Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

Cyber Friday

CMMC Level 3 – Completing the steps needed to protect Controlled Unclassified Information

March 5, 2021




ABOUT WPI
SUPPORTING THE MISSION

Celebrating 34 Years of serving Wisconsin Business!

WPI 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**

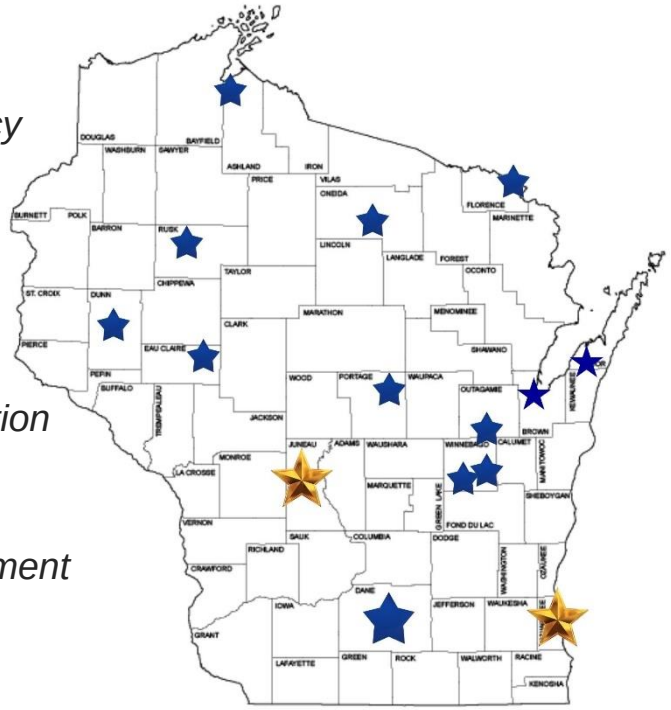
Last year WPI provided training at over 100 events and provided service to over 1,200 companies

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

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

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*
- **SUPERIOR**
  - *Small Business Dev Center; UW Superior*
- **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*
- **ASHLAND**
  - *Ashland Area Development Corporation*
- **FLORENCE**
  - *Florence County Economic Development*
- **DOOR COUNTY**
  - *NE WI Technical College*
  - *Door County Economic Development Corporation*



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

Cyber Friday

3/5/21

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

Completing the steps needed to protect Controlled Unclassified Information

Marc N. Violante

March 5, 2021

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

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

CMMC moving forward

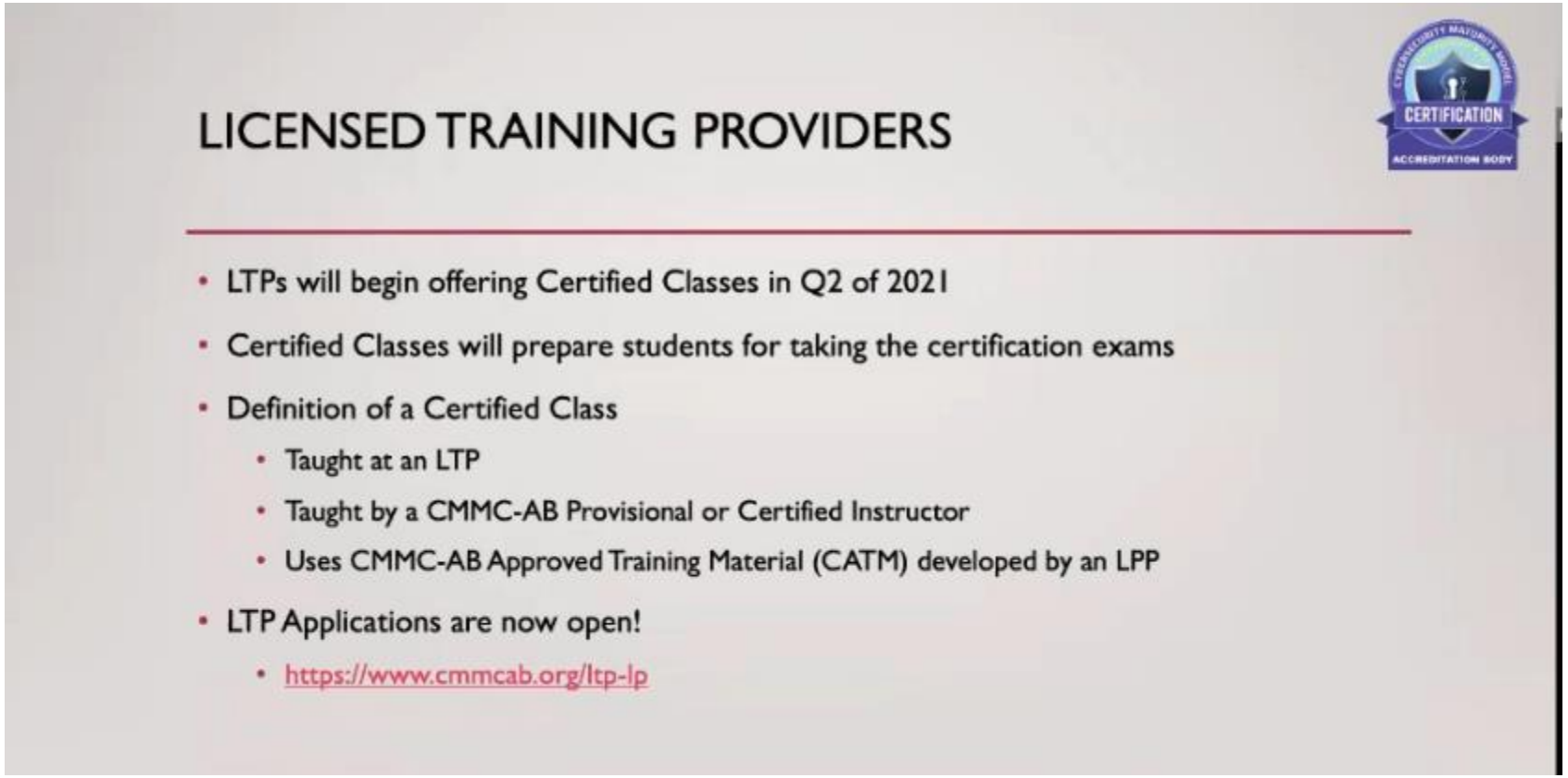
Subsequently changed to USD (A&S) CISO – Ms. Arrington*

- The Department is implementing CMMC through a phased rollout approach - FY2021-FY2025
- Until September 30, 2025, the Office of the Under Secretary of Defense for Acquisition and Sustainment must approve the inclusion of the CMMC requirement in any solicitation.
- These contracts will focus on mid-sized programs that require the contractor to process or store CUI (CMMC Level 3). Primes will be required to flow down the appropriate CMMC requirement to their subcontractors.

