Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

Cyber Friday

THE OTHER SIDE OF CMMC

January 8, 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/GoToWebinar**
- **SMALL GROUP TRAINING – Workshops and webinars**
- **CONFERENCES to include one on one or roundtable sessions**

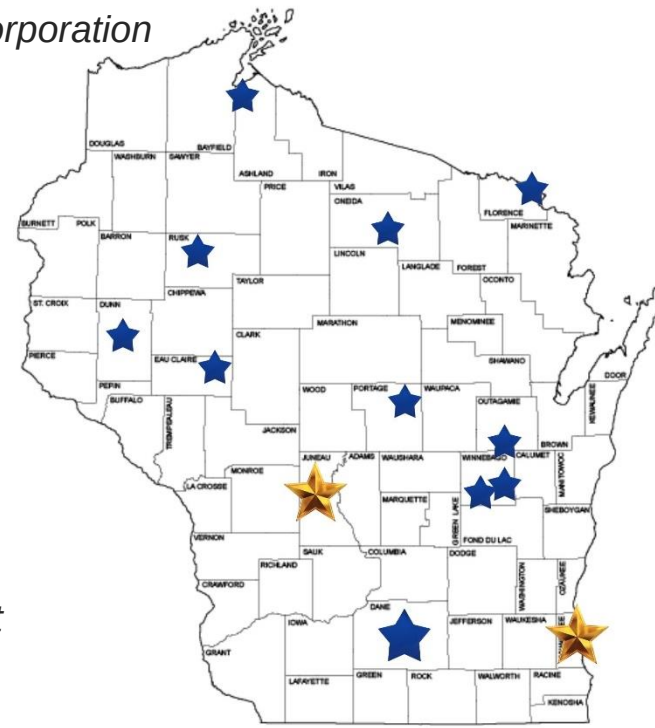
Last year WPI provided training at over 100 events and provided service to over 1,200 companies

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*
- **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*



Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

Cyber Friday

1/8/21

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

The other side of CMMC

Marc N. Violante

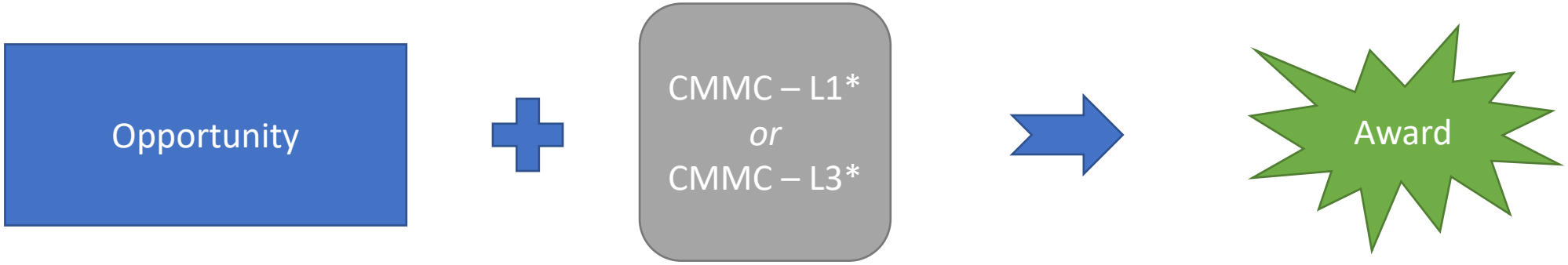
Wisconsin Procurement Institute

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

Current Status

- DFARS 252.204-7019 and 252.204-7020 > Basic Assessments + Medium/High as required
- DFARS 252.204-7021 active
- Interim rule input, being reviewed, outcome – any changes - unknown
- DoD is implementing a phased rollout of CMMC. Until September 30, 2025, the clause at 252.204–7021, Cybersecurity Maturity Model Certification Requirements, is prescribed for use in solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, excluding acquisitions exclusively for COTS items, if the requirement document or statement of work requires a contractor to have a specific CMMC level. In order to implement the phased rollout of CMMC, inclusion of a CMMC requirement in a solicitation during this time period must be approved by the Office of the Under Secretary of Defense for Acquisition and Sustainment. FR Sep 29, 2020, page 61506
- Pilot solicitations – nominations being reviewed
  - https://www.defense.gov/Newsroom/Releases/Release/Article/2447770/cybersecurity-maturity-model-certification-pilots-for-fiscal-year-2021/
- Dealing with the black & white of regulations and no feedback for context or better understanding

