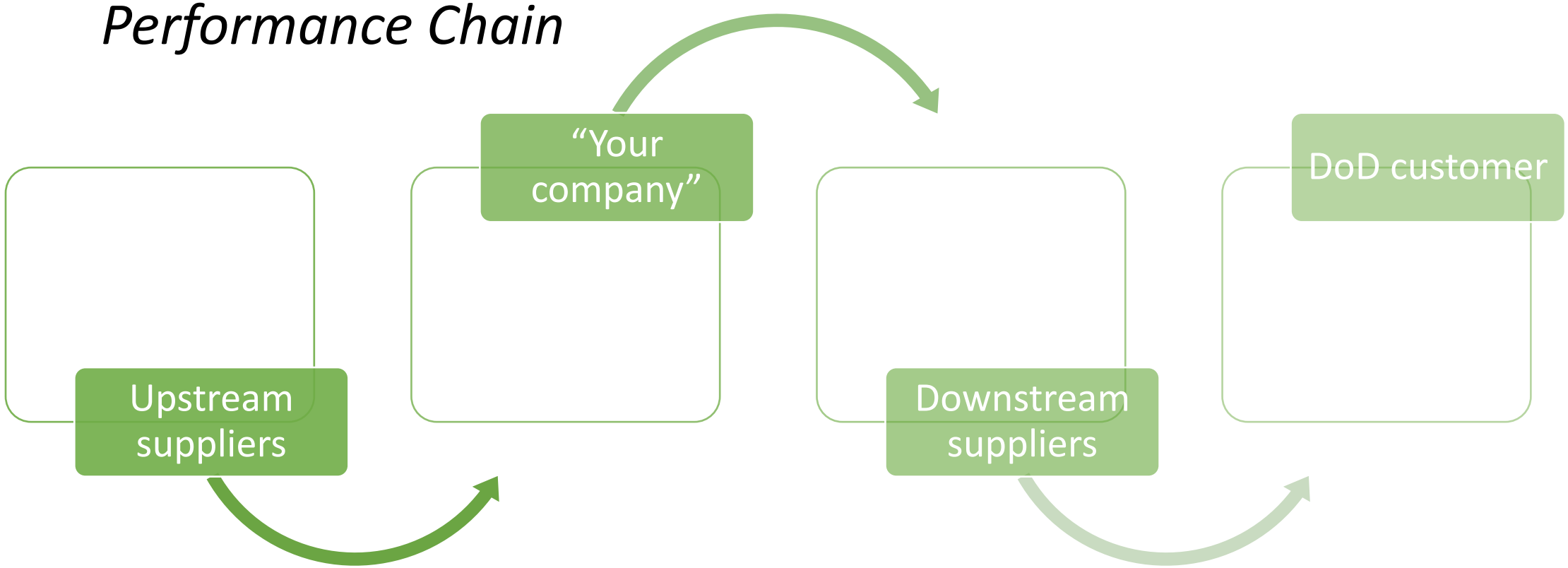
- Who will conduct?
- Consistency
- Questionnaire
- Site Visit
- Interviews
- Attend training
- Evaluate – assess the next tier
- As an alternative
  - Ask about their supply chain
  - How do they identify subcontractors/suppliers?
  - How do they vet these companies?

