Developments in Federal Contracting Law

AGC Annual Conference
Anchorage, Alaska

Thursday, November 7, 2024

Presenters:
Anne Marie Tavella, Construction & Government Contracts Counseling & Litigation
Jonathan DeMella, Construction & Government Contracts Counseling & Litigation
Mike O'Brien, Employment Services

- Supply Chain Updates
- Status of Davis-Bacon Rules
- Cybersecurity Considerations
- Project Labor Agreements

Supply Chain

Supply Chain Issues in 2024

- Recovery since 2020, but issues persist
  - Costs remain higher than pre-Covid – roughly 40%
  - Electrical equipment – switchgears, generators, and AV
    - Lead times are 42-60 weeks
  - Labor - 20% increase in wages
  - Material lead times remain longer than pre-Covid
- Competitive Labor Market
  - Increase in large construction projects throughout the country
  - Retiring workforce
  - Lower early career entrants
  - Increasing need for trades, PMs, field engineers, superintendents, safety and quality control

Supply Chain – Mitigate Risks

- Mitigation begins pre-bid
- Evaluate project location and labor pool before bid
- Negotiate price escalation clauses
- Develop supplier relationships
  - Diversify relationships with vendors
- Create a supply chain plan and have a back-up plan
- Manage owner expectations
  - Create realistic schedules based on availability

FAR 52.216-4 Economic Price Adjustment – Labor and Material

- Requires the contractor notify the contracting officer if labor rates or unit prices increase or decrease
- Notice shall include a proposal for an adjustment to the price and supporting data explaining the cause of the price change
- Clause can only be included in a fixed price contract IF the contracting officer determines it is necessary to "protect the contractor and the Government against significant fluctuations in labor or material cost or to provide for contract price adjustment in the event of changes in the contractor's established prices." FAR 16.203-3

Price Escalation Clauses

- If no EPA is included, ask in pre-bid Q&A if it can be added
  - If the answer is no, consider your pricing
- Ensure clauses in subcontracts meet the same requirements of the FAR clause
- Review force majeure clauses in subcontracts closely
- Negotiate escalation clauses in private contracts

Davis Bacon

Davis Bacon Update

- Generally, applies to construction contractors and subcontractors
- Federally funded or assisted contracts in excess of $2,000 for construction, alteration, or repair of public buildings/public works
- Applies to “mechanics and laborers employed directly on the site of the work”
- DOL issued a new rule effective October 23, 2023
- Purpose of changes:
  - Ensure that workers are paid locally prevailing wages
  - Ensure that Government’s contracting activity does not depress wages
  - Ensure that Government creates a fair opportunity for responsible contractors to bid

Davis Bacon Update

- Lawsuit by AGC of America
- On June 24, 2024, U.S. District Court for the Northern District of Texas issued a nationwide preliminary injunction on the following provisions:
  - Defining material suppliers as contractors if they perform ANY work onsite
  - Drivers who work for construction contractors are covered for any non *de minimis* time when their work requires them to come on and off site
  - Applies the clause via operation of law if the agency erroneously failed to include it in the contract, if the contract would otherwise be covered

Davis Bacon Update

Other changes have been in effect since last October

Ensure you know whether the job site is classified as rural or urban for estimating and compliance

Expanded definitions of building and work have expanded the DBA's reach

Record preservation requirements

- Three years after project completion

Cybersecurity / CMMC

Cybersecurity Maturity Model Certification – Final Rule

- Effective Date - December 16, 2024
- Represents 5-year effort to move away from “self-attestation” model of security
- CMMC – 3 key features:
  - *Tiered model* - CMMC requires companies entrusted with FCI and CUI to implement cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information
  - *Assessment requirement* – CMMC assessments allow the Department to verify the implementation of clear cybersecurity standards
  - *Phased implementation* – Once CMMC rules become effective, certain DoD contractors handling FCI and CUI will be required to achieve a particular CMMC level as a condition of contract award

DoD Proposed Acquisition Rule Still Coming

- Amend DFARS to address procurement-related considerations of CMMC. When finalized:
  - Will allow DoD to require CMMC specific level in solicitation or contract
  - Contracting officers will not make award, exercise option, or extend PoP if offeror does not have the passing results of a current certification assessment or self-assessment for the required CMMC level
  - Affirmation of continuous compliance for all systems that process store or transmit FCI or CUI
- The appropriate CMMC certification requirements will flow down to subcontractors at all tiers when the subcontractor processes, stores, or transmits FCI or CUI
- Contractors that fail to comply will be subject to "standard contractual remedies"