The Fundamental Equation



*As required

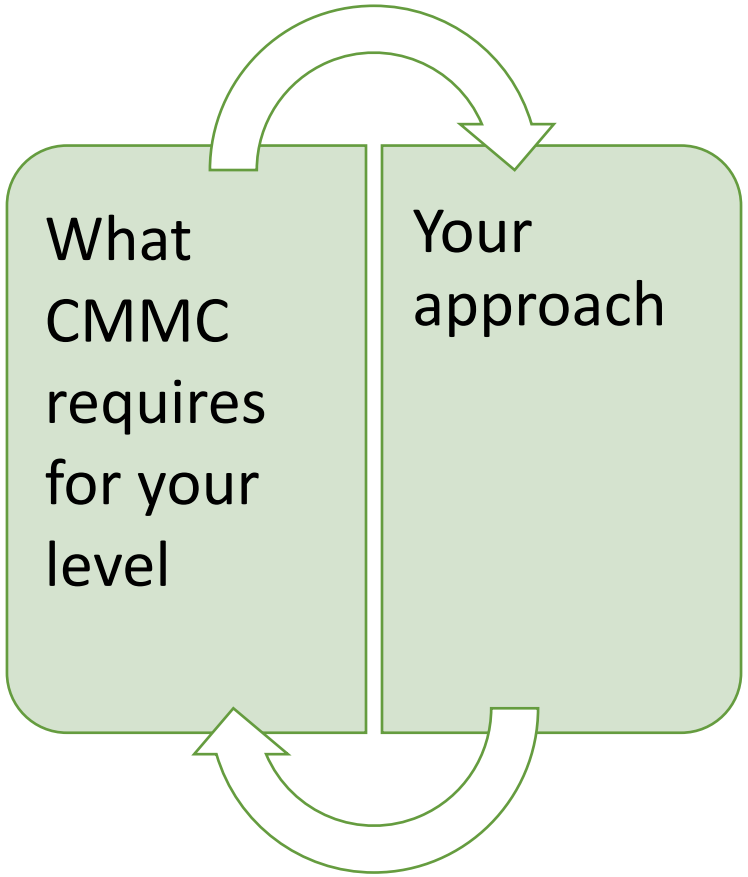
General Process

- Select/Determine CMMC level
- Go / No-go
- Download requirements & references
- Review
- Utilize SSP and POA
- Determine if date used for Basic Assessment (110) is accurate
- Update date if necessary
- Draft Work Breakdown Structure, assign POC – date – cost
- Assign POC/Responsibilities
- Establish milestone dates
- Determine reports and reporting periodicity – updates
- Identify slippage and reasons

To echo an often used phrase

CMMC – is not a checklist!

Top two issues -



Determine what level of effort will be required

There does not appear to be an easy or quick path to CMMC; any level. Undoubtedly, getting prepared will take time, resources and tremendous support from the top. Unfortunately, just amassing the tools is a small step in the process. Each company seeking certification will need to create a project plan, a timeline, assign responsibilities and then track progress and identify obstacles. The real questions are what is needed and how to get to this point?

CMMC is not equivalent to Basic Assessment

- Establish baseline – Basic Assessment, a starting point
- Assemble references
- Identify applicable portions
- Review terminology – define as needed
- Identify team – internal | external
- Develop standardization process – materials, policies, procedures, etc.
- Determine how to document, what records, retention, access, responsibility
- Refine process

Determine what should be included

When implementing CMMC, a DIB contractor can achieve a specific CMMC level for its entire enterprise network or for particular segment(s) or enclave(s), depending upon where the information to be protected is handled and stored.

https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf; page 2

Contractor Size

The CMMC assessment methodology follows a data-centric security process that applies the practices and processes equally, regardless of the contractor's size, constraints, or complexity. All CMMC levels are achievable by small, medium, and large contractors.

Size is not a factor!

https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl3_20201208_editable.pdf; page 3

Start with the end in mind

- The primary deliverable of an assessment is a report that contains the findings associated with each practice and process.
- For more detailed information on assessment methods, see Appendix D of NIST SP 800-171A - Assessing Security Requirements for Controlled Unclassified Information

https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl3_20201208_editable.pdf; page 5

What are the three assessment methods?

- Examine
  - The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time.
- Interview
  - The process of conducting discussions with individuals or groups of individuals in an organization to facilitate understanding, achieve clarification, or lead to the location of evidence. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time.
- Test
  - The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time.13 Objects

ASSESSING SECURITY REQUIREMENTS FOR CONTROLLED UNCLASSIFIED INFORMATION – NIST SP 800-171A; Table D-1

Examine Assessment Method

TABLE D-1: EXAMINE ASSESSMENT METHOD

Method	**EXAMINE** The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time.		
Objects	***Specifications***	Examples: policies, plans, procedures, system requirements, designs.	
	Mechanisms	Examples: functionality implemented in hardware, software, firmware.	
	Activities	Examples: system operations, administration, management, exercises.	
Attributes	***Depth***	Addresses the rigor of and level of detail in the *examination* process.	
		Basic	Examination that consists of high-level reviews, checks, observations, or inspections of the assessment object. This type of examination is conducted using a limited body of evidence or documentation. Examples include: functional-level descriptions for mechanisms; high-level process descriptions for activities; and documents for specifications. Basic examinations provide a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors.
		Focused	Examination that consists of high-level reviews, checks, observations, or inspections **and more in-depth studies and analyses** of the assessment object. This type of examination is conducted using a **substantial** body of evidence or documentation. Examples include: functional-level descriptions **and where appropriate and available, high-level design information** for mechanisms; high-level process descriptions **and implementation procedures** for activities; and documents **and related documents** for specifications. **Focused** examinations provide a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors **and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended**.
		Comprehensive	Examination that consists of high-level reviews, checks, observations, or inspections and more in-depth, **detailed, and thorough** studies and analyses of the assessment object. This type of examination is conducted using an **extensive** body of evidence or documentation. Examples include: functional-level descriptions and where appropriate and available, high-level design information, **low-level design information, and implementation information** for mechanisms; high-level process descriptions and **detailed** implementation procedures for activities; and documents and related documents for specifications.[10] **Comprehensive** examinations provide a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors and whether there are **further** increased grounds for confidence that the safeguards are implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the safeguards**.