Create an Initial Assessment

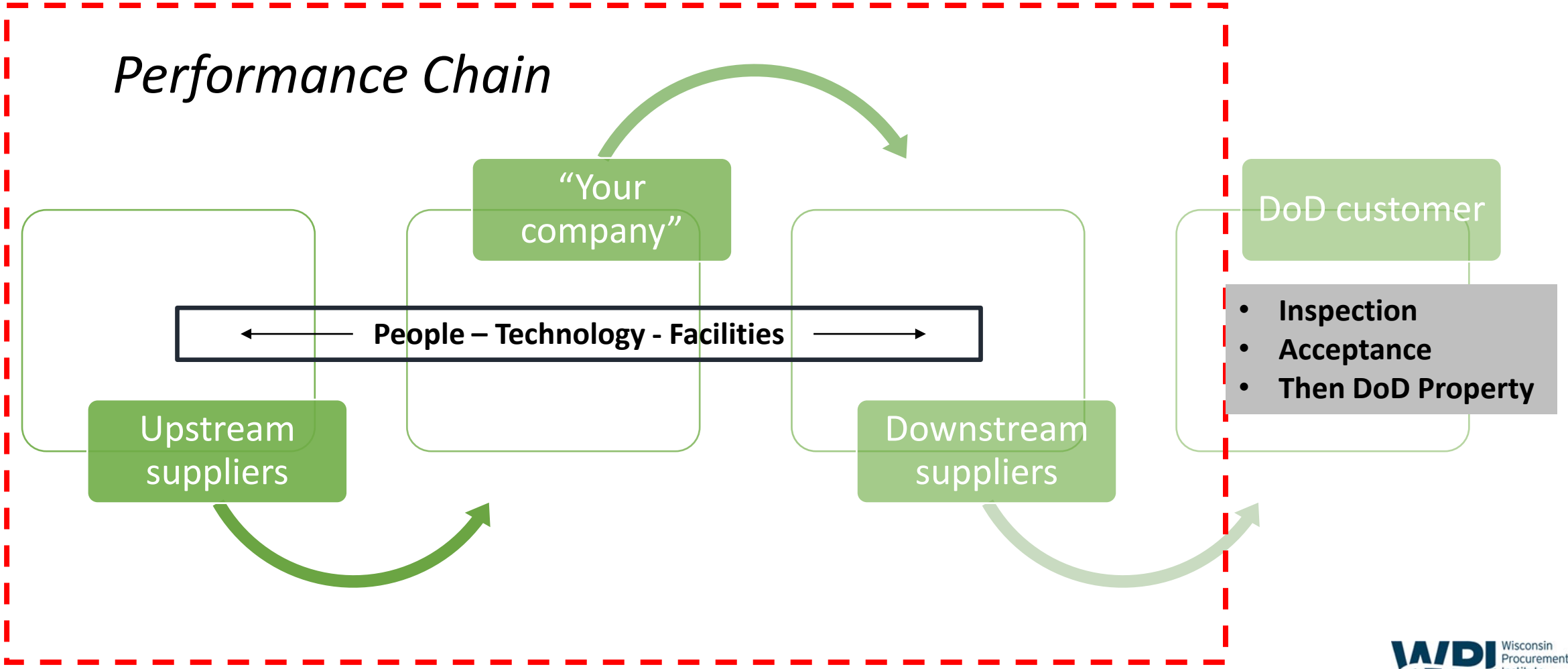
- Year first registered in SAM
- Date projected for achieving 110
- Date of Assessment
- Number of subsequent Assessments
- % increase in Summary Score
- Uses the Cloud?
- Third party IT support?
- Types of information handled/processed
- Show example of a “dummy” email forwarding CUI
- Review sensitive information Transmittal Log

Key Idea – Supply Chain – Not company

Performance Chain



Key Idea – Security concerns



Be aware of applicable Scope

Asset Type	Security Protection Asset Examples
People	• Consultants who provide cybersecurity service • Managed service provider personnel who perform system maintenance • Enterprise network administrators
Technology	• Cloud-based security solutions • Hosted Virtual Private Network (VPN) services • SIEM solutions
Facility	• Co-located data centers • Security Operations Centers (SOCs) • Contractor office buildings

Security Protection Assets are part of the assessment scope and are required to conform to applicable CMMC practices, regardless of their physical or logical placement.

https://www.acq.osd.mil/cmmc/docs/Scope_Level2_V2.0_FINAL_20211202_508.pdf

Identify general Risk Vectors

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

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

Review their subcontracting T&C's

- Flow down clauses
- Reporting
- Communications
- Training
- Cyber Incident Identification & Reporting
- Data sharing agreement
- Cloud usage/data sharing [1]

1 https://www.nist.gov/itl/57-sharing-access-data-cloud

Determine what plans are maintained?

- Business Continuity
- Data protection
- Data storage
- Data sharing
- Data marking
- Data type inventory
- Data usage agreement – internal
- Data type – access list
- Information security – exercise plan
- Information security – training requirements

252.204-7000 Disclosure of Information.

As prescribed in 204.404-70 (a), use the following clause:

DISCLOSURE OF INFORMATION (OCT 2016)

(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

204.404-70 Additional contract clauses.

(a) Use the clause at 252.204-7000 , Disclosure of Information, in solicitations and contracts when the contractor will have access to or generate unclassified information that may be sensitive and inappropriate for release to the public.

(b) Use the clause at 252.204-7003 , Control of Government Personnel Work Product, in all solicitations and contracts.

Test for familiarity with requirements

52.204-21 Basic Safeguarding of Covered Contractor Information Systems.

As prescribed in 4.1903 , insert the following clause:

BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (JUN 2016)

(a) *Definitions.* As used in this clause–

Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

Additionally -

(1) The DoD originator or authorized CUI holder must ensure a prepublication and security policy review is conducted, pursuant to the standard DoD Component process, before CUI is approved for public release, which includes publication to a publicly accessible website.