DoD Phasing Approach

- **Phase 1 (2025)**
  - Begins December 16, 2024 (Effective date of final rule)
  - Idea is to focus on **self-assessment**, give contractors time to meet CMMC requirements
- **Phase 2 (2026)**
  - Begins December 16, 2025
  - Expansion to **certification requirement**
- **Phase 3 (2027)**
  - Begins December 16, 2026
  - At this point, **CMMC in solicitations -** requirement applicable at contract award as well as option periods
  - PMs (KOs) can delay only the Level 3 cert assessment from award to exercise of option period, **but not Level 2**
- **Phase 4 (2028)**
  - Begins 1 December 16, 2027
  - CMMC identified in solicitations as **condition of contract award** and as **condition of contract option**
  - Gov PMs may seek DoD approval for waiver
  - **No avenue for offerors to seek waivers**

Best Practices

Key Understandings About CMMC

- Understand that CMMC is a “pre-award requirement”
- Understand the CMMC Contract Requirement: “The type and sensitivity of information to be utilized during the contract, FCI or CUI, determines the requirements in the solicitation, which then informs the CMMC level required.”
  - “The CMMC assessment level required does not change based on acquisition lifecycle phase, but based on whether FCI and CUI are processed, stored, or transmitted on contractor owned information systems”
- Understand Flowdown: “It is up to each OSA to protect FCI and CUI and to determine the assessment boundary, policies, and procedures necessary to do that.”
  - “Prime contractors are responsible for complying with contract terms and conditions, including the requirement to flow down applicable CMMC requirements to subcontractors.”

How do we know if we will have CUI?

- CUI may not always be marked correctly; it may also not be handled correctly by your customers. Which means you may receive CUI without protections.
  - CUI information provided should be marked on the header and footer with “CUI”
  - Review all documentation provided by the Government for CUI markings.
- Just because CUI isn’t marked on the contract documents doesn’t mean you won’t be handling CUI.
  - Check deliverables and specifications for requirements to mark data created or produced for the contract as CUI.
- What if nothing is marked and there are no requirements to mark data?
  - When the DFARS clause is present and nothing is marked, per the clause, the determination and risk is still on you (as the prime).
  - A simple question posed during the solicitation stage or after award is enough to mitigate your risk.

Is the 7012 or 7020 clause in the solicitation?

- Ensure the RFP documents, specs, drawings, etc., are fully reviewed for CUI markings
- If CUI is identified **only subcontractors that are compliant can receive CUI.** Before you provide documents, at a minimum:
  - Ask subcontractors the question in writing BEFORE providing CUI – email will work!
  - *"Is your company compliant with the DFARS clause 252.204-7012/7020?"*
  - Save the response in the proposal file.
- Ensure subs are aware of CUI obligations and are prepared to comply at bid time
  - Flowing down the clauses is not always sufficient, especially if you are aware the subcontractor cannot or will not comply with the requirements
  - Even sophisticated subcontractors could be using document management systems that are not compliant

Send a notice to the Contracting Officer

If CUI is delivered without protections and pages are marked as CUI, send this:

- *Pages within the contract documents provided [ADD PAGE #s] are marked "CUI." However, controls or protocols were not used to protect this information when received from the Government. Furthermore, the information does not appear to meet the criteria for Covered defense information," as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html* ***Therefore, we are treating this as improperly marked non-CUI data****, pursuant to DFARS 252.204-7012. If this is not correct, please advise us of the proper protection protocols as soon as possible.*

If the 7020 clause is in the solicitation or contract documents but no protections were required to receive them:

- *The contract documents include DFARS 252.204-7020 NIST SP 800-171 DoD Assessment Requirements. However, no controls or protocols were used to protect this information when received from the Government. Furthermore, the information does not appear to meet the criteria for Covered Defense Information," as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, and no CDI or CUI shall be collected, developed, received, transmitted, used, or stored by NOK or its subcontractors during the performance of the contract.* ***Therefore, compliance with the DFARS clause is not required, pursuant to DFARS 252.204-7012****. If this is not correct, please advise us of the data requiring protection protocols as soon as possible.*

Save the correspondence in the job folder as you would a serial letter.

If CUI is or will be in your contract

All CUI data should (must) be stored in the secure environment

Consider team members needing access to CUI and how accounts and data will be controlled and set up

Delete any CUI data from Outlook, any shared platform, any third-party cloud platform that is not approved

Resources

How Do CMMC Rules Work Together?

