**DFARS Case 2019-D041**

**Assessing Contractor Implementation of Cybersecurity Requirements**

**Final Rule**

**PART 204—ADMINISTRATIVE AND INFORMATION MATTERS**

**\* \* \* \* \***

**subpart 204.75–CYBERSECURITY MATURITY MODEL CERTIFICATION**

**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]**~~that measures a contractor’s cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes (see https://www.acq.osd.mil/cmmc/index.html)~~.

(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 the** **Supplier 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.]**

**204.750~~1~~[2] 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 ~~(i.e., not more than 3 years old)~~ CMMC **[status]** ~~certificate~~ at the **[CMMC]** level required by the solicitation.

(~~b~~**[3]**) Contractors are required to achieve, at time of award, a CMMC ~~certificate~~ **[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 ~~(i.e., not more than 3 years old)~~ CMMC ~~certificate~~ **[status]** at the specified **[CMMC]** level **[or higher]**, if required by the ~~statement of work or requirement document~~**[contract, task order, or delivery order]**, throughout the life of the contract, task order, or delivery order. ~~Contracting officers shall not exercise an option period or extend the period of performance on a contract, task order, or delivery order, unless the contract has a current~~ ~~(i.e., not more than 3 years old) CMMC certificate at the level required by 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.**

~~(c) The CMMC Assessments shall not duplicate efforts from any other comparable DoD assessment, except for rare circumstances when a re-assessment may be necessary such as, but not limited to~~ ~~when there are indications of issues with cybersecurity and/or compliance with CMMC requirements.~~

**204.750~~2~~[3] Procedures.**

(a) **[*CMMC level*.]**~~When a requiring activity identifies a requirement for a contract, task order, or delivery order to include a specific CMMC level, the contractor shall not—~~**[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.]**

~~(1) Award to an offeror that does not have a CMMC certificate at the level required by the solicitation; or~~

~~(2) Exercise an option or extend any period of performance on a contract, task order, or delivery order unless the contractor has a~~ ~~CMMC certificate at the level required by the contract.~~

~~(b) Contracting officers shall use Supplier Performance Risk System (SPRS) (~~[~~https://www.sprs.csd.disa.mil/~~](https://www.sprs.csd.disa.mil/)~~) to verify an offeror or contractor’s CMMC level.~~

**204.750~~3~~[4 Solicitation provision and c]~~C~~ontract clause**.

**[(a)** **Unless the requirements at 32 CFR 170.5(d) are met, u]**~~U~~se the clause at 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement**[s]**, as follows:

~~(a)~~ [(1)] Until ~~September 30, 2025,~~ [November 9, 2028] in solicitations and contracts[,] ~~or~~ task orders[,] or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, except for ~~solicitations and contracts or orders~~[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] ~~if the requirement document or statement of work requires a contractor to have a specific CMMC level. In order to implement a phased rollout of CMMC, inclusion of a CMMC requirement in a solicitation during this time period must be approved by OUSD(A&S)~~.

(~~b~~[2]) On or after ~~October 1, 2025,~~[November 10, 2028] in ~~all~~ solicitations and contracts[,] ~~or~~ task orders[,] or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, except for ~~solicitations and contracts or orders~~[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.]

**\* \* \* \* \***

**PART 212—ACQUISITION OF COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES**

**\* \* \* \* \***

**SUBPART 212.3—SOLICITATION PROVISIONS AND CONTRACT CLAUSES FOR THE ACQUISITION OF COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES**

**212.301 Solicitation provisions and contract clauses for acquisition of commercial products and commercial services.**

**\* \* \* \* \***

(f) \* \* \*

(ii) *Part 204—Administrative and Information Matters.*

**\* \* \* \* \***

(J) Use the provision at 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements, as prescribed in 204.7304(d).

(K) Use the clause at 252.204-7020, NIST SP 800-171 DoD Assessment Requirements, as prescribed in 204.7304(e).

(L) Use the clause at 252.204-7021, Cybersecurity Maturity Model Certification Requirements, as prescribed in 204.750~~3~~**[4]**(a) ~~and (b)~~.

(M) Use the clause at 252.204–7022, Expediting Contract Closeout, as prescribed in 204.804–70.

(N) Use the clause at 252.204–7023, Reporting Requirements for Contracted Services, to comply with 10 U.S.C. 4505.

(*1*) Use the basic clause as prescribed in 204.1705(a)(i) and (ii).

(*2*) Use the alternate I clause as prescribed in 204.1705(a)(i) and (iii).

(O) Use the provision at 252.204–7024, Notice on the Use of the Supplier Performance Risk System, as prescribed in 204.7604.

