Michigan Defense Expo (MDEX)

ACC-DTA Contracting Updates

Agenda

- ✓CARES Act Section 3610
- ✓Section 889
- ✓Cybersecurity & CMMC

CARES Act Section 3610

✓**Allows agencies to reimburse a contractor for paid leave utilized to keep its employees or subcontractors in a ready state during the public health emergency declared for COVID–19**

- Reimbursement allowed at the minimum applicable contract billing rates (not to exceed an average of 40 hours per week), for any paid leave including sick leave, including to protect the life and safety of Government and contractor personnel

✓**EFFECTIVE DATES**: 27 March 2020 through **30 September 2021**

✓**FACTS**:

- Reimbursement is permissive not mandatory
- Reimbursement is subject to the availability of funds
- Profit and fee will NOT be reimbursed
- Contractors are responsible for supporting claimed costs & requests should include subcontractor requests for same time/contract
- Contractor must be determined to be an affected contractor

CARES Act Section 3610 cont.

✓**ACTIONS TO TAKE: Reimbursement requests shall follow the applicable DPC Checklist, which may be tailored at Contracting Officer discretion (Reference: Class Deviation 2020-O0021 Rev 3, Section 3610 Reimbursement Requests, dated 23 March 2021)**

- Three types of 3610 reimbursement requests: Single Contract, Multiple Contracts, and Business Unit/Segment
- Single Contracts
  - Abbreviated Reimbursement Checklist (if amount requested is below $2M)
  - Multipurpose Reimbursement Checklist (if Abbreviated Checklist not utilized)
- Multiple Contracts
  - Multipurpose Reimbursement Checklist
  - Should be a similar group of contracts, such as contracts for a single program or with a single contracting activity or DoD Component
- Business Unit/Segment
  - Global Reimbursement Checklist
  - DCMA acts as the Cognizant Federal Agency Official (CFAO) on behalf of the Department

Section 889

✓**Section 889 of the FY19 NDAA contained two prohibitions related to Contracting:**

- **Sec 889(a)(1)(A):** Took effect 13 August 2019 & prohibits the Government from buying and using covered telecommunications equipment or services from the five named Chinese companies and their subsidiaries or affiliates.

PROHIBITED SOURCES
***Huawei Technologies Company**
***ZTE Corporation**
***Hangzhou Hikvision Digital Technology Company**
***Hytera Communications**
***Dahua Technology Company**

- **Section 889(a)(1)(B):** Took effect 13 August 2020 & prohibits contracting with entities that use any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system

Section 889 cont.

✓**FACTS**:

- Applies to ALL dollar values, including Micro Purchases
- Applies to Non-Commercial and Commercial Items (including COTS)
- Requirements flow down to subcontracts
- FAR 52.204-24 (provision) requires offerors to represent whether covered telecommunications equipment or services are used, and if so, to provide further information
- FAR 52.204-25 (clause) prohibits contracting with entities that use covered telecommunications or services and requires contractor to report use of any such equipment, systems, or services discovered during contract performance
- FAR 52.204-26 (provision) requires offerors to represent whether covered telecommunications equipment or services are provided as part of offered products or services to the Government in the performance of any contract

Section 889 cont.

✓**<u>ACTIONS TO TAKE</u>: FAR 52.204-24, FAR 52.204-25, & 52.204-26 mandatory in:**

- ALL new solicitations, resulting contracts, and task/delivery orders
- ALL existing indefinite delivery vehicles PRIOR to placing any future orders
- Existing contracts/orders PRIOR TO or AS they are modified to add new work or extend the POP (including exercising options)
- Contractor Representations required by FAR 52.204-24 & 52.204-26 must be provided prior to award
  - If contractor represents they use covered telecommunications in response to 52.204-24(d)(2), a detailed lay-down and phase out plan is also required

Section 889 cont.

✓**EXCEPTIONS: Reference FAR 4.2102(b)**

- Third-party connections (e.g. backhaul, roaming, or interconnection arrangements)
- Telecommunications that cannot route or redirect traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles

✓**WAIVERS: Reference FAR 4.2104**

- PCO is not required to pursue & can reject offers that include covered telecommunications
- Section 889 (d)(1) Executive Agency Waiver, expires 13 August 2022
  - 1-time waiver
- Section 889(d)(2) Director of National Intelligence (DNI) Waiver, no expiration
  - Must meet national security interests of the US, no expiration
- DNI granted temporary waiver, expires 30 September 2022
  - Allows DoD to execute actions for goods and services deemed to be low risk
  - Contractor still required to provide required representations prior to award

Cybersecurity and the Department of Defense

✓**Section 1648 of the NDAA for FY 2020 (Pub. L. 116-92) required the Department of Defense (DoD) develop a consistent, comprehensive framework to enhance the cybersecurity of the United States Defense Industrial Base (DIB)**