ASSESSING SECURITY REQUIREMENTS FOR CONTROLLED UNCLASSIFIED INFORMATION – NIST SP 800-171A; Table D-1

Interview - Discussion

- Typical assessor actions may include, for example, interviewing chief executive officers, chief information officers, senior information security officers, information owners, system and mission owners, system security officers, system security managers, personnel officers, human resource managers, network and system administrators, facilities managers, training officers, physical security officers, system operators, site managers and users.

Understand what is required

"Furthermore, an organization must demonstrate both the requisite institutionalization of processes (i.e., the left side in Figure 2) and the implementation of practices (i.e., the right side in Figure 2) for a specific CMMC level and the preceding lower levels in order to achieve that level. For the case where an organization demonstrates different achievements with respect to process institutionalization and practice implementation, the organization will be certified at the lower of the two levels. "

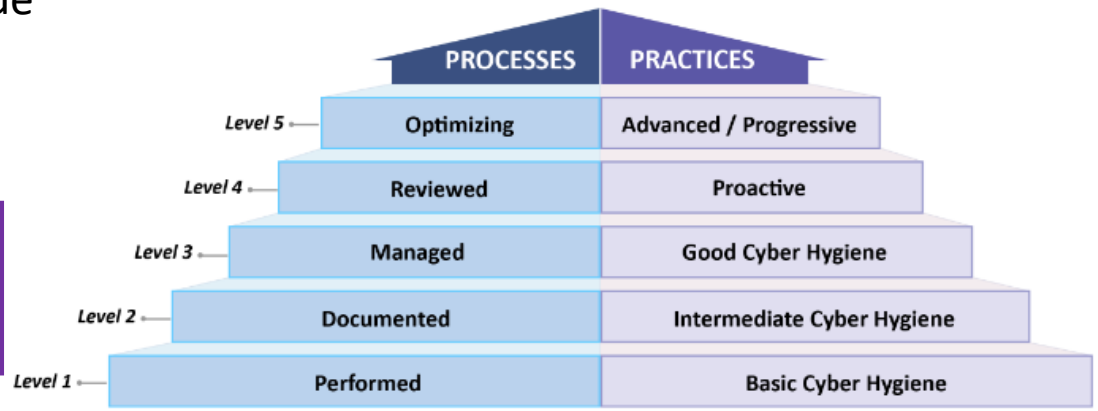


Figure 2. CMMC Levels and Descriptions

Goal	Processes	Practices	Certification
Level 1	Level 1	Fail	Fail
Level 3	Level 3	Level 1	Level 1

