19 September 2024

To: CMMC Program Management Office
Chief Information Officer
U.S. Department of Defense

Attn: Ms. Stacy Bostjanick, SES

Ms. Bostjanick and the CMMC Program Management Office (PMO);

Overall, we found the draft Defense Federal Acquisition Regulation Supplement clauses for Cybersecurity Maturity Model Certification (CMMC) to be well written and in-line with our expectations.

In the following pages, we identified four possible areas of improvement. In doing so, we also provided suggested recommendations to address what we identified.

Again, kudos to you and your team for building out the CMMC program.

Matthew Titcombe

Digitally signed by Matthew Titcombe
Date: 2024.09.20 12:58:19 -04'00'

Matthew A. Titcombe, CCA, CCP, CISSP
Chief Executive Officer

Overlap with DFARS Clause

The draft rule creates an overlapping reporting requirement for “cybersecurity lapses” to the contracting officer. Foremost, this is unactionable down the prime contractor’s supply chain as tier 2+ subcontractors don’t know who the contracting officer is and how to report to them. Secondly, it is unclear what value-add this will do by informing the contracting officer of a “lapse” when the contracting officer is not a qualified cybersecurity professional. This will likely generate negative performance ratings from the contracting officer, which in turn, will only stifle reporting as word gets out. Lastly, this will generate additional friction and overhead as the contractor must report to multiple DoD entities, respond to inquiries, and drag out its corrective actions instead of continuing to let all cybersecurity breaches go through DC3 as the current clearing house.

Cited Paragraphs

Draft DFARS Clause 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements, para (b)(4), “Notify the Contracting Officer within 72 hours when there are any lapses in information security or changes in the status of CMMC certificate or CMMC self-assessment levels during performance of the contract.”

DFARS Clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting, para (c) *Cyber incident reporting requirement.*

Recommendation

Remove the statement “lapses in information security or” from para (b)(4) and let DFARS Clause 252.204-7012 para (c) manage this requirement.

Lack of definition for “Lapse”

Presuming the CMMC PMO rejects the prior comment, the phrase “any lapses in information security” is ambiguous and lacking a definition for the word “lapse.” Additionally, the terminology is contradictory to the language found in DFARS Clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting, paragraphs (a) and (c)(1).

Cited Paragraph

Draft DFARS Clause 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements, para (b)(4), “Notify the Contracting Officer within 72 hours when there are any lapses in information security or changes in the status of CMMC certificate or CMMC self-assessment levels during performance of the contract.”

DFARS Clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting, para (a) *Definitions.*
“Compromise” means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.
“Cyber incident” means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

DFARS Clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting, para (c)(1) “When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor’s ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract.”

Recommendation

DoD should:

1. Add the compromise and cyber incident definitions from DFARS Clause 252.204-7012 to this clause

2. Replace “any lapses in information security” with “any cyber incidents.”

Assessment Level Reporting

It appears paragraph (b)(4) is missing a qualifier for the last “or” statement. If you were to take the first two “or” clauses out of para (b)(4), the sentence would read “Notify the Contracting Officer within 72 hours when there are any ... CMMC self-assessment levels during performance of the contract.” This doesn’t make any sense.

Cited Paragraph

Draft DFARS Clause 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements, para (b)(4), “Notify the Contracting Officer within 72 hours when there are any lapses in information security or changes in the status of CMMC certificate or CMMC self-assessment levels during performance of the contract.”

Recommendation

Presuming the missing qualifier is “changes in the status of,” we suggest changing para (b)(4) to “Notify the Contracting Officer within 72 hours when there are any lapses in information security or changes in the status of CMMC certificate or **changes in the status of** CMMC self-assessment levels during performance of the contract” to ensure there is clarity.

DoD may also want to adjust the language to include reporting to their primes any changes to DoD UID data in SPRS.

Reporting Any Changes

The words “any changes” Draft DFARS Clause 252.204-7021, para (c)(3) is ambiguous. An organization could interpret the statement to read as changes to the information system at-large or just changes to the DoD UID information in SPRS.

Cited Paragraph

Draft DFARS Clause 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements, para (c)(3), “Report to the Contracting Officer any changes to the list of DoD UIDs 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.”

Recommendation

We are presuming DoD does not want to have the contracting officer buried with all changes to every change, to include those in the contactor’s supply chain, and this is only relevant to SPRS data. If so, we recommend para (c)(3) be changed to “Report to the Contracting Officer any changes to the **information reported in SPRS for the list of** DoD UIDs 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.”

DoD may also want to adjust the language to include reporting to their primes any changes to DoD UID data in SPRS.