FY2021	FY2022	FY2023	FY2024	FY2025
15	75	250	325	475

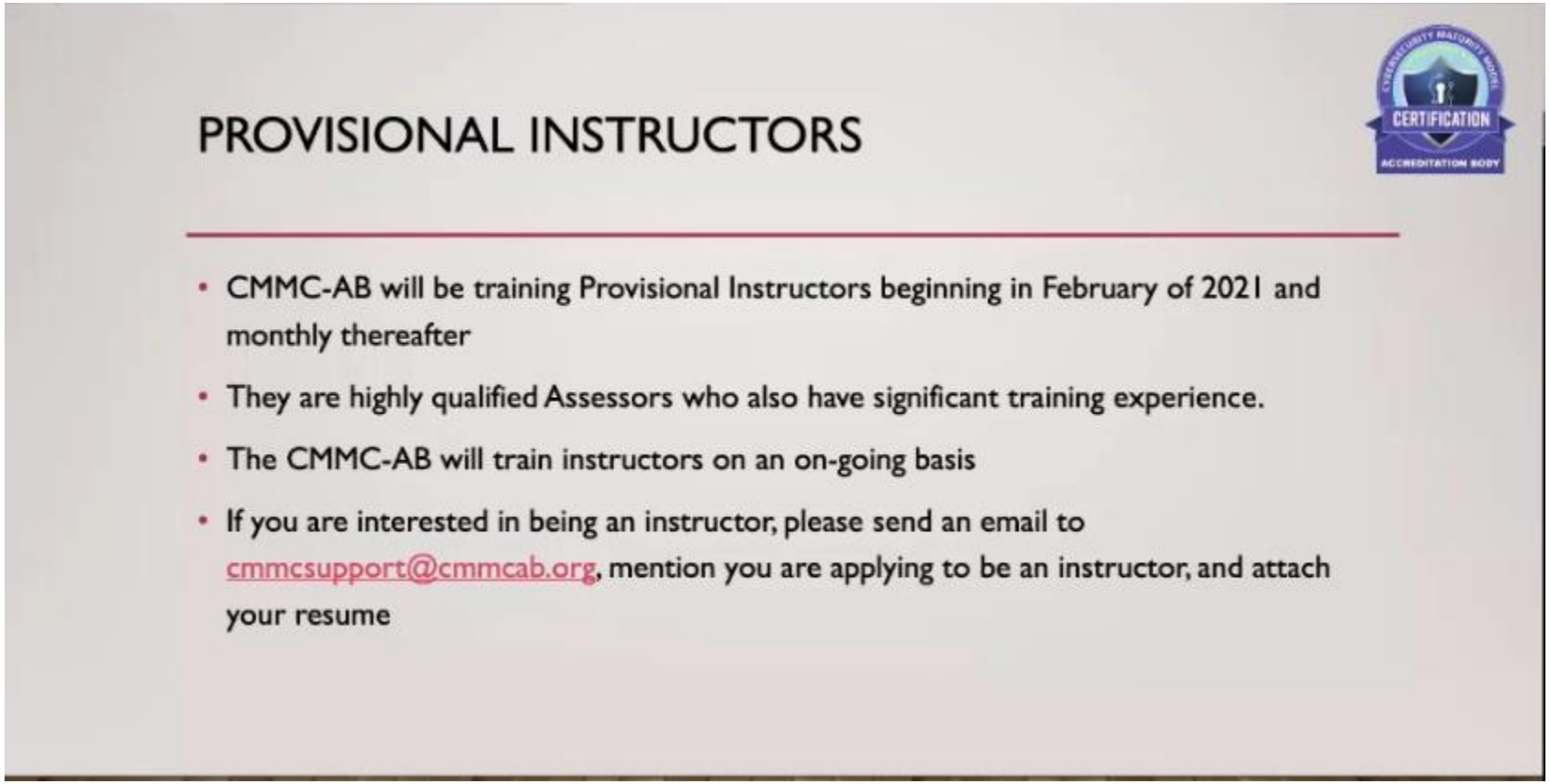
https://www.acq.osd.mil/cmmc/faq.html FAQ - 26
*CMMC-AB January Townhall, comments

CMMC-AB: update items (1)



CMMC-AB January Townhall

CMMC-AB: update items (2)



CMMC-AB January Townhall

Pilot Key Takeaways

Until 1 Oct 2025, CMMC requirements will only be included in new acquisitions with the approval of OUSD(A&S) / OCISO(A&S)

CMMC Pilot programs will include applicable CMMC requirements in RFPs

- OUSD(A&S) is not funding CMMC Pilots
- CMMC certification must be met by contract award
- CMMC certification is required of the enterprise network or particular segment where FCI or CUI is processed, stored, or transmitted in performance of the particular contract
- CMMC certification must be maintained for the duration of the contract; recertification may be necessary depending on expiration date of the CMMC certification versus the contract end date

CMMC Pilot contractors will be required to achieve CMMC Certification

- DIB Contractor enters into Business Relationship with an authorized / approved C3PAO
- CMMC certification is achieved by passing a CMMC assessment conducted by C3PAO
- All CMMC practices and processes must be implemented at the required CMMC Level
- CMMC does not allow POAMs
- If there are assessment findings, the contractor will need to remediate to achieve CMMC certification
- CMMC Certification is good for three years

OUSD(A&S) will provide guidance and support during Pilot roll-outs

10

Webinar Description

Achieving a CMMC certification is both an end and a starting point. Certification is the end of a long involved process that focuses on practices and procedures. The certification indicates that the foundational elements that are required are in place. However, certification is also a beginning as now a company is eligible to be awarded a contract, receive, handle and most importantly protect Controlled Unclassified Information. This is not only the most difficult task, it is the most important. This webinar will explore the issues related to making these transitions, what makes them difficult to achieve and possible strategies that may support these efforts.

Congratulations on achieving

Now it's time for the hard work?

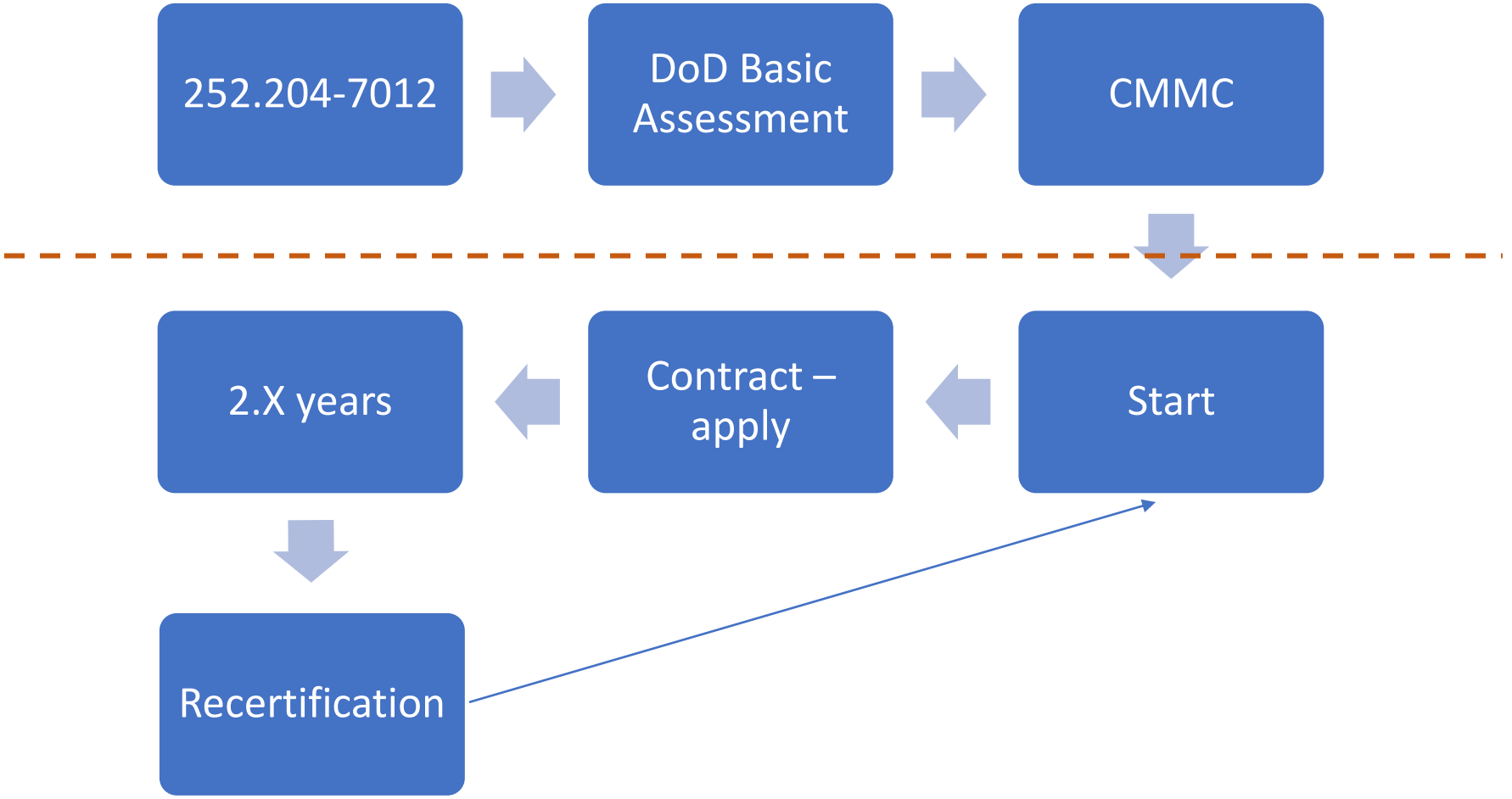
Start with the end in mind!