**[(P) Use the provision at 252.204-7025, Notice of Cybersecurity Maturity Model Certification Level Requirements, as prescribed in 204.7504(b).]**

**\* \* \* \* \***

**PART 217—SPECIAL CONTRACTING METHODS**

**\* \* \* \* \***

**subpart 217.2—OPTIONS**

**\* \* \* \* \***

**217.207 Exercise of options.**

(c) In addition to the requirements at FAR 17.207(c), exercise an option only after**[—]**~~:~~

(1) \* \* \* parts**[; and]**~~.~~

(2) **[Working with the program office or requiring activity to verify]**~~Verifying~~ in the Supplier Performance Risk System ~~(SPRS)~~ ~~(~~[~~https://www.sprs.csd.disa.mil/~~](https://www.sprs.csd.disa.mil/)~~)~~**[(**[***https://piee.eb.mil***](https://piee.eb.mil)**)]** that—

(i) \* \* \* (see 204.7303)**[; and]**~~.~~

(ii) **[If there is a requirement for the contractor to have a Cybersecurity Maturity Model Certification (CMMC) status at a specific CMMC level,]** ~~T~~**[t]**he contractor has **[a current CMMC status]** ~~a CMMC certificate~~ at the **[CMMC]** level required by the contract**[, or higher, for each of the CMMC unique identifiers applicable to each of the contractor information systems that process, store, or transmit Federal contract information or controlled unclassified information (see 204.7503(c)).]**~~, and that it is current(i.e., not more than 3 years old~~ ~~(see 204.7502).~~

**\* \* \* \* \***

**PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES**

**\* \* \* \* \***

**SUBPART 252.2—TEXT OF PROVISIONS AND CLAUSES**

**\* \* \* \* \***

**252.204-7021** **Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirement[s].**

As prescribed in 204.750~~3~~**[4]**(a) ~~and (b)~~, ~~insert~~**[use]** the following clause:

CONTRACTOR COMPLIANCE WITH THE CYBERSECURITY MATURITY MODEL CERTIFICATION LEVEL REQUIREMENT**[S]** (~~JAN 2023~~**[NOV 2025]**)

(a) *~~Scope.~~* ~~The Cybersecurity Maturity Model Certification (CMMC) CMMC is a framework that measures a contractor’s cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes (see~~ [~~https://www.acq.osd.mil/cmmc/index.html~~](https://www.acq.osd.mil/cmmc/index.html)~~).~~**[*Definitions*. As used in this clause—**

**[ “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 the** **Supplier 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.**

**“Plan of action and milestones” means a document that identifies tasks to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones, as defined in National Institute of Standards and Technology Special Publication 800-115 (32 CFR 170.21).]**

(b) **[*Framework*. The Cybersecurity Maturity Model Certification (CMMC) is a framework for assessing a contractor’s compliance with applicable information security protections (see 32 CFR part 170).**

**(c) *Duplication*. The CMMC assessments will not duplicate efforts from any other comparable DoD assessment, except for rare circumstances when a reassessment may be necessary, for example, when there are indications of issues with cybersecurity and/or compliance with CMMC requirements.**

**(d)]** *Requirements.* The Contractor shall**[—**

**[(1)(i) H]**~~h~~ave **[and maintain for the duration of the contract]** a current ~~(i.e., not older than 3 years)~~ CMMC ~~certificate~~**[status at the following CMMC level, or higher:** **\_\_\_\_\_\_\_\_\_\_\_\_ *[Contracting Officer insert: CMMC Level 1 (Self); CMMC Level 2 (Self); CMMC Level 2 (C3PAO); or CMMC Level 3 (DIBCAC)]* for all information systems used in performance of the contract, task order, or delivery order that process, store, or transmit FCI or CUI; and]** ~~at the CMMC level required by this contract and~~

**[(ii) Consult 32 CFR 170.23 related to the flowdown of the CMMC requirements,** **and flow down the correct CMMC level to subcontracts and other contractual instruments;]**~~maintain the CMMC certificate at the required level for the duration of the contract.~~

**(****2)** **Only process, store, or transmit FCI or CUI** **on contractor information systems that have a CMMC** **status at the CMMC level required** **in paragraph (d)(1) of this clause, or higher;**

**(3) Complete** **on an annual basis, and maintain as current,** **an affirmation, by the affirming official (see 32 CFR 170.4), of continuous compliance** **with the** **requirements associated with the CMMC level required in paragraph (d)(1) of this clause in the Supplier Performance Risk System** **(SPRS) (*https://piee.eb.mil*) for each** **CMMC UID applicable to each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract;**