- **VISION**: Establish a unified cybersecurity standard for DoD acquisitions to reduce exfiltration of Controlled Unclassified Information (CUI) from the DIB

- **GOAL**: Provide increased assurance to the DoD that a DIB contractor can adequately protect sensitive unclassified information such as Federal Contract Information (FCI) and CUI

Current Cybersecurity Requirements

- ✓**DFARS 252.204-7012 (clause) directs <u>how</u> the contractor shall protect covered defense information**
  - Requires the contractor to provide adequate security to safeguard covered defense information that is on or is transiting through a contractor's internal information system/network
    - Implement at a minimum, NIST SP 800-171, Protecting CUI in Nonfederal systems and Organizations
  - Report cyber incidents (https://dibnet.dod.mil)

Future Cybersecurity Requirements

✓**DoD published Interim Rule DFARS Case 2019-D041**

- Amends DFARS 204 & DFARS 252.204 to implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification (CMMC) framework
- Assesses contractor implementation of cybersecurity requirements and enhances the protection of unclassified information within the DoD supply chain
- Includes new NIST SP 800-171 Assessment Methodology

Interim Rule: New DFARS Provisions/Clauses

✓**DFARS 252.204-7019 (provision): Notice of NIST 800-171 DoD Assessment Requirements**

- Requires the contractor to perform an assessment prior to award and maintain a record within the Supplier Performance Risk System (SPRS), assessments generally valid 3 years
  - Information that must be posted include systems security plan, schedule for implementing controls (POAM), Summary level score

✓**DFARS 252.204-7020 (clause): Notice NIST 800-171 DoD Assessment Requirements**

- Describes the DoD Assessment requirements
- Requires contractors provide access to its facilities, systems, and personnel when the DoD is conducting a Medium or High assessment

✓**DFARS 252.204-7021 (clause): Cybersecurity Maturity Model Certification Requirements**

- Describes CMMC requirements (which must be achieved prior to award) and requires CMMC be used or included in all contracts, task orders, solicitations, etc. valued greater than micro-purchase threshold (except for COTS items)
- Prior to 01 October 2025, Office of Secretary of Defense must approve the use of this clause
  - On/After 01 October 2025 CMMC (minimum Level 1) becomes a requirement in all contracts

Actions to Take Now

1. Register on the Supplier Performance Risk System (SPRS)
2. Produce and maintain a System Security Plan (SSP) and Plan of Action and Milestones (POA&M) for each system, (per DFARS 252.204-7012)
3. Conduct a self-assessment in accordance with the NIST SP 800-171 "DoD Assessment Methodology" (110 controls)
4. Verify the self-assessment score into SPRS prior to award, option exercise, or extension of a contract, task order, or delivery order (if Basic Assessment is not in SPRS follow procedure in 252.204-7019 (c)(2))
5. Produce and maintain policy, process, and system documentation / evidence of compliance
6. Remediate all open POA&M items to achieve a perfect score of 110 and update SPRS accordingly
7. Ensure all sub-contractors also perform the above
8. Repeat #4-7 no less than once every 3 years

Prepare for the Future

1. Achieve a 100% "Basic" self-assessment score in strict adherence to the NIST SP 800-171 "DoD Assessment Methodology"

2. Remediate all known weaknesses as identified in the POA&M

3. Conduct a formal Risk Assessment to understand the contract assets, business needs, and data being protected

CMMC Facts

✓**Five-tier certification model that consists of maturity levels that range from "Basic Cybersecurity Hygiene" to "Advanced/Progressive", each with processes and practices**

✓**CMMC Accreditation Body will accredit CMMC Third Party Assessment Organizations (C3PAOs) and individual assessors**

- Still establishing requirements for becoming a C3PAO

✓**DIB companies will be able to select an approved C3PAO and schedule a CMMC assessment for a specific level**

- CMMC Certificates generally valid for 3 years
- Minimum Level 1 Certification required beginning 01 October 2025

CMMC Details can be found at:
https://www.acq.osd.mil/cmmc

CMMC Certification Levels

- ✓**Level 1:** Consists of the 15 basic safeguarding requirements from FAR clause 52.204-21, basic cyber hygiene

- ✓**Level 2:** Consists of 65 security requirements from NIST SP 800-171 implemented via DFARS clause 252.204-7012, 7 CMMC practices to support intermediate cyber hygiene, and 2 CMMC processes. Intended as an optional intermediary step for contractors as part of their progression to Level 3

- ✓**Level 3:** Consists of all 110 security requirements from NIST SP 800-171, 20 CMMC practices to support good cyber hygiene, and 3 CMMC processes

- ✓**Level 4:** Consists of all 110 security requirements from NIST SP 800-171, 46 CMMC practices to include proactive processes, and 4 CMMC processes

- ✓**Level 5:** Consists of all 110 security requirements from NIST SP 800-171, 61 CMMC practices to include advanced/progressive practices, and 5 CMMC processes