DoDI 5200.48, March 6, 2020; page 13; 3.3 a (1)

5.3. REQUIREMENTS FOR DOD CONTRACTORS

a. Whenever DoD provides information to contractors, it must identify whether any of the information is CUI via the contracting vehicle, in whole or part, and mark such documents, material, or media in accordance with this issuance.

b. Whenever the DoD provides CUI to, or CUI is generated by, non-DoD entities, protective measures and dissemination controls, including those directed by relevant law, regulation, or government-wide policy, will be articulated in the contract, grant, or other legal agreement, as appropriate.

c. DoD contracts must require contractors to monitor CUI for aggregation and compilation based on the potential to generate classified information pursuant to security classification guidance addressing the accumulation of unclassified data or information. DoD contracts shall require contractors to report the potential classification of aggregated or compiled CUI to a DoD representative.

d. DoD personnel and contractors, pursuant to mandatory DoD contract provisions, will submit unclassified DoD information for review and approval for release in accordance with the standard DoD Component processes and DoDI 5230.09.

https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/DoDI%205200.48%20CUI.pdf, page 32

DoD Guidance

- Requiring delivery of the contractor's system security plan (or extracts thereof)
- Requiring the contractor to identify known Tier 1 Level suppliers
- Requesting the contractor's plan to track flow down of covered defense information and to assess DFARS clause 252.204-7012 compliance of known Tier 1 Level suppliers.

https://www.acq.osd.mil/dpap/pdi/cyber/docs/Guidance_for_Assessing_Compliance_and_Enhancing_Protections.pdf

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

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

Cloud Security

After a year when digital transformation took a quantum leap at most enterprises and remote work exploded, it's no surprise that the majority of enterprise workloads are now running in cloud-based infrastructure as a service (IaaS) and platform as a service (PaaS) offerings.

This is creating a whole new set of security challenges around managing access to your organisation's infrastructure across multiple cloud platforms—with all the various identities and configurations they bring. Studies have shown this is where security failures happen—when the combinations of identities, access entitlements and privileges break down; Gartner forecasts that will account for about three-quarters of security incidents in the cloud by 2023.

https://cloudcomputing-news.net/news/2021/mar/10/a-guide-to-privileged-access-management-the-doorman-for-the-cloud/
https://www.forbes.com/sites/forbestechcouncil/2020/11/30/dont-underestimate-the-business-risk-of-cloud-entitlements

Perimeter Defense & the Cloud

“We use the cloud”

Identity is the new perimeter

When identity becomes the security perimeter —as it does in the cloud —then privileged access is even more crucial. Not every account needs an all-access pass to the VIP rooms in your environment, not even admins. So the ability to grant granular access permissions and privileges based on who has access, who really needs it and when, is important.

If you have hundreds or thousands of privileges in the cloud and only one percent of them are in use, this leaves an enormous attack surface exposed to the bad guys. The cloud gets points for scalability and flexibility, but that means that services are constantly growing, and spinning off more identities and privileges left open to attack.

https://cloudcomputing-news.net/news/2021/mar/10/a-guide-to-privileged-access-management-the-doorman-for-the-cloud/

Don’t assume

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 5230.25, November 6, 1984; Change 2, 10/15/2018 - JCP

Preventing Uncontrolled Foreign Access

4.2. Because public disclosure of technical data subject to this Directive is tantamount to providing uncontrolled foreign access, withholding such data from public disclosure, unless approved, authorized, or licensed in accordance with export control laws, is necessary and in the national interest. Unclassified technical data that are not governed by this Directive, unless otherwise restricted, shall continue to be made available to the public as well as to State and local governments.

DoDD 5230.25, November 6, 1984; Change 2, 10/15/2018 – JCP

Controlled Technical Information

c. CTI compiled or aggregated may become classified. Such classified CTI is subject to the requirements of the National Industrial Security Program, which has different requirements than Section 252.204-7012 of the DFARS for unclassified CTI.

(1) CTI is to be marked with one of the Distribution Statements B through F, in accordance with DoDI 5230.24.

DoDI 5200.48, March 6, 2020, page 20

Identify and validate requirements

3.6. GENERAL DOD CUI PROCEDURES

b. In accordance with this issuance, every individual at every level, including DoD civilian and military personnel as well as contractors providing support to the DoD pursuant to contractual requirements, will comply with the requirements in Paragraph 3.6.f of this issuance for initial and annual refresher CUI training.

https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/DoDI%205200.48%20CUI.pdf; pages 17-18
DoDI 5200.48, March 6, 2020

Inquire about

(1) Implementation activities.