Avoid complacency

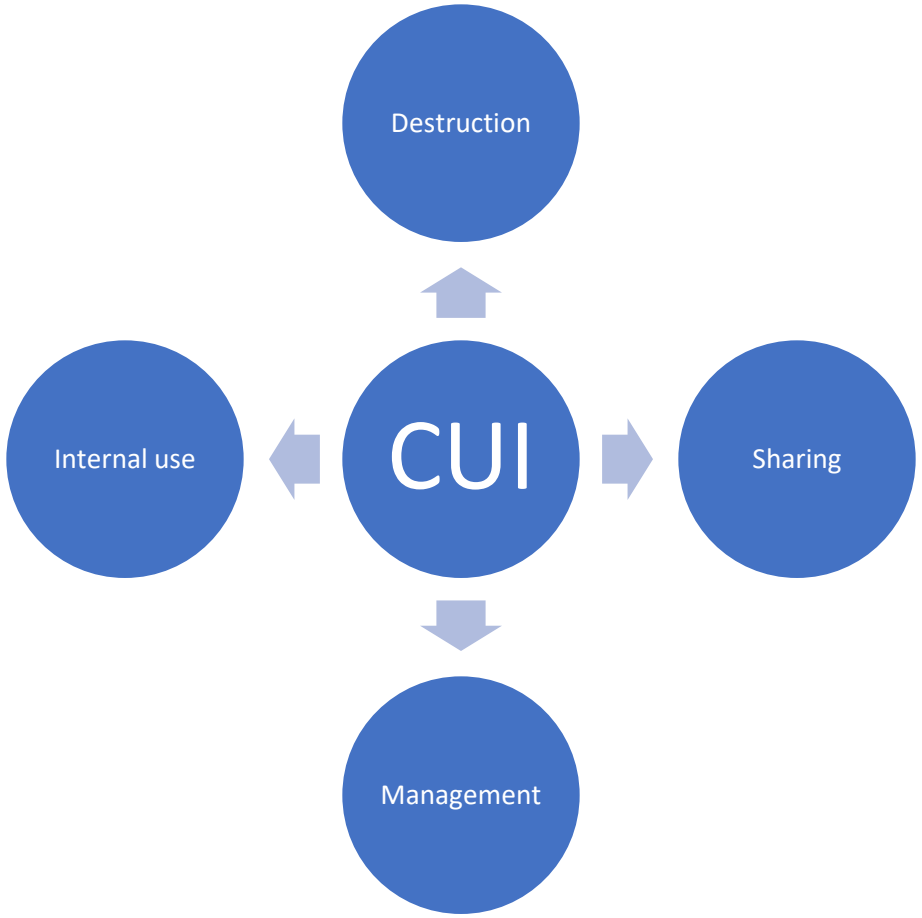
Beware of atrophying skills and competencies

What helped yesterday may not be of value today

Generalized Process



Main issues



After Certification

- Key issues will be
  - Managing the process
  - Maintaining policies, procedures and the appropriate level of institutionalization
  - Most importantly – applying; using what has been established through the certification process

Manage natural performance decline

Occasional
access/use of CUI

Routine
access/use of CUI

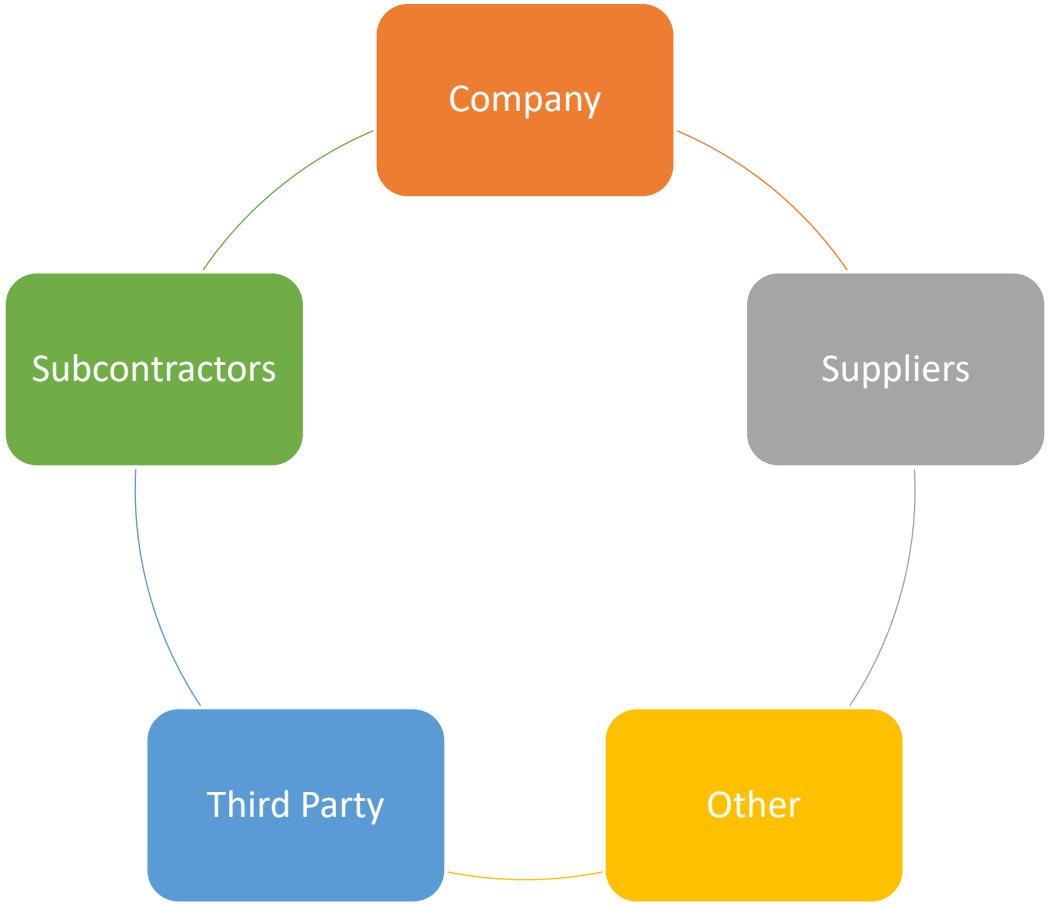
Issues – when handling CUI is not a daily event

- CUI Program Maintenance
- Keeping focus
- Keeping momentum
- Keeping current
  - Information/requirements
  - Staff
  - Systems
- Third Party management & changes
- Threat awareness
- New threats; new requirements; don’t rely upon yesterday’s fixes