CMMC Model Framework

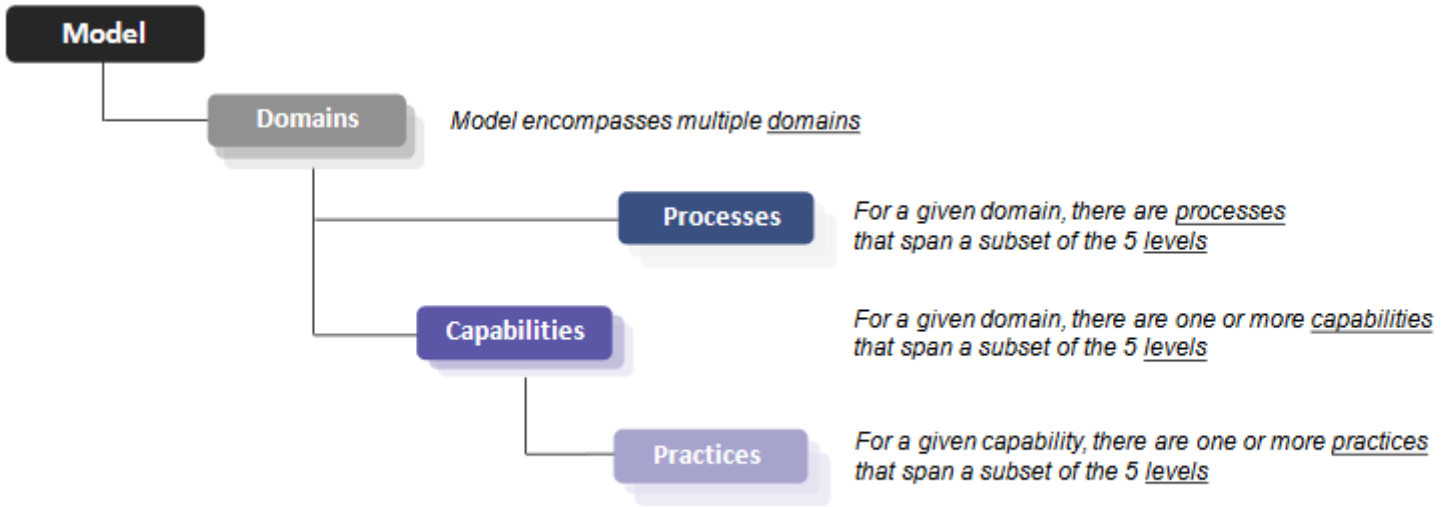


Figure 1. CMMC Model Framework (Simplified Hierarchical View)

https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf; page 3

CMMC Domains

https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf; page 7

CMMC Practices

ACCESS CONTROL (AC)

Level 1

AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
AC.1.003	Verify and control/limit connections to and use of external information systems.
AC.1.004	Control information posted or processed on publicly accessible information systems.

https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf; page 12

CMMC Processes

Maturity Level	Maturity Level Description	Processes
ML 1	**Performed**	*There are no maturity processes assessed at Maturity Level 1.* *An organization performs Level 1 practices but does not have process institutionalization requirements.*
ML 2	**Documented**	Establish a policy that includes [DOMAIN NAME].
		Document the CMMC practices to implement the [DOMAIN NAME] policy.
ML 3	**Managed**	Establish, maintain, and resource a plan that includes [DOMAIN NAME].
ML 4	**Reviewed**	Review and measure [DOMAIN NAME] activities for effectiveness.
ML 5	**Optimizing**	Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organization units.

https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf; page 9

Context can help with understanding – why?

Disgruntled former VP hacks company, disrupts PPE supply, earns jail term

The sabotage of electronic records led to delays in shipping critical PPE during the COVID-19 pandemic.

- Christopher Dobbins once worked for Stradis Healthcare, a medical equipment packaging company that facilitates the delivery of PPE, supplies, and surgical kits. After being fired in March 2020, with final paycheck in hand, the 41-year-old accessed a secret, fake staff account he had created while still in Stradis' employ.
- The ex-employee, described as "disgruntled" by the Federal Bureau of Investigation (FBI), was then able to maintain secret access to the company's systems, despite his legitimate account being revoked.
- Dobbins set about disrupting Stradis' electronic records by creating a secondary user account and both editing over 115,000 records and deleting over 2,300 entries.

https://www.zdnet.com/article/disgruntled-former-vp-hacks-company-disrupts-ppe-supply-earns-jail-term

Passwords

IDENTIFICATION AND AUTHENTICATION (IA)

CAPABILITY	Level 1 (L1)	Level 2 (L2)
C015 Grant access to authenticated entities	IA.1.076 Identify information system users, processes acting on behalf of users, or devices. • FAR Clause 52.204-21 b.1.v • NIST SP 800-171 Rev 1 3.5.1 • CIS Controls v7.1 4.2, 4.3, 16.8, 16.9 • NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7 • CERT RMM v1.2 ID:SG1.SP1 • NIST SP 800-53 Rev 4 IA-2, IA-3, IA-5	IA.2.078 Enforce a minimum password complexity and change of characters when new passwords are created. • NIST SP 800-171 Rev 1 3.5.7 • CIS Controls v7.1 4.2, 4.4 • NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7 • NIST SP 800-53 Rev 4 IA-5(1) • UK NCSC Cyber Essentials
	IA.1.077 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. • FAR Clause 52.204-21 b.1.vi • NIST SP 800-171 Rev 1 3.5.2 • CIS Controls v7.1 4.2, 4.3, 16.8, 16.9 • NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7	IA.2.079 Prohibit password reuse for a specified number of generations. • NIST SP 800-171 Rev 1 3.5.8 • CIS Controls v7.1 4.2, 4.4 • NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7 • NIST SP 800-53 Rev 4 IA-5(1)

https://www.acq.osd.mil/cmmc/docs/CMMC_Appendices_V1.02_20200318.pdf; page A-15

Wait – there is more

CISA: SolarWinds Hackers Got Into Networks by Guessing Passwords

DR_FLASH/SHUTTERSTOCK.COM

https://www.nextgov.com/cybersecurity/2021/01/cisa-solarwinds-hackers-got-networks-guessing-passwords/171265/

Starting Point

- System Security Plan – most recent
- Plan of Action – most recent
- Most current assessment
  - Basic
  - Medium
  - High
- Assessments might be Yes/No based; CMMC is not

CMMC Assessments

This section provides detailed information for assessing each CMMC practice beyond what is provided in the CMMC Model Overview document. The section is organized by domain and then practices. Each practice description contains the following elements:

