KIERI SOLUTIONS LLC
(301) 253-5150 www.kieri.com
Authorized C3PAO

October 12, 2024

Comments on the 48 CFR Parts 204, 212, 217, and 252
"Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)"

Over the last five years, I and my company, Kieri Solutions, have been involved with the CMMC program in the following roles:

- Providing DFARS 252.204-7012 and NIST SP 800-171 consulting to hundreds of defense industrial base contractors
- Becoming one of the first authorized C3PAOs, which included passing a CMMC Level 2 assessment and building an ISO 17020-compliant assessment program
- Performing Joint Surveillance Voluntary Assessments and preparing for the start of formal CMMC assessments
- Teaching over 300 CCP and CCA students about CMMC and how to be an assessor
- Providing free educational content to the masses via CMMCAudit.org and LinkedIn (more than 5,000 subscribers, 30k unique users in the last 12 months)
- Advocating for the CMMC program as well as providing critical feedback to the Cyber-AB and DoD

The work that I and my company perform will affect whether defense contractors are able to obtain contracts according to this 48CFR Proposed Rule. The fate of my company and CMMC are tied together – I want to see this program succeed. My purpose in commenting is to make the CMMC program more functional and to reduce the possibility of misinterpretation or multiple interpretations.

1 ADD CUI IDENTIFICATION INSTRUCTIONS

This rule is the ideal place to add instructions to the Contract Officer to identify sensitive data for each contract using a Contract Data Requirements List (CDRL) or similar instrument.

In my experience, the leading issue that plagues efforts to protect CUI by defense contractors is the identification of CUI related to each contract:

- Contractors and subcontractors receive information that seems to fit into a CUI category, but it was not labeled by the creator. We have many clients with a 99:1 ratio of unlabeled-but-suspect materials versus labeled CUI. Legal counsel has advised that

the responsibility for labeling CUI is held by the creator, therefore, the contractor may treat this unlabeled information as FCI.

- Contractors and subcontractors receive and hold data with legacy labels (ITAR, NOFORN, FOUO, NNPI, Distribution Statements) without guidance for how to update labeling to CUI for this legacy material.
- The CUI category "Controlled Technical Information" (CTI) in particular is extremely difficult to work with, as the regulation defining it is incredibly broad. Contracts including CTI need active involvement by a government authority to identify which types of data are considered CTI.
- Contractors and subcontractors are not provided the government authority details for the types of CUI in their contract. This prevents labeling for contractor-created CUI (which requires identification of the authority and POC). It also prevents contractors from being able to reach an authority for decisions about decontrolling mixed material or controlling newly created material.

Current efforts seem to be focused on proper labeling of CUI during creation by government personnel. Unfortunately, that only addresses a small portion of the issue. Contractors know that they should label CUI if they generate it, but they do not know what is considered CUI for their contract, nor do they know the details required to label it properly. The result is that contractors have a large amount of unlabeled data that they think might be CUI, but they do not treat it as CUI.

Contractors desperately need standardized instructions for each of their contracts which describes what data is considered CUI for the contract. This 48CFR rule is the ideal place to add instructions which require creation and dissemination of a CDRL (or similar instrument) that identifies sensitive information for the contract.

In addition to instructions to the contract officer to create and provide a CDRL (or similar instrument), the 252.204-7021 clause should include a prime contractor flow-down requirement to provide the CDRL to all subcontractors working with FCI or CUI. Prime contractors are notorious for prohibiting communication between their supply chain and government contract officers. Without a flow-down requirement, I do not think that prime contractors will provide this information, which is necessary to protect CUI, to their supply chain.

I am concerned that some CDRLs themselves may be categorized as CUI due to descriptions of sensitive data types within. I do not want to inadvertently create a situation where all subcontractors are forced to receive CUI. In general, limited information such as the names of reports or deliverables should not be considered CUI. But accidental overmarking happens. The DoD could prevent this issue by including instructions that explicitly say that the CDRL should

not include or be considered CUI. Or the instructions could require portion-marking of the CDRL to allow a prime to only provide non-CUI portions to their FCI subcontractors.

2 CLARIFY SELF-ASSESSMENT VERSUS CERTIFICATE

204.7503(i) requires "*A current CMMC certificate or CMMC self-assessment at the level required by the contract…*"
252.204-7021(b)(1)(i) states "*Have a current CMMC certificate or current CMMC self-assessment at the following CMMC level, or higher…"*
217.207 (c)(2)(ii) includes similar "*or*" language between certificate and self-assessment.
252.204-7021(d)(2) includes similar "*or*" language between certificate and self-assessment.

This wording can be interpreted as either certificate or self-assessment are equivalently acceptable, as long as the level is Level 1, Level 2, etc. This language defeats the purpose of CMMC entirely and reverts us to a self-attestation environment.