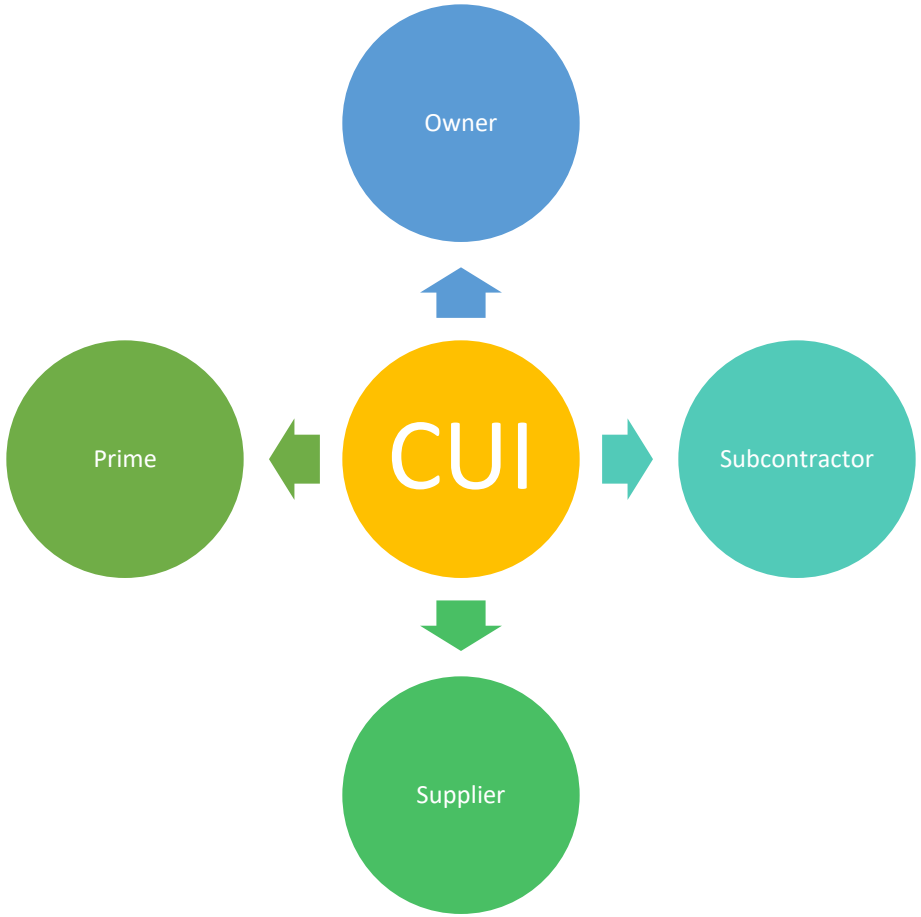
CMMC in the field means

- Using and applying CMMC & other regulations
- It means making decisions; important decisions
- Decisions that require not only familiarity with applicable source information but
- Decisions that require “fluency” with the relevant information
- Decisions that require the application of “first principles”
  - Knowledge of definitions

Define organizational management needs



Identify unique roles/responsibilities



The issue

- *Moving from theory to application*
- *Which entails*
  - *Actions*
    - *Handling*
    - *Storing*
    - *Sharing*
    - *Transmitting*
  - *Decisions*
  - *Responsibility*
  - **Integrating procedures into company processes
  - Application of First Principles

First Principles

- Information identification
- Eligibility to share
- Requirements for sharing
  - Purpose/Access
  - Recipient
  - Channel
    - Encrypted
    - USPS
    - Other
  - Destruction
  - General Premise – “don’t arbitrarily create more”
- Awareness of – CUI + CUI + CUI may equal CLASSIFIED

Applying definition/requirements

CUI SECURITY REQUIREMENTS

The recommended security requirements contained in this publication are only *applicable* to a nonfederal system or organization when *mandated* by a federal agency in a contract, grant, or other agreement. The security requirements apply to the components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.

SP 800-171, REVISION 2, page VII

Single-state Information

IMPLEMENTING A SINGLE STATE SECURITY SOLUTION FOR CUI

Controlled Unclassified Information has the *same value*, whether such information is resident in a federal system that is part of a federal agency or a nonfederal system that is part of a nonfederal organization. Accordingly, the recommended security requirements contained in this publication are consistent with and are complementary to the standards and guidelines used by federal agencies to protect CUI.

SP 800-171, REVISION 2, Chapter 2, page 6

Manage external organizational change

- Must assume that there will be/have been changes
- Staff – contact/resident expert may have moved on
- Location
  - New building
  - New location
  - New country
- Systems
- Registrations/certifications
- Their third parties
- Ownership
- Other

HUGE

Decisions – specific case or broader?

- Process
- Resources
- Basis
- Consistency
- Documentation
- Review
- Lessons Learned
- Sharing/Training

Include

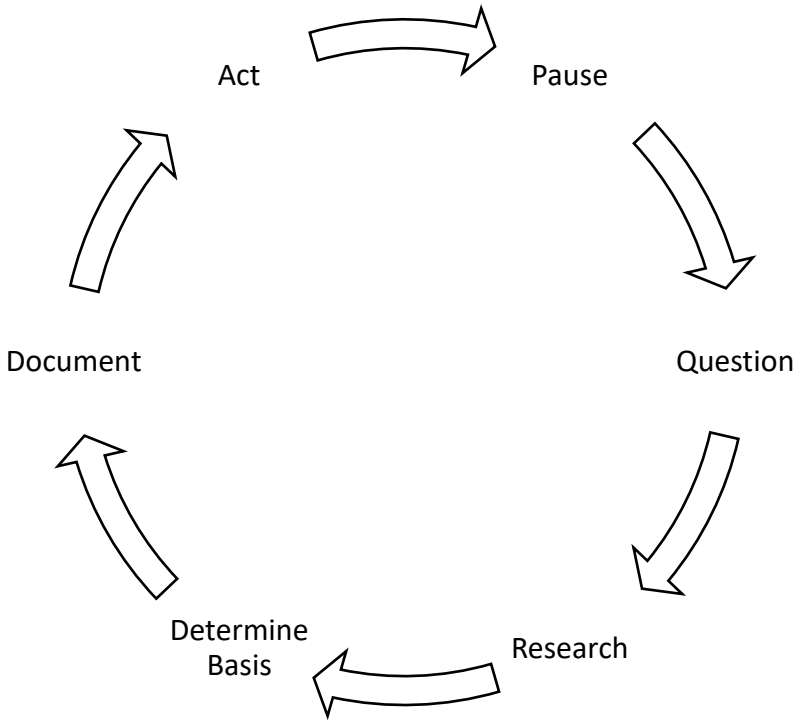
Processes
Stores
Transits

Protect

Confidentiality
Integrity
Availability

Moving forward

- In some cases – easier said than done
- Fact base may be subtly different
- Do not engage auto-pilot
- Be proactive
- Avoid/be ware of reactive compliance



Blast from the past

- In the late ‘60’s a popular saying was –
  - *“make peace not war”*

- Today with these new requirement as similar thought/saying may apply

  - *Make less not more*

252.204-7012

(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

(2) Require subcontractors to—

When and to what does/will CMMC apply

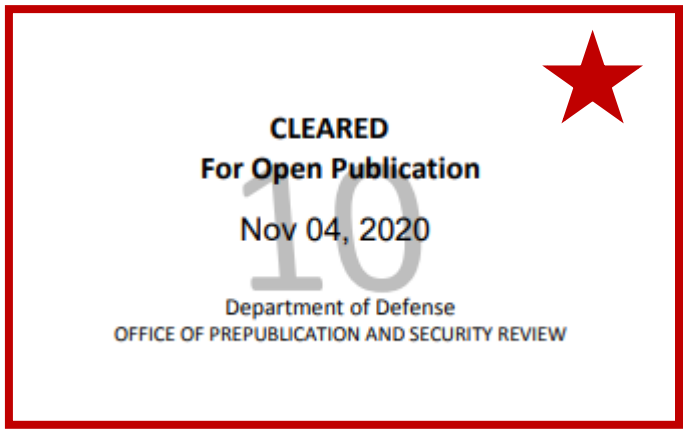
CMMC will apply to all DoD solicitations and contracts, including those for the acquisition of commercial items (except those exclusively COTS items) valued at greater than the micro-purchase threshold, starting on or after October 1, 2025. Contracting officers will not make award, or exercise an option on a contract, if the offeror or contractor does not have current (*i.e.* not older than three years) certification for the required CMMC level. Furthermore, CMMC certification requirements are

- Starting on or after October 1, 2025
- “except those exclusively COTS items”
- “valued at greater than the micro-purchase threshold”
- Contractor must have required certification (not older than 3 years) at required level

Federal Register / Vol. 85, No. 189 / Tuesday, September 29, 2020 / Rules and Regulations; page 61506

CUI Markings for Unclassified Documents

- What might a solicitation look like in the future?



Example of markings on a CUI document with portion markings.

If all the sub-paragraphs or sub-bullet points carry the same classification as the main paragraph or bullet point, portion marking is not required for the sub-paragraphs or sub-bullet points.

However, if any of the sub-paragraphs or sub-bullet points carry different classifications from the main paragraph or bullet point, portion marking is required for all the sub-paragraphs or sub-bullet points as demonstrated here.

Portion marks

Portions include subjects, titles, paragraphs and sub-paragraphs, bullet points and sub-bullet points, headings, pictures, graphs, charts, maps, reference list, etc.

The CUI designation indicator block does not require a portion mark.

Header

CUI

FOR: See Distribution

FROM: USD(I&S)

SUBJECT: (U) Information Security Considerations during Novel Coronavirus Disease (COVID-19) Mitigation Telework

(U) The President of the United States declared a National Emergency concerning the Novel Coronavirus Disease (COVID-19) outbreak on March 13, 2020. One aspect of the Federal Executive Branch's response is encouraging maximum telework flexibility. The Department of Defense is maximizing social-distancing COVID-19 mitigation efforts for all telework-ready employees.