**(4)** **Ensure all subcontractors and suppliers complete prior to subcontract award, and maintain on an annual basis,** **an affirmation, by the affirming official (see 32 CFR 170.4), of continuous compliance with the** **requirements associated with the CMMC level required for the subcontract or other contractual instrument** **for each of the subcontractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the subcontract; and**

**(5) If the Contractor has a CMMC Status of Conditional, successfully close out a valid plan of action and milestones (32 CFR 170.21) to achieve a CMMC Status of Final.]**

**(e)** ***Reporting.*  The Contractor shall—**

**(1)** **Submit to the Contracting Officer—**

**(i) The** **CMMC UID(s) issued by SPRS for contractor information systems that will process, store, or transmit FCI or CUI during performance of the contract; and**

**(ii)** **Any changes in the CMMC UIDs generated in SPRS throughout the life of the contract, task order, or delivery order, if applicable;**

**(2)** **Enter into SPRS the results of a current self-assessment for each** **CMMC UID, not covered by a C3PAO assessment or DIBCAC assessment, applicable to each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract; and**

**(3)** **Complete in SPRS on an annual basis and maintain as current** **an affirmation of continuous compliance by the affirming official (see 32 CFR 170.4) for each self-assessment, C3PAO assessment, or DIBCAC assessment required under the contract in SPRS.]**

(~~c~~**[f]**) *Subcontracts.*  The Contractor shall—

(1) Insert the substance of this clause, including this paragraph (~~c~~**[f]**)**[ and excluding paragraph (e)(1)]**, in ~~all~~ subcontracts and other contractual instruments, including ~~subcontracts~~**[those]** for the acquisition of commercial products and commercial services, excluding commercially available off-the-shelf items**[,** **if the subcontract or other contractual instrument will contain a requirement to process, store, or transmit FCI or CUI]**; and

(2) Prior to awarding ~~to a subcontractor~~**[****a subcontract or other contractual instrument]**, ensure that the subcontractor has a current ~~(~~*~~i.e.,~~* ~~not older than 3 years)~~ CMMC certificate **[or current CMMC status]** at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor **[based on the requirements at 32 CFR 170.23]**.

(End of clause)

**\* \* \* \* \***

**[****252.204-7025** **Notice of Cybersecurity Maturity Model Certification Level Requirements.**

**As prescribed in 204.7504(b), use the following provision:**

**NOTICE OF CYBERSECURITY MATURITY MODEL CERTIFICATION LEVEL REQUIREMENTS (NOV 2025)**

**(a) *Definitions*.** **As used in this provision, “****controlled unclassified information (CUI),” “current,” “Cybersecurity Maturity Model Certification (CMMC) status,” “Cybersecurity Maturity Model Certification unique identifier (CMMC UID),” “Federal contract information (FCI)”, and “plan of action and milestones” have** **the meaning given in the Defense Federal Acquisition Regulation Supplement 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements, clause of this solicitation.**

**(b****)(1) *Cybersecurity Maturity Model Certification (CMMC) level*. The CMMC** **level required by this solicitation is: \_\_\_\_\_\_\_\_\_\_\_\_ *[Contracting Officer insert:*** ***CMMC Level 1 (Self); CMMC Level 2 (Self); CMMC Level 2 (C3PAO); or CMMC Level 3 (DIBCAC)]*. This CMMC** **level, or higher (see 32 CFR part 170), is required prior to award for each contractor information system that will process, store, or transmit Federal contract information (FCI) or controlled unclassified information (CUI) during performance of the contract.**

**(2)** **The Offeror** **will not be eligible for award of a contract, task order, or delivery order resulting from this solicitation if the Offeror** **does not have, for each of the contractor information systems that will process, store, or transmit FCI or CUI and that will be used in performance of a contract resulting from this solicitation—**

**(i) The** **current CMMC** **status** **entered in the Supplier Performance Risk System (SPRS) (*https://piee.eb.mil*) at the CMMC level required by paragraph (b)(1) of this provision; and**

**(ii) A** **current affirmation of continuous compliance with the security requirements identified at 32 CFR part 170 in SPRS.**

**(c)** ***Plan of action and milestones*. If the Offeror has a CMMC Status of Conditional, the Offeror shall successfully close out a valid plan of action and milestones (32 CFR 170.21) to achieve a CMMC Status of Final.**

**(d)** ***CMMC unique identifiers*.** **The Offeror** **shall provide, in the proposal, the CMMC** **unique identifier(s) (CMMC UIDs) issued by SPRS for each contractor information system that will process, store, or transmit FCI or CUI during performance of a contract, task order, or delivery order resulting from this solicitation.** **The Offeror also shall update the list when new CMMC UIDs are generated in SPRS. The** **CMMC UIDs are provided in SPRS after the Offeror enters the results of self-assessment(s) for each such information system.**

**(End of provision)]**