- FAR 52.204–21 requires compliance with 15 security requirements, the minimum necessary for any entity wishing to receive FCI from the USG
- DFARS 252.2024-7012 is applicable to Defense contracts involving the development or transfer of CUI to a non-Government organization. Requires defense contractors to provide adequate security on all covered contractor information systems by implementing the 110 security requirements specified in NIST SP 800–171
  - Compliance requires SSP explaining how you will comply with NIST SP 800-171
- DFARS 252.204–7019 and DFARS 252.204–7020 require submission of self-assessment scores to SPRS. Highest score is 110.
  - If you don't meet the 110 score, you need a POAM
- DFARS 252.204–7020 notifies contractors that DoD reserves the right to conduct a higher-level assessment of contractors' cybersecurity compliance, and contractors must give DoD assessors full access to their facilities, systems, and personnel
- DFARS 252.204–7021 paves the way for rollout of the CMMC Program. Once CMMC is implemented, the required CMMC Level and assessment type will be specified in the solicitation and resulting contract.

CMMC Level and Assessment Requirements

CMMC status	Source & number of security reqts.	Assessment reqts.	Plan of action & milestones (POA&M) reqts.	Affirmation reqts.
Level 1 (Self)	• 15 required by FAR clause 52.204–21.	• Conducted by Organization Seeking Assessment (OSA) annually. • Results entered into SPRS (or its successor capability).	• Not permitted	• After each assessment. • Entered into SPRS.
Level 2 (Self)	• 110 NIST SP 800–171 R2 required by DFARS clause 252.204–7012.	• Conducted by OSA every 3 years • Results entered into SPRS (or its successor capability). • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4.	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days. • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date.	• After each assessment and annually thereafter. • Assessment will lapse upon failure to annually affirm. • Entered into SPRS (or its successor capability).
Level 2 (C3PAO).	• 110 NIST SP 800–171 R2 required by DFARS clause 252.204–7012.	• Conducted by C3PAO every 3 years • Results entered into CMMC Enterprise Mission Assurance Support Service (eMASS) (or its successor capability). • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4.	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days. • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date.	• After each assessment and annually thereafter. • Assessment will lapse upon failure to annually affirm. • Entered into SPRS (or its successor capability).
Level 3 (DIBCAC).	• 110 NIST SP 800–171 R2 required by DFARS clause 252.204–7012. • 24 selected from NIST SP 800–172 Feb2021, as detailed in table 1 to § 170.14(c)(4).	• Pre-requisite CMMC Status of Level 2 (C3PAO) for the same CMMC Assessment Scope, for each Level 3 certification assessment. • Conducted by Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) every 3 years. • Results entered into CMMC eMASS (or its successor capability). • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4.	• Permitted as defined in § 170.21(a)(3) and must be closed out within 180 days. • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date.	• After each assessment and annually thereafter. • Assessment will lapse upon failure to annually affirm. • Level 2 (C3PAO) affirmation must also continue to be completed annually. • Entered into SPRS (or its successor capability).