(CUI) While the Department strongly encourages every reasonable effort to keep the DoD population and its family members and loved ones safe through social-distancing telework, we must also ensure that non-public, protected information—including Controlled Unclassified Information (CUI) and Classified National Security Information (CNSI) is safeguarded from unauthorized disclosure. Safeguarding includes a combination of physical, cyber, and other security measures.

(U) While performing COVID-19-related telework, DoD employees and contractors must make every reasonable effort to protect CUI information from unauthorized disclosure. In accordance with references (a), (c), and (d), CUI requires safeguarding measures identified in Part 2002.14 of Title 32, CFR and, as necessary, in the law, regulation, or government-wide policy with which it is associated.

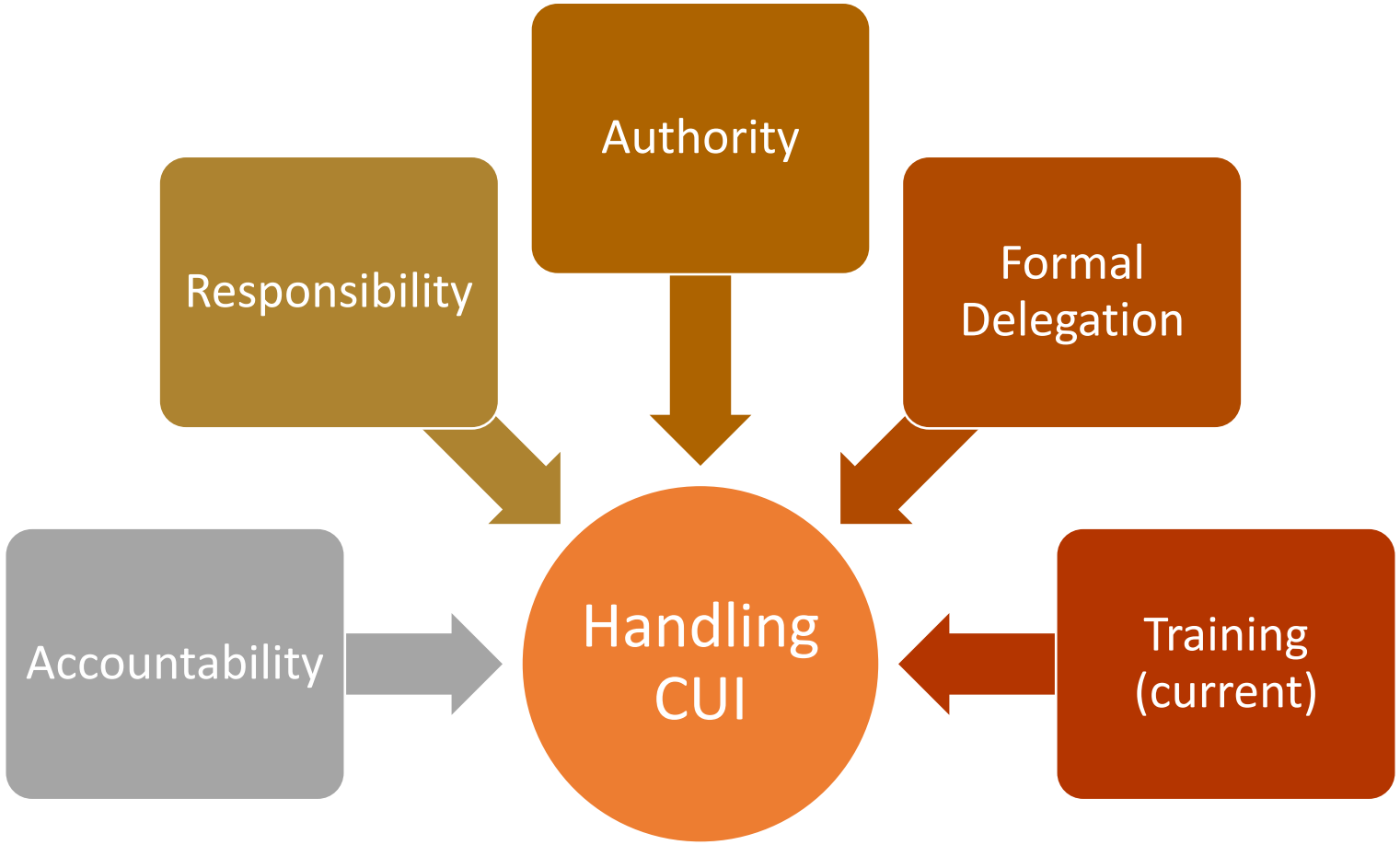
(CUI) No individual may have access to CUI information unless it is determined he or she has an authorized, lawful government purpose.

(CUI) CUI information may only be shared to conduct official DoD business and must be secured from unauthorized access or exposure.

(U) Unauthorized disclosures of CUI information may result in administrative, civil, or criminal penalties, depending on the category.

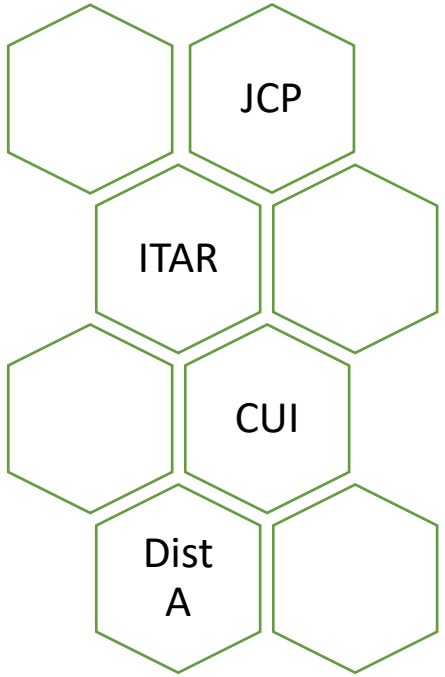
Controlled Unclassified Information Markings October 23, 2020

Handling CUI



Sharing of Information

1. Identify the type(s)
2. Review requirements
    1. Eligibility
    2. Process
    3. Flow-down requirements
    4. Other
3. Determine eligibility
4. Coordinate/specify
5. Execute – Supply Chain Support Agreement (idea – non-specific)



3.6. GENERAL DOD CUI PROCEDURES.

- DoD CUI is clustered into organizational indexes (e.g., defense, privacy, proprietary) with associated categories, and is categorized by the DoD according to the specific law, regulation, or government-wide policy requiring control. Unclassified information associated with a law, regulation, or government-wide policy and identified as needing safeguarding is considered CUI. It requires access control, handling, marking, dissemination controls, and other protective measures for safeguarding.

  a. The authorized holder of a document or material is responsible for determining, at the time of creation, whether information in a document or material falls into a CUI category. If so, the authorized holder is responsible for applying CUI markings and dissemination instructions accordingly.

DoDI 5200.48, March 6, 2020

Awareness of existing and internal CUI

- For example –
  - Cyber Summary Scores
  - Non-public SAM information
  - Export Controlled
  - Procurement & Acquisition – Source Selection
  - Proprietary Business Information

Defense	Controlled Technical Information (CTI) DoD Critical Infrastructure Security Information Naval Nuclear Propulsion Information Unclassified Controlled Nuclear Information - Defense (USNI)
Export Control	Export Controlled Export Controlled Research
Procurement and Acquisition	General Procurement and Acquisition Small Business Research and Technology Source Selection
Proprietary Business Information	Entity Registration Information General Proprietary Business Information Ocean Common Carrier/Marine Terminal Operator Agreements Ocean Common Carrier Service Contracts Proprietary Manufacturer Proprietary Postal

https://www.dodcui.mil/Home/DoD-CUI-Registry/

CMMC doesn't directly require but

- The recipient will need,
  - Sound knowledge of
    - Each program
    - Types of information
    - Handling restrictions
    - Other requirements***
  - A methodology to review and identify all relevant information types
  - To determine which if any of the information needs to be shared

Paragraph (l) 252.204-7012 - Other safeguarding or reporting requirements. The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

Internal management

- JCP requires 1 – Data Custodian
- ITAR penalty can be substantial
- Internal sharing practices/expectations
- Informal – work on this
- Formal –
  - Training
  - Appointment
  - Tools to use
  - Assessment
  - Other

Letter of Delegation – as an example

Company Letterhead

Date: March 5, 2021

References: (a) ……. ( )

Subject: Appointment as CUI handler for <this company>

1. As a DoD contractor, the company will receive and handle Controlled Unclassified Information(CUI). During the course of your work assignments you will have exposure to and responsibilities for correctly handling this information.