- **Identifier and Practice Statement:** is headed by the practice identifier in the format Domain.Level.Number (e.g., AC.1.001) and followed by the CMMC practice statement.
- **Assessment Objectives [NIST SP 800-171A]:** identifies the specific list of objectives that must be met to receive MET for the practice as defined in NIST SP 800-171A.
- **Potential Assessment Methods and Objects [NIST SP 800-171A]:** defines the nature and the extent of the Certified Assessor's actions as defined in NIST SP 800-171A. The methods include *examine*, *interview*, and *test*. Assessment objects identify the items being assessed and can include specifications, mechanisms, activities, and individuals.
- **Discussion [NIST SP 800-171 R2]:** contains discussion written by NIST[2] for the associated NIST SP 800-171 security requirement. CMMC Level 1 aligns with FAR Clause 52.204-21, which focuses on FCI, and the NIST text has been modified to reflect this.
- **Further Discussion:**

https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl1_20201208_editable.pdf; page 7

Access Control – for example

Level 1 AC Practices

AC.1.001

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] authorized users are identified;

[b] processes acting on behalf of authorized users are identified;

[c] devices (and other systems) authorized to connect to the system are identified;

[d] system access is limited to authorized users;

[e] system access is limited to processes acting on behalf of authorized users; and

[f] system access is limited to authorized devices (including other systems).

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl1_20201208_editable.pdf; page 8

Common documents reviewed

- policy, process, and procedure documents;
- training materials;
- plans and planning documents; and
- system-level, network, and data flow diagrams.

This list of documents is not exhaustive or prescriptive. A contractor may not have these specific documents, and other documents may be used to provide evidence of compliance.

https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl1_20201208_editable.pdf; page 5

What is tested?

- Testing is an important part of the assessment process.
- Interviews tell the Certified Assessor what the contractor staff believe to be true, documentation provides evidence of intent, and testing demonstrates what has or has not been done.

For example, contractor staff may talk about how users are identified, documentation may provide details on how users are identified, but seeing a demonstration of identifying users provides evidence that the practice is met.

The Certified Assessor will determine which practices, or objectives within a practice need demonstration or testing. Not all practices will require testing

https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl1_20201208_editable.pdf; page 5

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?

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?

Assessment Criteria and Methodology

- The CMMC assessment procedure leverages the Assessment Procedure defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171A Section 2.11:

> *Assessment objects identify the specific items being assessed and can include specifications, mechanisms, activities, and individuals.*
>
> - *Specifications are the document-based artifacts (e.g., policies, procedures, security plans, security requirements, functional specifications, and architectural designs) associated with a system.*
> - *Mechanisms are the specific hardware, software, or firmware safeguards employed within a system.*
> - *Activities are the protection-related actions supporting a system that involve people (e.g., conducting system backup operations, exercising a contingency plan, and monitoring network traffic).*
> - *Individuals, or groups of individuals, are people applying the specifications, mechanisms, or activities described above.*

https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl1_20201208_editable.pdf; page 4

Fundamental to preparation

- Who is interviewed?
- What will be examined?
- What will be tested?

- Should the assessment be the first time that –
  - Interviews are conducted?
  - Processes, procedures and/or other documentation will be examined?
  - Reviews will be conducted to test an item of interest?

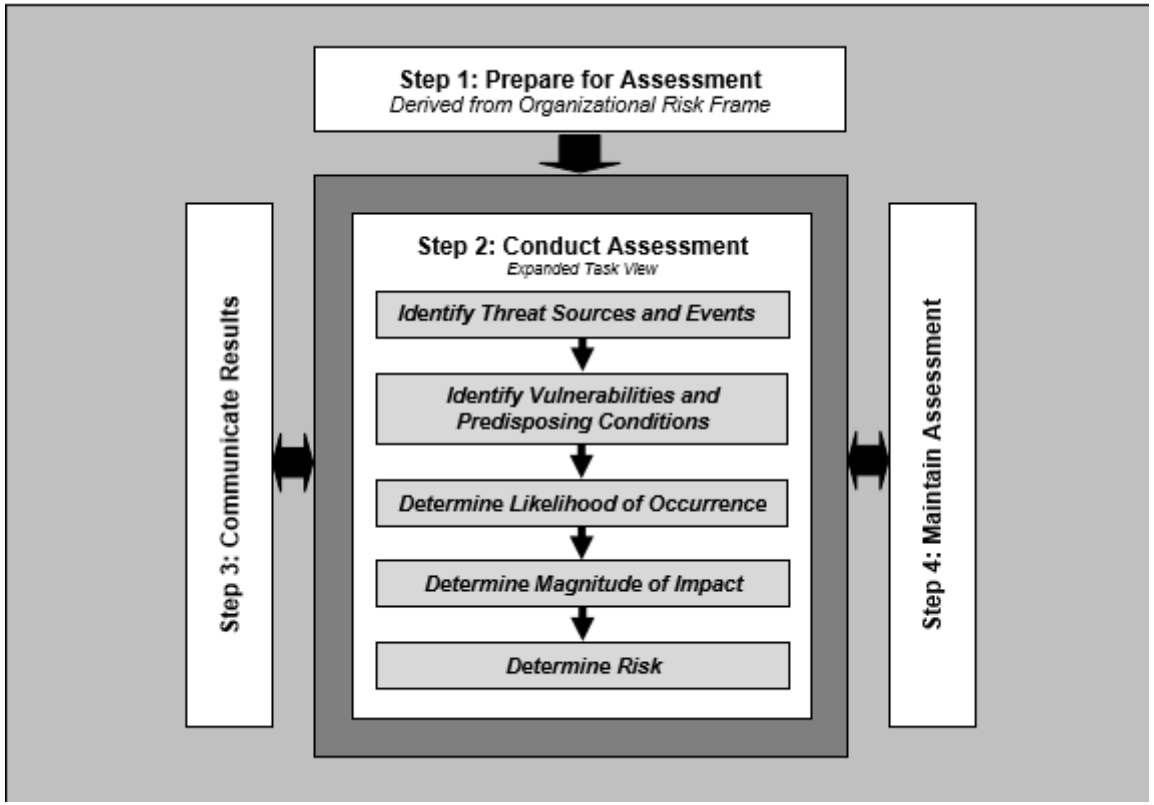
Generate your own questions - How do you know?

