Subpart 204.75 - CYBERSECURITY MATURITY MODEL CERTIFICATION

Parent topic: Part 204 - ADMINISTRATIVE AND INFORMATION MATTERS

204.7500 Scope of subpart.

(a) This subpart prescribes policies and procedures for including the Cybersecurity Maturity Model Certification (CMMC) level requirements in DoD contracts. CMMC is a framework (see 32 CFR part 170) for assessing a contractor's information security protections.

(b) This subpart does not abrogate any other requirements regarding contractor physical, personnel, information, technical, or general administrative security operations governing the protection of unclassified information, nor does it affect requirements of the National Industrial Security Program.

(c) This subpart applies to unclassified contractor information systems.

204.7501 Definitions.

As used in this subpart—

"Controlled unclassified information" means information the Government creates or possesses, or information an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls (32 CFR 2002.4(h)).

"Current" means—

(1) With regard to Conditional Cybersecurity Maturity Model Certification (CMMC) Status—

(i) Not older than 180 days for Conditional Level 2 (Self) assessments and Conditional Level 2 (certified third-party assessment organization (C3PAO)) assessments, with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Conditional CMMC Status date (see 32 CFR 170.16 and 170.17); and

(B) A corresponding affirmation of continuous compliance by an affirming official (see 32 CFR 170.4); and

(ii) Not older than 180 days for Conditional Level 3 (Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)) assessments, with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Conditional CMMC Status date (see 32 CFR 170.18); and

(B) A corresponding affirmation of continuous compliance by an affirming official;

(2) With regard to Final CMMC Status—

(i) Not older than 1 year for Final Level 1 (Self), with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Final CMMC Status date (see 32 CFR 170.15); and

(B) A corresponding affirmation of continuous compliance, not older than 1 year, by an affirming official;

(ii) Not older than 3 years for Final Level 2 (Self) assessments and Final Level 2 (C3PAO) assessments, with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Final CMMC Status date (see 32 CFR 170.16 and 170.17); and

(B) A corresponding affirmation of continuous compliance, not older than 1 year, by an affirming official; and

(iii) Not older than 3 years for Final Level 3 (DIBCAC) assessments, with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Final CMMC Status date (see 32 CFR 170.18); and

(B) A corresponding affirmation of continuous compliance, not older than 1 year, by an affirming official; and

(3) With regard to affirmation of continuous compliance (32 CFR 170.22), not older than 1 year with no changes in compliance with the requirements at 32 CFR part 170.

“Cybersecurity Maturity Model Certification (CMMC) status” means the result of meeting or exceeding the minimum required score for the corresponding assessment. The potential statuses are as follows:

(1) Final Level 1 (Self).

(2) Conditional Level 2 (Self).

(3) Final Level 2 (Self).

(4) Conditional Level 2 (C3PAO).

(5) Final Level 2 (C3PAO).

(6) Conditional Level 3 (DIBCAC).

(7) Final Level 3 (DIBCAC).

“Cybersecurity Maturity Model Certification unique identifier (CMMC UID)” means 10 alpha-numeric characters assigned to each CMMC assessment and reflected in theSupplier Performance Risk System (SPRS) for each contractor information system.

“Federal contract information (FCI)” means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government. It does not include information provided by the Government to the public, such as on public websites, or simple transactional information, such as information

necessary to process payments.

204.7502 Policy.

(a) Award eligibility.

(1) The contracting officer shall include in the solicitation the required CMMC level, if provided by the program office or the requiring activity.

(2) Contracting officers shall not award a contract, task order, or delivery order to an offeror that does not have a current CMMC status at the CMMC level required by the solicitation.

(3) Contractors are required to achieve, at time of award, a CMMC status at the CMMC level specified in the solicitation, or higher, for all information systems used in the performance of the contract, task order, or delivery order that will process, store, or transmit FCI or CUI. Contractors are required to maintain a current CMMC status at the specified CMMC level or higher, if required by the contract, task order, or delivery order, throughout the life of the contract, task order, or delivery order.

(b) CMMC status.

(1) Contracting officers may award a contract, task order, delivery order, or modification to exercise an option or extend a period of performance, if the offeror's or contractor's CMMC status is—

(i) Listed in the definition of "CMMC status"; and

(ii) Equal to or higher than the CMMC level required by the solicitation or contract, task order, or delivery order.

(2) CMMC levels 2 and 3 can be in a conditional level for a period not to exceed 180 days from the CMMC status date (32 CFR 170.21), and award can occur with a conditional CMMC level. CMMC level 1 requires a final CMMC level for award.

204.7503 Procedures.

(a) *CMMC level*. The contracting officer shall include the CMMC level (see 32 CFR 170.19) required by the program office or requiring activity in the solicitation provision and contract clause prescribed at 204.7504.

(b) *Award*. Contracting officers shall check SPRS and not award a contract, task order, or delivery order to an offeror that does not have a current CMMC status posted in SPRS at the CMMC level (see 32 CFR 170.15 through 170.18) required by the solicitation, or higher, for each CMMC UID provided by the offeror. The CMMC UIDs are applicable to each of the contractor information systems that will process, store, or transmit FCI or CUI and that will be used in performance of the contract.

(c) *Option exercise or period of performance extension*. Contracting officers shall check SPRS and not exercise an option or extend the period of performance on a contract, task order, or delivery

order, unless the contractor has a current CMMC status posted in SPRS at the CMMC level (see 32 CFR 170.15 through 170.18) required by the contract, task order, or delivery order, or higher, for each CMMC UID provided by the contractor. The contractor's CMMC UIDs are applicable to each of the contractor information systems that process, store, or transmit FCI or CUI and that are or will be used in performance of the contract.

(d) *CMMC UIDs*. If the contractor provides new CMMC UIDs during performance of the contract, task order, or delivery order, the contracting officer shall check in SPRS, using the CMMC UIDs assigned by SPRS, that the contractor has a current CMMC status at the required CMMC level, or higher, for each of the contractor information systems identified that will process, store, or transmit FCI or CUI during contract performance.

204.7504 Solicitation provision and contract clause.

(a) Unless the requirements at 32 CFR 170.5(d) are met, use the clause at 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements, as follows:

(1) Until November 9, 2028 in solicitations and contracts, task orders, or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, except for those solely for the acquisition of commercially available off-the-shelf (COTS) items, if the program office or requiring activity determines that the contractor is required to have a specific CMMC level.

(2) On or after November 10, 2028 in solicitations and contracts, task orders, or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, except for those solely for the acquisition of COTS items, if the program office or requiring activity determines that the contractor is required to use contractor information systems in the performance of the contract, task order, or delivery order to process, store, or transmit FCI or CUI.

(b) Use the provision at 252.204-7025, Notice of Cybersecurity Maturity Model Certification Level Requirements, in solicitations that include the clause at 252.204-7021.