2. It is imperative that this information be handled in accordance with applicable regulations cited as references to this letter of appointment.

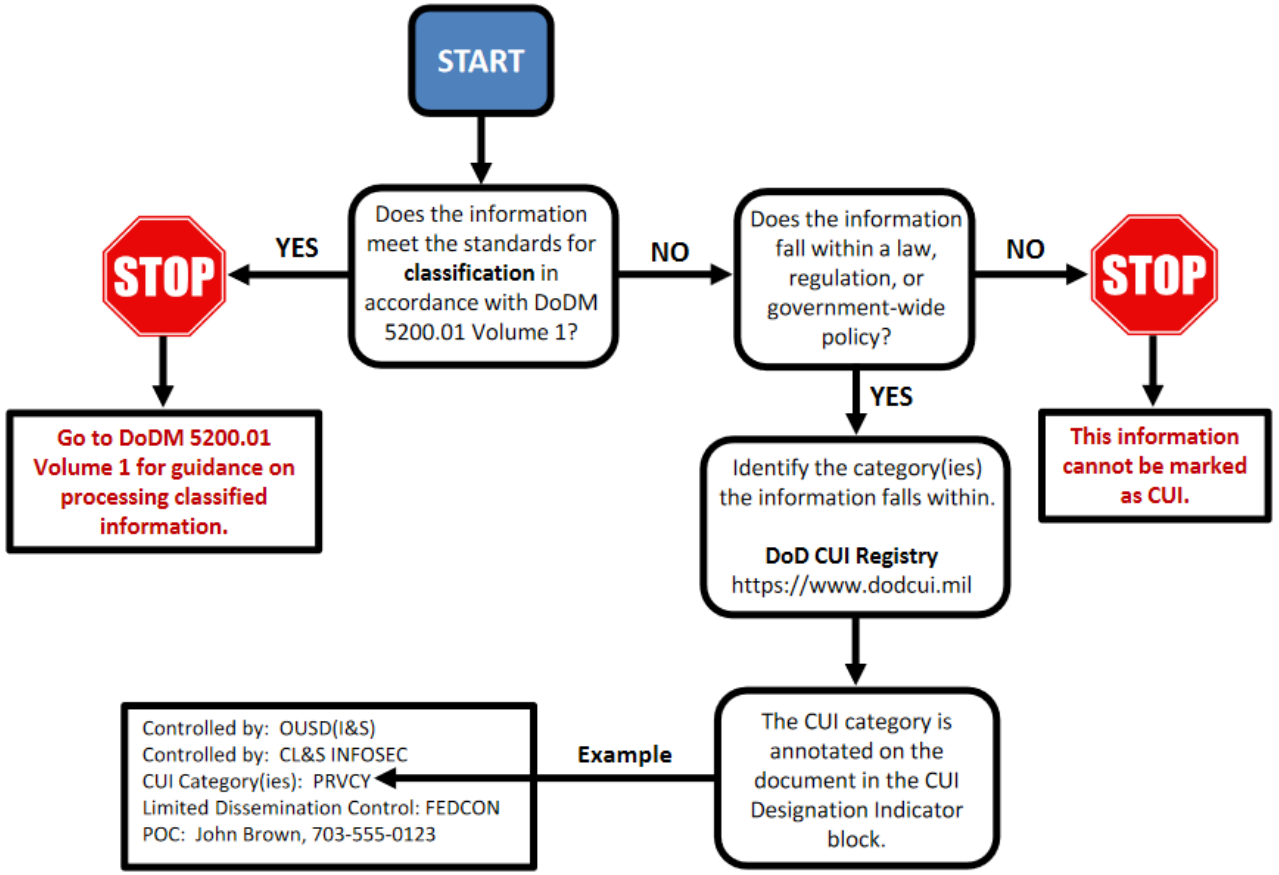
3. Of critical importance is the proper storage of and sharing of this information. Refer to company policies with respect to both of these issues. When in doubt, ask questions prior to taking action.

3. In addition to company provided training, you are expected to maintain familiarity with these requirements.

Signed: Employee

Signed: Company

Process for CUI Determination



https://www.dodcui.mil/Portals/109/Documents/Desktop Aid Docs/CUI Training Aids_Oct 23 2020.pdf, page 3

DISSEMINATION,DECONTROLLING, AND DESTRUCTION OF CUI

What to expect

4.1. GENERAL.

Part 2002 of Title 32, CFR requires dissemination statements to be placed on classified and unclassified documents or other materials when CUI necessitates access restrictions, including those required by law, regulation, or government-wide policy. These statements facilitate ★ control, secondary sharing, decontrol, and release without the need to repeatedly obtain approval or authorization from the controlling DoD office.

a. Dissemination controls identify the audience deemed to have a lawful government purpose to use the CUI and specify the rationale for applying the controls by specific codes in accordance with DoDI 5230.24 and this issuance.

https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/DoDI%205200.48%20CUI.pdf, page 27

Understand the process

PGI 204.7303-1 General.

(a) The contracting officer will be notified by the requiring activity when a solicitation is expected to result in a contract, task order, or delivery order that will involve—

(1) Covered defense information; or

(2) Operationally critical support.

(b) The contracting officer shall—

(1) Ensure that the requiring activity provides a work statement or specification that includes the identification of covered defense information or operationally critical support consistent with paragraph (a).

(2) Ensure that the solicitation and resultant contract, task order, or delivery order includes the requirement (such as a contract data requirements list), as provided by the requiring activity, for the contractor to apply markings, when appropriate, on covered defense information.

Parent topic: PGI 204.7303 Procedures.

Protecting CUI

- (1) During working hours, steps will be taken to minimize the risk of access by unauthorized personnel, such as not reading, discussing, or leaving CUI information unattended where unauthorized personnel are present. After working hours, CUI information will be stored in unlocked containers, desks, or cabinets if the government or government-contract building provides security for continuous monitoring of access. If building security is not provided, the information will be stored in locked desks, file cabinets, bookcases, locked rooms, or similarly secured areas. The concept of a controlled environment means there is sufficient internal security measures in place to prevent or detect unauthorized access to CUI. For DoD, an open storage environment meets these requirements.

https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/DoDI%205200.48%20CUI.pdf, page 27

Transmitting CUI

- (2) CUI information and material may be transmitted via first class mail, parcel post, or, bulk shipments. When practical, CUI information may be transmitted electronically (e.g., data, website, or e-mail), via approved secure communications systems or systems utilizing other protective measures such as Public Key Infrastructure or transport layer security (e.g., https). Avoid wireless telephone transmission of CUI when other options are available. CUI transmission via facsimile machine is permitted; however, the sender is responsible for determining whether appropriate protection will be available at the receiving location before transmission (e.g., facsimile machine attended by a person authorized to receive CUI; facsimile machine located in a controlled government environment).

https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/DoDI%205200.48%20CUI.pdf, page 27

DISSEMINATION REQUIREMENTS FOR DOD CUI

a. In accordance with this issuance, CUI access should be encouraged and permitted to the extent the access or dissemination:

(1) Complies with the law, regulation, or government-wide policy identifying the information as CUI.

(2) Furthers a lawful government purpose.

(3) Is not restricted by an authorized LDC established by the CUI EA.

(4) Is not otherwise prohibited by any other law, regulation, or government-wide policy.

https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/DoDI%205200.48%20CUI.pdf, page 28

Table 2. Dissemination Control and Distribution Statement Markings

LDC – Limited Dissemination Controls

LDCs or distribution statements cannot unnecessarily restrict CUI access.