(2) Training statistics.

(3) Incident management.

(4) Implementation and sustainment costs.

(5) Self-inspection activities.

- DoD activities are required to submit a CUI Implementation Annual Report.
- Does it make sense for your vendors to do so as well?

DoDI 5200.48, March 6, 2020; page 17

CYBER FRIDAY LIVE WEBINAR SERIES

- October 21, 2022

  Vetting and Creating Agreements with Subcontractors and 3rd Party Service Providers

  CLICK HERE for additional information

  Presented by Marc Violante, Wisconsin Procurement Institute

- November 4, 2022

  Developing and Implementing Essential Security Policies, Practices, and Procedures

  CLICK HERE for additional information

  Presented by Marc Violante, Wisconsin Procurement Institute

- November 18, 2022

  Incident Identification, Reporting Requirements, and Recovery

  CLICK HERE for additional information

  Presented by Marc Violante, Wisconsin Procurement Institute

- December 2, 2022

  Designing and Using Security Exercises to Test and Improve Security Programs

  CLICK HERE for additional information

  Presented by Marc Violante, Wisconsin Procurement Institute

PRESENTED BY

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

TECHNOLOGY INNOVATION CENTER at Research Park

NCMA National Contract Management Association
WISCONSIN

ACQUISITION HOUR LIVE WEBINAR SERIES

- November 1
  Preparing for One-on-One Buyer Meetings
- November 15
  Certifications for Veteran Owned Businesses
- November 29
  The HUBZone Program – Certification Benefits and Regulations
- January 10
  The SBA 8(a) Program and Small Disadvantaged Business (SDB) Program

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
ACQUISITION HOUR

…More information and registrations at wispro.org/events

DOD SUPPLIER ROADMAP SERIES

- October 20
  Performance
- October 27
  Locating Opportunities
- November 3
  Non-Traditional Acquisition Methods
- November 10
  Information Types & Handling Procedures
- November 17
  Developing a DoD Business Strategy

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
DOD SUPPLIER ROADMAP

…More information and registrations at wispro.org/events

LOCAL GOVERNMENT SALES OPPORTUNITIES

- **October 13**
  SE WI and the Milwaukee Area - Virtual
- **October 20**
  Sales Opportunities with the City of Madison – In Person
- **November 9**
  Sales Opportunities with Dane County – In Person
- **November 10**
  Green Bay Area (Virtual)

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
LOCAL GOV'T SALES OPPS

…More information and registrations at wispro.org/events

Government Opportunities Business Day in Partnership with Truax Field/115th Fighter Wing

November 15

Including 1-1 Buyer Meetings

Wispro.org/Events

Save the date

MARKETPLACE WISCONSIN

Plus 1-1 Buyer Meetings

The Contracting Academy

Developing and Growing Government Contractors

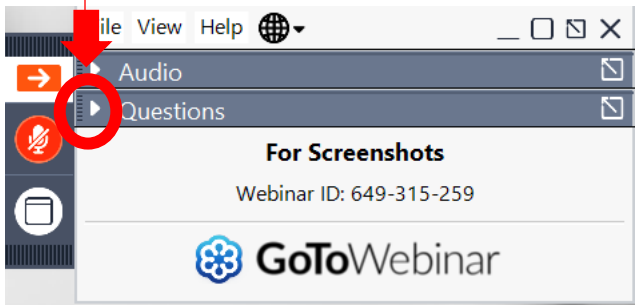
December 6-7, 2022

MarketplaceWisconsin.com

QUESTIONS?

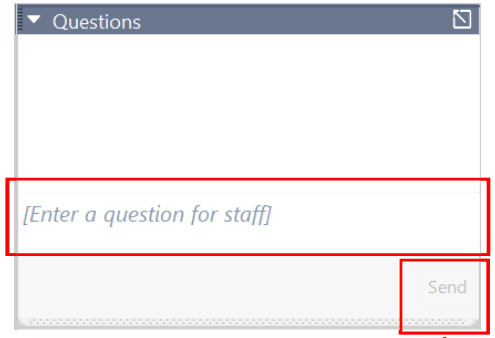
OPENING THE QUESTIONS BOX

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

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
Cyber Friday

SURVEY

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

Cyber Friday

CONTINUING PROFESSIONAL EDUCATION

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

Caroline Boettcher
carolineb@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