Subcontractor Flowdown Requirements

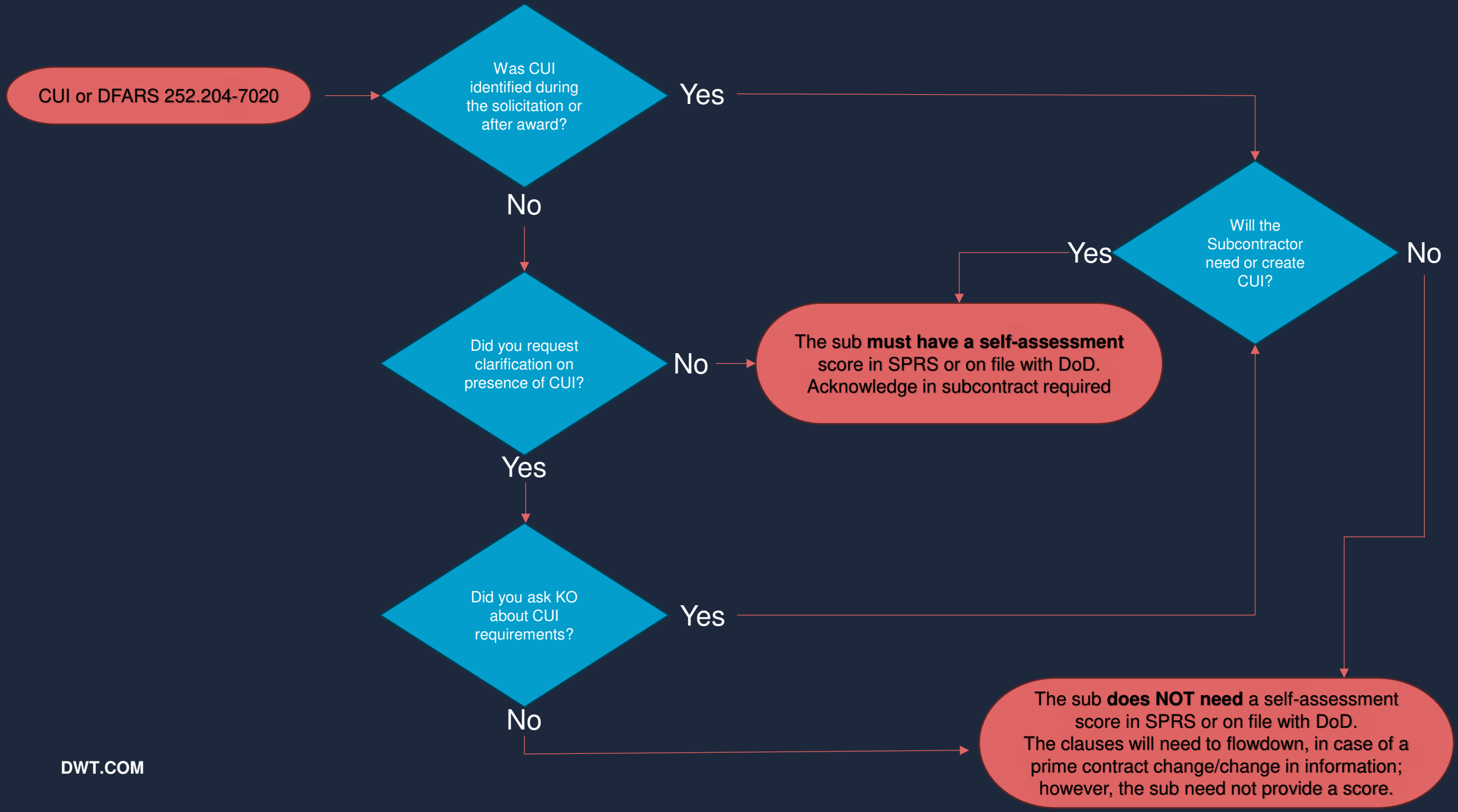
Prime contractor requirement	Minimum subcontractor requirement If the subcontractor will process, store, or transmit	
	FCI	CUI
Level 1 (Self)	Level 1 (Self)	N/A.
Level 2 (Self)	Level 1 (Self)	Level 2 (Self).
Level 2 (C3PAO)	Level 1 (Self)	Level 2 (C3PAO).
Level 3 (DIBCAC)	Level 1 (Self)	Level 2 (C3PAO).

Abbreviations & Definitions

Abb.	Phase	Notes and Definitions
C3PAO	CMMC Third Party Assessor Organization	Authorized to conduct and deliver CMMC assessments
CDI	Covered Defense Information	Unclassified controlled technical information or other information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is (1) marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or (2) collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract
CUI	Controlled Unclassified Information	A broad spectrum of data that is not classified but requires security protections
CMMC	Cybersecurity Maturity Model Certification	The DoD's program to enforce protection of sensitive unclassified information that is shared by the DoD with its contractors and subcontractors
CMMC AB	CMMC Accredited Body	Accredits C3PAOs
CSP	Cloud Service Provider	

Abbreviations & Definitions

Abb.	Phase	Notes and Definitions
DIB CAC	Defense Industrial Base Cybersecurity Assessment Center	Conducts assessments of contractor compliance with cybersecurity regulations
ESP	External Service Provider	
FCI	Federal Contract Information	All data that is generated during a contract with the Government that is not CUI. Generally covered by FAR 52.204-21
Fed RAMP	Federal Risk and Authorization Management Program	Government program that provides a standard approach to security assessment, authorization, and monitoring for cloud products or services
NIST	National Institute of Standards and Technology	Government agency that developed the framework for the Government's cybersecurity requirements
OSC	Organization Seeking Compliance	
POA&M	Plan of Action & Milestone	Contractors who fail to meet NIST standards can develop a POA&M in order to maintain compliance with DFARS 252.204-7012
SPRS	Supplier Performance Risk System	DoD application that provides information regarding supplier performance
SSP	System Security Plan	Describes security requirements for an information system and the security controls in place or planned for meeting those requirements


CUI or DFARS 252.204-7020
Was CUI identified during the solicitation or after award?
Yes
No
Did you request clarification on presence of CUI?
No
The sub **must have a self-assessment** score in SPRS or on file with DoD. Acknowledge in subcontract required
Yes
Did you ask KO about CUI requirements?
Yes
No
Will the Subcontractor need or create CUI?
Yes
No
The sub **does NOT need** a self-assessment score in SPRS or on file with DoD. The clauses will need to flowdown, in case of a prime contract change/change in information; however, the sub need not provide a score.