- - only authorized users have accessed the network?
- - information requiring destruction was destroyed appropriately?
- - email/ftp/other digital communications were handled correctly?
- - there is no malware on the network / computers / devices?
- - there have been no reportable incidents?
- - all other issues
- Walk through a policy/procedure.
- Ask – what happens if?
- Look for weaknesses – even low probability.

Consider alternatives – 360 look at threats

- Normal environment
- Stressed
- Need it now
- Over achiever
- Good performer – why not?
- Position related – automatic
- Close friendships – help me out.
- Insider issues

Risk Assessment Process



Guide for Conducting Risk Assessments; NIST 800-30, page 23

Identify & include staff members

- The term institutionalization characterizes the extent to which an activity is embedded or ingrained in the operations of an organization [9,10].

9. *Cybersecurity Capability Maturity Model (C2M2)*, Version 1.1, Department of Energy, Department of Homeland Security, and Carnegie Mellon University Software Engineering Institute, February 2017

10. *Advancing Cybersecurity Capability Measurement Using the CERT-RMM Maturity Indicator Level Scale*, Technical Note CMU/SEI-2013-TN-028, M. J. Butkovic and R. A. Caralli, Carnegie Mellon University Software Engineering Institute, November 2013

- The more deeply ingrained an activity, the more likely it is that an organization will continue to perform the activity – including under times of stress – and that the outcomes will be consistent, repeatable, and of high quality [9,10].
- Within the context of the CMMC model, process institutionalization provides additional assurances that the practices associated with each level are implemented effectively.

https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf; page 9

Institutionalization

- The term institutionalization characterizes the extent to which an activity is embedded or ingrained in the operations of an organization [9,10]. The more deeply ingrained an activity, the more likely it is that an organization will continue to perform the activity – including under times of stress – and that the outcomes will be consistent, repeatable, and of high quality [9,10].

9. *Cybersecurity Capability Maturity Model (C2M2)*, Version 1.1, Department of Energy, Department of Homeland Security, and Carnegie Mellon University Software Engineering Institute, February 2017

10. *Advancing Cybersecurity Capability Measurement Using the CERT-RMM Maturity Indicator Level Scale*, Technical Note CMU/SEI-2013-TN-028, M. J. Butkovic and R. A. Caralli, Carnegie Mellon University Software Engineering Institute, November 2013

https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf; page 9

Become familiar with the requirements

- NIST 800-171 r2
- FAR 52.204-21
- DFARS 252.204-7012
- DFARS 252.204-7021
- NIST 800-171A
- CMMC Model
- CMMC Assessment Guide – relevant CMMC Level

Understand the terminology

- During the CMMC assessment, the Certified Assessor will verify and validate that the contractor has properly implemented the practices and processes. Because a contractor can meet the assessment objectives in different ways (e.g., through documentation, computer configuration, network configuration, or training) the Certified Assessor may use a variety of techniques, including any of the three assessment methods described above from NIST SP 800-171A, to determine if the contractor meets the intent of the practices and processes.

https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl3_20201208_editable.pdf; page 5

Understand the terminology

- During the CMMC assessment, the Certified Assessor will verify and validate that the contractor has properly implemented the practices and processes. Because a contractor can meet the assessment objectives in different ways (e.g., through documentation, computer configuration, network configuration, or training) the Certified Assessor may use a variety of techniques, including any of the three assessment methods described above from NIST SP 800-171A, to determine if the contractor meets the intent of the practices and processes.

Assessment Criteria & Methodology

- The CMMC assessment procedure leverages the Assessment Procedure defined in NIST SP 800-171A Section 2.11:
  - An assessment procedure consists of an assessment objective and a set of potential assessment methods and assessment objects that can be used to conduct the assessment.
  - Each assessment objective includes a determination statement related to the [CMMC practice or process] that is the subject of the assessment. The determination statements are linked to the content of the [CMMC practice or process] to ensure traceability of the assessment results to the requirements.
  - The application of an assessment procedure to a [CMMC practice or process] produces assessment findings. These findings reflect, or are subsequently used, to help determine if the [CMMC practice or process] has been satisfied.