NEW LDC	ALIGNMENT TO CURRENT
NONE – Publicly Releasable **AFTER** Review	DISTRO A
No Foreign Dissemination (NOFORN / NF)	
Federal Employees Only (FED ONLY)	DISTRO B
Federal Employees and Contractors Only (FEDCON)	DISTRO C
No Dissemination to Contractors (NOCON)	
Dissemination List Controlled (DL ONLY)	DISTRO F
Authorized for Release to Certain Foreign Nationals Only (REL TO USA, LIST)	
Display Only (DISPLAY ONLY)	
Dissemination List – (Include Separate List for Government Only)*	DISTRO E
Dissemination List – (Include Separate List for Government and Contractors Only)*	DISTRO D
NONE	DISTRO X: U.S. Government Agencies and private individuals or enterprises eligible to obtain export controlled technical data in accordance with DoDD 5230.25. DISTRO X was cancelled and superseded by DISTRO C.
*The dissemination list limits access to the specified individuals, groups, or agencies and must accompany the document	

https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/DoDI%205200.48%20CUI.pdf, page 29

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.

e. All CUI records must follow the approved mandatory disposition authorities whenever the DoD provides CUI to, or CUI is generated by, non-DoD entities in accordance with Section 1220-1236 of Title 36, CFR, Section 3301a of Title 44, U.S.C., and this issuance.

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

Aggregation of CUI (chicken and the egg)

- The aggregation of CUI may create classified information
- This is tough –
  - How does one know what is classified unless they are told?
- Classification is based upon various definitions and standards
- Determining whether something is classified is not an individual determination
- There is a reference that defines levels and information that qualify

National Security - Definitions

- National security information
  - **CONFIDENTIAL** – some damage to national security would occur
  - **SECRET** – serious damage to national security would occur
  - **TOP SECRET** – exceptionally grave damage to national security would occur as defined by the Department of Defense (DoD) 5220.22-M, National Industrial Security Program Operating Manual.
- Requirements
  - Clearance – equal to or higher than classification level – federal review
  - Access - Need to know – owner, holder of information

https://www.doncio.navy.mil/Chips/ArticleDetails.aspx?ID=3204

Example – Classification criteria - *Example*

- Made up – law enforcement

Level	General Criteria
U	Police Uniform
U	Badge number
U	Existence of specialized units (drug, gang, etc)
C	Color of the day are used
S	Color of the day
S	Roster of under-cover officers
TS	Assignments of under-cover officers
TS++	Algorithm for determining future Color of the day

Develop a Rubric (academic def)

- Number of CUI awards with TDP
- Number of CUI awards with TDP to a single platform/weapons system
- Nature of the information
  - General – may be in public view
  - Intricate
  - Specialized
  - Requires unique material, use of specified subcontractor, other
- <u>At some point (?) may require asking – taking action</u>
- Underscores the importance for proper safeguarding of CUI

Put simply, it is a set of criteria for grading assignments. Rubrics usually contain evaluative criteria, quality definitions for those criteria at particular levels of achievement, and a scoring strategy.[1] (Wikipedia) 1. Popham, James Oct 1997

Export Controlled Technical Information

c. CUI export controlled technical information or other scientific, technical, and engineering information will still use distribution statements. Export controlled information must also be marked with an export control warning as directed in DoDI 5230.24, DoDD 5230.25, and Part 250 of Title 32, CFR.

https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/DoDI%205200.48%20CUI.pdf, page 29

Stay current

Joint NSA and CISA Guidance on Strengthening Cyber Defense Through Protective DNS

03/04/2021 01:50 PM EST

Original release date: March 4, 2021

The National Security Agency (NSA) and CISA have released a Joint Cybersecurity Information (CSI) sheet with guidance on selecting a protective Domain Name System (PDNS) service as a key defense against malicious cyber activity. Protective DNS can greatly reduce the effectiveness of ransomware, phishing, botnet, and malware campaigns by blocking known-malicious domains. Additionally organizations can use DNS query logs for incident response and threat hunting activities.

CISA encourages users and administrators to consider the benefits of using a protective DNS service and review NSA and CISA's CSI sheet on Selecting a Protective DNS Service for more information.

Take advice from the Pro's

National Security Agency | Cybersecurity & Infrastructure Security Agency

Cybersecurity Information

Selecting a Protective DNS Service

Why Protective DNS?

The Domain Name System (DNS) is central to the operation of modern networks, translating human-readable domain names into machine-usable Internet Protocol (IP) addresses. DNS makes navigating to a website, sending an email, or making a secure shell connection easier, and is a key component of the Internet's resilience. As with many Internet protocols, DNS was not built to withstand abuse from bad actors intent on causing harm. "Protective DNS" (PDNS) is different from earlier security-related changes to DNS in that it is envisioned as a security service – *not a protocol* – that analyzes DNS queries and takes action to mitigate threats, leveraging the existing DNS protocol and architecture.

Works Cited

[1] Cybersecurity and Infrastructure Security Agency (2020), Addressing Domain Name System Resolution on Federal Networks. Available at: https://www.cisa.gov/sites/default/files/publications/Addressing_DNS_Resolution_on_Federal_Networks_Memo.pdf

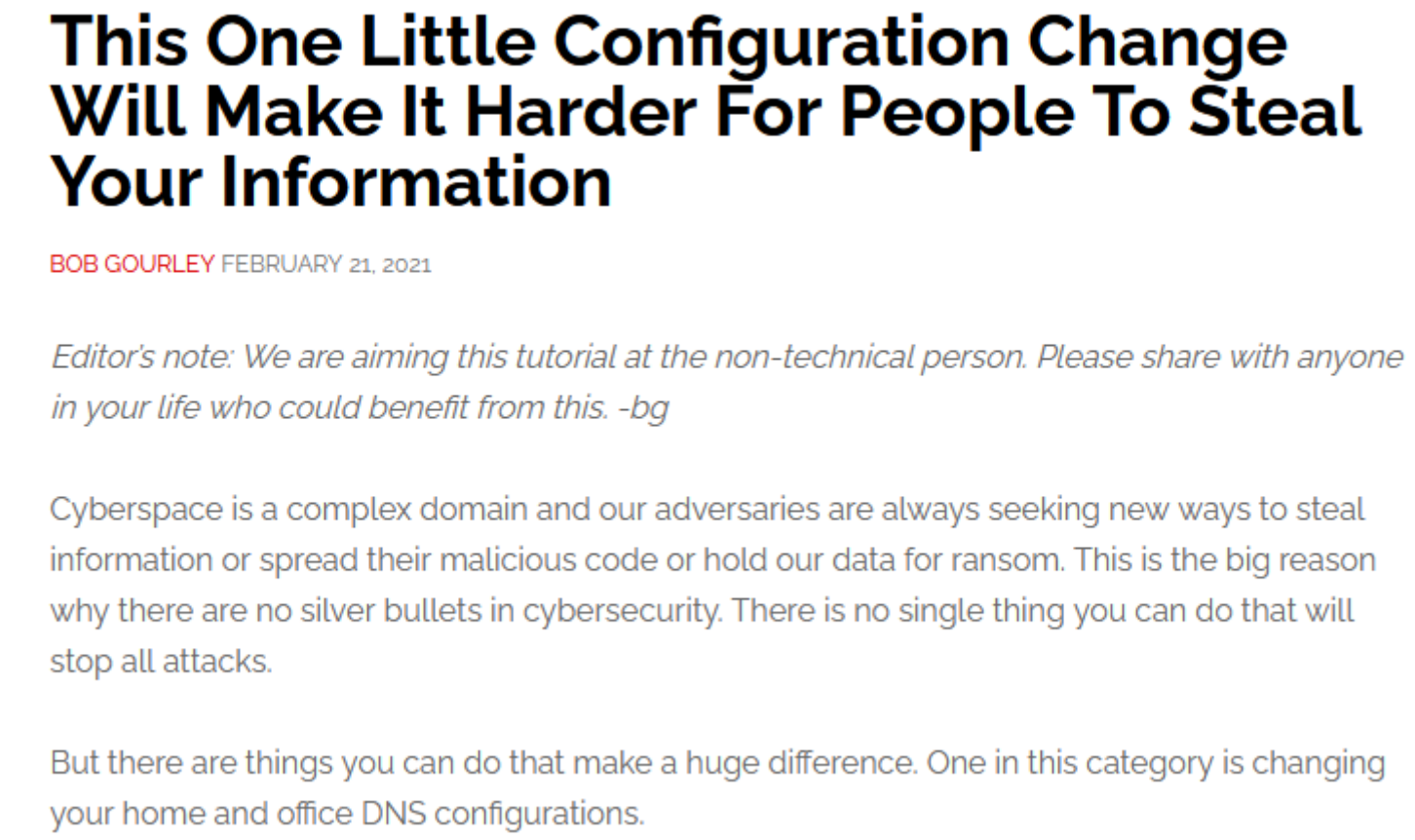
[2] Cybersecurity and Infrastructure Security Agency, (2019) Emergency Directive 19-01: Mitigate DNS Infrastructure Tampering. Available at: https://cyber.dhs.gov/ed/19-01/