CMMC – Best Practices, Questions

Do you have a solid understanding of which level you will be seeking and scope?	Have you defined your "senior official" for affirmation?	Do you consider what support/continuous monitoring will be the basis of that affirmation?
Have you inventoried all the ESP and CSP that are part of your scope? Have you engaged those parties for their readiness?	Are you prepared for all the non-POA&M-allowed practices?	Do you have a plan for when to get certified?

Project Labor Agreements

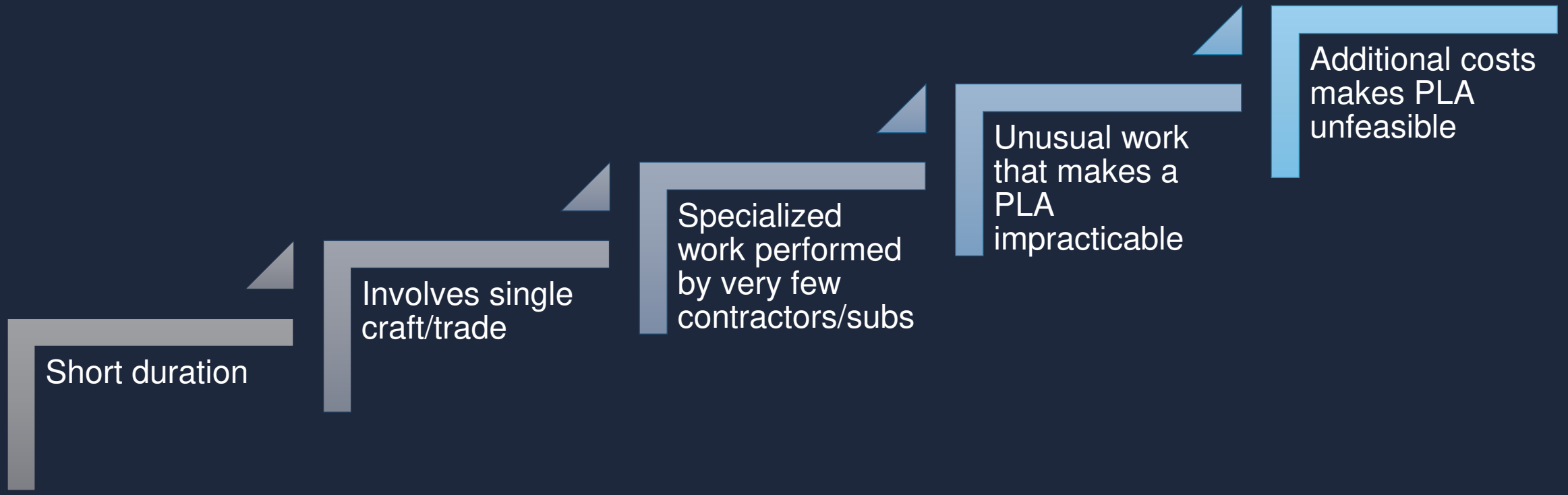
February 4, 2022 Executive Order

- Project labor agreements are illegal outside of construction industry
- Affects federal construction projects
- Applies to projects $35 MM or more
- Mandates federal contractor/union cooperation on large projects with multiple trades
- Aims to avoid labor/management disputes
- Took effect January 22, 2024

Project Labor Agreements Must

- Must bind all contractors and subcontractors
- Make it clear that contractors and subs are not mandated to be union shops
- Bar strikes, lockouts, other “work action”
- Set out dispute resolution process, usually arbitration
- Set out terms and conditions of productivity/deadlines, work quality, health and safety

Exempted Work



Challenges

- Contractors have very little leverage establishing the PLA's terms.
- Instead of awarding subcontracts based on cost-effective bids and performance history, the contractor makes awards based, foremost, on a company's willingness to agree to the PLA.
- Contractors are typically given no opportunity to negotiate the terms of the PLA. Most often, government representatives simply adopt terms presented to them by the building trade unions or negotiate the terms themselves.
- PLAs may require contractors to deal with as many as 15 different unions and to comply with the wage, benefits, and labor practices of such unions.
- The PLA may establish different, more onerous, work rules from those in area-wide agreements.
- The PLA may impose different grievance or arbitration procedures than the area-wide agreements.

Questions?

Anne Marie Tavella

Counsel, Anchorage

annemarietavella@dwt.com

907.257.5345

Jonathan DeMella

Partner, Seattle

JonathanDemella@dwt.com

206.757.8338

Mike O’Brien

Partner, Anchorage

mikeobrien@dwt.com

907.257.5342