Criteria

- Assessment objectives are provided for each practice and process and are based on existing criteria (e.g., NIST SP 800-171A). The criteria are authoritative and provide a basis for a CMMC Certified Assessor to conduct an assessment of a practice or process.

Methodology

- During the CMMC assessment, the Certified Assessor will verify and validate that the contractor has properly implemented the practices and processes. Because a contractor can meet the assessment objectives in different ways (e.g., through documentation, computer configuration, network configuration, or training) the Certified Assessor may use a variety of techniques, including any of the three assessment methods described above from NIST SP 800-171A, to determine if the contractor meets the intent of the practices and processes.

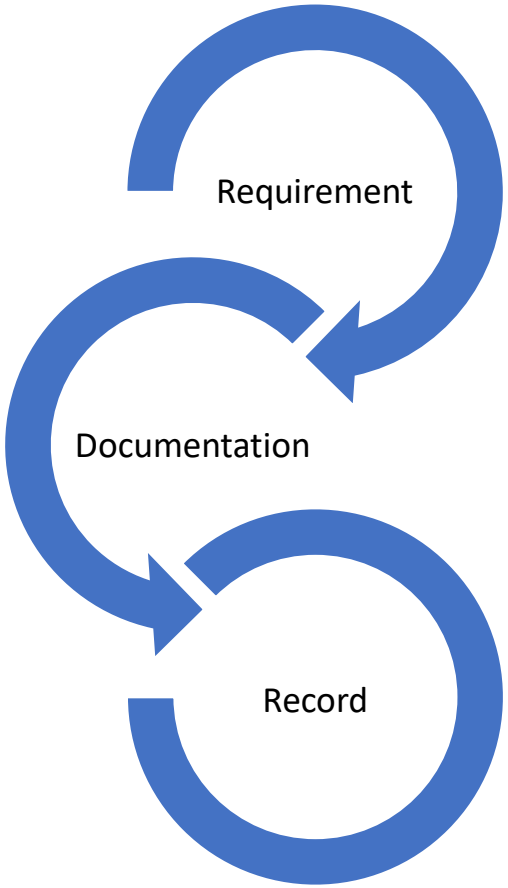
Verification v. Validation

- *Verification*
  - *is the process for determining whether or not a product fulfills the requirements or specifications established for it.*

- *Validation*
  - *is the assessment of a planned or delivered system to meet the sponsor's operational need in the most realistic environment achievable.*

https://www.mitre.org/publications/systems-engineering-guide/se-lifecycle-building-blocks/test-and-evaluation/verification-and-validation

What information/data is required?



Identify Necessary steps

- Management involvement
- Staff
- Commitment
- Funding
- Project Planning
- Resources
- Training

Visitors – do policies consider?

- Sales/marketing
- Temporary employees
- Visiting engineer
- Customer
- Prospective customers
- Contract Services – repair, janitorial, suppliers, OEM, other
- Friends/family
- Others

The contractor is accountable

- (c) *Cyber incident reporting requirement*.
- (1) When the Contractor discovers a cyber incident that affects a covered contractor information system or …
- (d) *Malicious software.* When the Contractor or subcontractors discover and isolate malicious software …
- (e) *Media preservation and protection*. When a Contractor discovers a cyber incident has occurred, the Contractor shall …

DFARS 252.204-7012

Be aware – due diligence

CMMC Center of Excellence Announces Engagement Agreement with SideChannel

Yahoo Finance

The **Cybersecurity Maturity Model** Certification Center of Excellence (CMMC COE), hosted by the Information Technology Acquisition Advisory ...

What does CMMC really mean for small businesses?

Read more Commentary news.

Les Buday is a Member of the CMMC Advisory Body and Director for Cybersecurity at HumanTouch, LLC in Tysons, Va.

Google Alerts | https://federalnewsnetwork.com/commentary/2021/01/what-does-cmmc-really-mean-for-small-businesses/

Assemble Applicable References

Include references for related programs

- DFARS 252.204-7021
- DFARS 252.204-7008
- DFARS 252.204-7012
- NIST 800-171 revision 2 – Feb 2021
- NIST 800-171A
- NIST Handbook 162
- FAR 52.204-21
- NISTIR 8286 -Integrating Cybersecurity and Enterprise Risk Management (ERM)
- CMMC Model
- CMMC Assessment – appropriate level
- 32 CFR 2002
- *Export Control program & references (EAR, ITAR, JCP, NOFORN)
- NIST Cybersecurity Framework
- Regulations
- MITRE ATT&CK

Be familiar with requirements

DEFENSE LOGISTICS AGENCY (DLA) MASTER SOLICITATION
FOR AUTOMATED SIMPLIFIED ACQUISITIONS
REVISION 74 (DEC 3 2020)