[3] Office of the Undersecretary of Defense for Acquisition & Sustainment (2020), Cybersecurity Maturity Model Certification. Available at: https://www.acq.osd.mil/cmmc/draft.html

[4] UK National Cyber Security Centre (2017), Protective DNS (PDNS). Available at: https://www.ncsc.gov.uk/information/pdns

[5] National Security Agency (2020), Adopting Encrypted DNS in Enterprise Environments. Available at: https://www.nsa.gov/cybersecurity-guidance

Use a variety of resources



This One Little Configuration Change Will Make It Harder For People To Steal Your Information

BOB GOURLEY FEBRUARY 21, 2021

Editor's note: We are aiming this tutorial at the non-technical person. Please share with anyone in your life who could benefit from this. -bg

Cyberspace is a complex domain and our adversaries are always seeking new ways to steal information or spread their malicious code or hold our data for ransom. This is the big reason why there are no silver bullets in cybersecurity. There is no single thing you can do that will stop all attacks.

But there are things you can do that make a huge difference. One in this category is changing your home and office DNS configurations.

https://ctovision.com/this-one-little-configuration-change-will-make-it-harder-for-people-to-steal-your-information/

Managed DNS & DFARS 252.204-7012

Consider for example, the example of the old fashioned phone operator. What if you were receiving a call from someone you do not know, and before connecting the operator gets on the line with you and says "Based on our historical records, the person calling you has a record of conducting fraud and they are probably going to try to deceive you." That would have been a nice feature back in the day.

If you configure your DNS properly, you can put features like that, and far more, at your command. Depending on which DNS features you want and which provider you select, you can use a managed DNS service to speed up your web browsing. You can also use it to make customized filtering decisions for your home system (for example, you can tell it that no one should have access to certain types of sites). You can also use managed DNS to prevent viruses and other types of malicious code from communicating with their bosses (their control servers), which can help reduce the chance that your information will be stolen from malicious code.

https://ctovision.com/this-one-little-configuration-change-will-make-it-harder-for-people-to-steal-your-information/

Details – can matter

204.7304 Solicitation provision and contract clauses.

(a) Use the provision at 252.204-7008 , Compliance with Safeguarding Covered Defense Information Controls, in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items.

(b) Use the clause at 252.204-7009 , Limitations on the Use or Disclosure of Third- Party Contractor Reported Cyber Incident Information, in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting.

(c) Use the clause at 252.204-7012 , Safeguarding Covered Defense Information and Cyber Incident Reporting, in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts solely for the acquisition of COTS items.

(d) Use the provision at 252.204-7019 , Notice of NIST SP 800-171 DoD Assessment Requirements, in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items.

(e) Use the clause at 252.204-7020 , NIST SP 800-171 DoD Assessment Requirements, in all solicitations and contracts, task orders, or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for those that are solely for the acquisition of COTS items.

Provision v. Clause

- *Contract clause* or "clause" means a term or condition used in contracts or in both solicitations and contracts, and applying after contract award or both before and after award.
- *Solicitation provision or provision* means a term or condition used only in solicitations and applying only before contract award.

CMMC in the Field

- Would not expect the government to be a “life-line”
- They may but …
- Due to their position, their remarks, guidance, or other can be taken as – policy; typically policy is not set in an ad hoc manner

- Federal rep 1 – says Yes
- Federal rep 2 (inspector) – says No
- Company steps back; now it is Fed 1 v. Fed 2
- Therefore – a general answer will be – from a reg or along the lines Yes, if it permitted or they are eligible or something similar

Blending security with changes

- Employees
- Markets
- Upgrades
- Quality v. Cyber
  - Quality, in many cases – stable, subtle shifts, acceptable variance
  - Cyber – could be like – picking up and dropping a machine
    - Malware
    - Zero-day
    - Some other type of incident

Change management

- Checklist Development – purposeful decisions; not reactions
- Communicating
- Determining interrelationships
- Documentation
- Prioritization
- Process for determining when changes are required
- Regulations
- Threat awareness
- Training
- Testing

Testing the system

- Continuous Improvement
  - Staff
  - System
  - Support
  - Third-parties

Supply Chain

- Understanding
- Vetting
- Testing
- Certifying
- Developing & executing - Subcontractor/supplier agreements
  - CUI, JCP, ITAR, other as applicable
- Transparency
- Routine communications

Preparing for renewal

- Monitor/evaluate current policies/procedures
- Monitor changes to CMMC
- Monitor changes to regulations and other programs
  - 52.204-26 | 52.204-25 | 52.204 – 24 – telcom/devices
- Continue training
- Refine decision matrix

UPCOMING TRAINING - EVENTS

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

CYBER FRIDAY LIVE WEBINAR SERIES

Mar 5, 2021	CMMC Level 3 - Completing the steps needed to protect Controlled Unclassified Information.
Mar 19, 2021	Managing Vendor Risk
April 16, 2021	Your Cyber Plan Cannot Be Static – Here's Why!
April 30, 2021	Testing and Strengthening Your Cyber-Defenses Using Exercises
May 14, 2021	Corporate Acquisition, Insider threats, or Strategic Investments – All Threats to Consider

Register at: https://www.wispro.org/faqs/what-is-wpis-current-cyber-friday-webinar-schedule/

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

- March 10, 2021

  Acquisition Hour: Using Data to Develop You Federal Business Strategic Plan
  CLICK HERE for additional information
  Presented by Marc Violante, Wisconsin Procurement Institute

- March 16, 2021

  Acquisition Hour: The HUBZone Program – Certification Benefits and Regulations
  CLICK HERE for additional information
  Presented by Shane Mahaffy, U.S. Small Business Administration

- March 17, 2021

  Acquisition Hour: Responding to Sources Sought Request and Capabilities Statements
  CLICK HERE for additional information
  Presented by Helen Henningsen and Mark Dennis, Wisconsin Procurement Institute

- March 23, 2021

  The SBA 8(a) Certification Program and Small Disadvantaged Businesses (SDB)
  CLICK HERE for additional information
  Presented by Shane Mahaffy, U.S. Small Business Administration

- March 24, 2021

  Acquisition Hour: Using the New FPDS and Desktop Tools to Analyze Federal Procurement Data
  CLICK HERE for additional information
  Presented by Marc Violante, Wisconsin Procurement Institute

- April 6, 2021

  Acquisition Hour: Intellectual Property for Government Contractors & Subcontractors & the STTR/SBIR Stakeholder
  CLICK HERE for additional information
  Presented by Laura Grebe, Husch Blackwell

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

…More at wispro.org/events

8th Annual FAR Evening Study Sessions

Presented by the National Contract Management Association (NCMA Wisconsin) and WPI

February 2, 2021	Intro & FAR Part 16	**March 2, 2021**	FAR Parts 19-29
February 9, 2021	FAR Parts 1-4	**March 9, 2021**	FAR Parts 30-33
February 16, 2021	FAR Parts 5-12	**March 16, 2021**	FAR Parts 34-41
February 23, 2021	FAR Parts 13-18	**March 23, 2021**	FAR Parts 42-53

Register at: https://www.wispro.org/wpis-2021-far-evening-study-sessions-schedule/

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

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

2021 FAR Up Close Series

February 10, 2021	Overview of the FAR
February 17, 2021	FAR Regulations and Clauses on Subcontracting
March 3, 2021	FAR Regulations and Clauses in Commercial Items
March 10, 2021	FAR and DFARS Regulations and Clauses in Manufacturing Contracts
March 17, 2021	FAR Regulations and Clauses in Federal Service Contracts
April 7, 2021	FAR Clauses in Federal Construction Services
April 14, 2021	FAR Regulations for Procurement of Architect Engineer Services

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
FAR Up Close

Register at: https://www.wispro.org/wpis-2021-far-up-close-schedule/

3/5/21

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