DFARS 252.204-7000 (Oct 2016) Disclosure of Information
DFARS 252.204-7003 (Apr 1992) Control of Government Personnel Work Product
DFARS 252.204-7007 (Dec 2019) Alternate A, Annual Representations and Certifications. ***(Includes DFARS 252.204-7016 (Dec 2019), Covered Defense Telecommunications Equipment Or Services – Representation)***
DFARS 252.204-7008 (Oct 2016) Compliance with Safeguarding Covered Defense Information Controls
DFARS 252.204-7009 (Oct 2016) Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information
DFARS 252.204-7012 (Dec 2019) Safeguarding Covered Defense Information and Cyber Incident Reporting
DFARS 252.204-7015 (May 2016) Notice of Authorized Disclosure of Information for Litigation Support
DFARS 252.204-7019 (Nov 2020) Notice Of NIST SP 800-171 DoD Assessment Requirements
DFARS 252.204-7020 (Nov 2020) NIST SP 800-171 DoD Assessment Requirements
DFARS 252.213-7000 (Sep 2019) Notice to Prospective Suppliers on Use of Supplier Performance Risk System in Past Performance Evaluations.
DFARS 252.222-7999 (Nov 2020) Combating Race And Sex Stereotyping (Deviation 2021-O0001)
https://www.acq.osd.mil/dpap/policy/policyvault/USA002235-20-DPC.pdf

C001- Establish system access requirements –a

- AC.1.001
  Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

  - FAR Clause 52.204-21 b.1.i
  - NIST SP 800-171 Rev 1 3.1.1
  - CIS Controls v7.1 1.4, 1.6, 5.1, 14.6, 15.10, 16.8, 16.9, 16.11
  - NIST CSF v1.1 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4
  - CERT RMM v1.2 TM:SG4.SP1
  - NIST SP 800-53 Rev 4 AC-2, AC-3, AC-17
  - AU ACSC Essential Eight

Third Party – coordination / considerations

- “Malicious software” means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.
- (d) *Malicious software.* When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.
- Develop processes/procedures to deal with the issue
- Determine if there was a reportable cyber incident
- Cyber forensic image
- Review update System Security Plan | Procedures | Policies

DFARS 252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2019)

SI.1.212 Update malicious code protection mechanisms when new releases are available

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] malicious code protection mechanisms are updated when new releases are available.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; system security plan; system design documentation; system configuration settings and associated documentation; scan results from malicious code protection mechanisms; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for malicious code protection; personnel with configuration management responsibility].

Test

Policy – at a minimum

- clearly state the purpose of the policy;
- clearly define the scope of the policy: for example, enterprise-wide, department-wide, or information-system specific;
- describe the roles and responsibilities of the activities covered by this policy: the responsibility, authority, and ownership of [DOMAIN NAME] domain activities; and
- establish or direct the establishment of procedures to carry out and meet the intent of the policy, include any regulatory guidelines this policy addresses.

https://www.acq.osd.mil/cmmc/docs/CMMC_Appendices_V1.02_20200318.pdf; B-2
CERT RMM v1.2 GG2.GP1 Subpractice 2; https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf

Policy v. Procedure

- “Policies are guidelines that regulate organization action. They control the conduct of people and the activities of systems.”
- “Procedures supplement the policy guidelines with specifics and complete the information users need. It’s not sufficient to say, “It is our policy to provide the best customer service in the industry and stop there.”
- “Users need to know what that means.”
- “How do I provide the best service.’”

Writing Effect Policies and Procedures, Nancy J. Campbell, AMACOM 1998 pages 1 and 3

References

- FAR 52.204-21 – entirety https://www.acquisition.gov
- NIST 800-171 r1 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
- NIST 800-171 r2 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST SP 800-53 Rev 4 - https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
- NIST CSF v1.1 - https://doi.org/10.6028/NIST.CSWP.04162018
- CERT RMM v1.2 - https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf
- CISecurity Controls - https://www.cisecurity.org/controls/
- AU ACSC Essential Eight - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
- UK NCSC Cyber Essentials - https://www.ncsc.gov.uk/cyberessentials/overview

UPCOMING TRAINING - EVENTS

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

CYBER FRIDAY LIVE WEBINAR SERIES

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.

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

- 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 10, 2021

  Acquisition Hour: Understanding Trends and Evolving Areas of Emphasis in the Federal Marketplace
  CLICK HERE for additional information
  Presented by Marc Violante, 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)
Cyber Friday

…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/

- REGISTER NOW -

January 26, 2021

CYBER SECURITY IS NO LONGER OPTIONAL – WEBINAR

This webinar will address key questions business executives should ask and discuss concerning cyber risks to their companies and the importance of using a common cybersecurity framework such as NIST 800-171 or CISecurity controls to protect their systems and business information.

All businesses, corporations, non-profits, and education professionals are encouraged to join us for this informative event.

More info at https://www.wispro.org/event/cyber-security-is-no-longer-optional-webinar/

January 28, 2021

13TH ANNUAL END OF YEAR FEDERAL CONTRACTOR UPDATE – VIRTUAL

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/

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

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