Possible way to re-word the requirement: Define "CMMC level" by explicitly stating that self-assessment and certification assessment are considered different CMMC Levels and must always be written out in full as follows.

- CMMC Level 1 (Self)
- CMMC Level 2 (Self)
- CMMC Level 2 (C3PAO)
- CMMC Level 3 (DIBCAC)

3 CLARIFY "ALL DATA RELATED TO THE CONTRACT"

252.204-7021(b)(2) states "***Maintain the CMMC level required by this contract*** *for the duration of the contract* ***for all information systems****, used in performance of the contract, that process, store, or transmit Federal contract information (****FCI****)* ***or*** *controlled unclassified information (****CUI****);"*
252.204-7021(b)(3) states "Only process, store, or transmit **data** on information systems that have a CMMC certificate or CMMC self-assessment **at the CMMC level required by the contract**, or higher;"

These statements will be interpreted as requiring prime contractors to keep *all* data related to the contract on information systems that meet the highest level required by the contract. This contradicts earlier descriptions of the CMMC program: i.e., that in a contract with CUI, FCI, and non-FCI data (accounting or publicly releasable data), the contractor is allowed to segregate the data into different systems and different security levels.

I can see security value in the current wording and wonder if it was written purposefully. We have such an issue with identification and mishandling of CUI that forcing primes to perform all contract work in their most secure system is a way of guaranteeing protection of unlabeled and unidentified CUI.

This current wording also prevents the issue where a contractor required to have a CMMC Level 3 certification assessment could decide that some CUI for their contract can be protected at Level 2. I haven't seen anything in the 32CFR rule that specifies *all CUI* for a Level 3 contract must be held in a Level 3 information system, just that at least one information system must be certified at that level.

This current wording allows a disconnect in security between prime contractors and their subcontractors. Subcontractors are allowed to use an appropriate system depending on the type of data (Level 1 for FCI, Level 2 for CUI, but similarly open to interpretation for Level 3).

However, again, this wording is contrary to everything I've heard about the CMMC program, so it probably wasn't meant to be interpreted that way.

Alternative wording could be "will maintain CMMC Level 1 (Self) on all systems that store, process, or transmit FCI for this contract, and will maintain Conditional or Final CMMC Level 2 (Self) / 2 (C3PAO) / 3 (DIBCAC)] on all systems that store, process, or transmit CUI for this contract."

If the DoD decides to implement my first recommendation: to require formal identification of sensitive data for each contract, then a CDRL or similar instrument could be used to specify which data needs to be kept in a Level 2 system versus a Level 3 system.

Note that C3PAOs have been given no instructions to verify the data flows of FCI during CMMC Level 2 assessments, nor have we been given instructions regarding CUI that needs to be protected at Level 3. If the current wording prevails, there will not be any third-party review to confirm that *all data* is kept in the correct system.

4 SUBCONTRACTORS SELF-ATTEST THEIR CERTIFICATION?

The 48CFR proposed rule does not provide any mechanism for a contractor to verify self-assessments or certifications of subcontractors. I expect that higher-level contractors will be forced to accept subcontractor-provided screenshots of Supplier Performance Risk System (SPRS) entries as their only proof of certification.

The CMMC rule estimates C3PAO certification assessments will cost upwards of $100,000. A prime might have 100 subcontractors that need to be certified to work a single contract ($10,000,000). All this to force third-party verification that cybersecurity is being performed, because we have proof that it is *not* performed without third-party verification. Does it make sense to allow self-attestation by all subcontractors at this most critical point?

There needs to be a way for higher-tier contractors to verify their subcontractors without relying on attestation by the subcontractor alone. Here are some recommendations that could work:

- Establish a function within the DoD to forward SPRS statuses upon request by a subcontractor. This can be done via cryptographically signed email to prevent impersonation.
- Update the SPRS system to allow voluntary sharing of subcontractor's records with higher tier contractors. This would ideally be specific to a single DODID (a combination of the information system and timestamp of assessment) to prevent over-sharing.

5 MISTYPE IN SUBCONTRACTS?

252.204-7021(d) states "*Insert the substance of this clause, including this paragraph (d), and exclude paragraphs **(b)(5)** and (c)…"*

Was paragraph (b)(5) the correct target of that exclusion?

6 WHAT CONSTITUTES A SECURITY LAPSE?

252.204-7021(b)(4) requires notification within 72 hours "*when there are any lapses in information security*…"

This language is interpretable to make any issue a mandatory report, no matter how small. A single user failing to complete awareness training on time would be reportable.

The language should be clarified such that only long-term security issues which would cause a contractor to fail their CMMC assessment need to be reported.

I recommend changing the language to clarify that security events which cause or may cause a failure of one or more CMMC requirements for more than 30 days must be reported.

Thank you for the opportunity to give feedback on this 48CFR Proposed Rule.

V. Amira Armond
Certified CMMC Assessor and
Provisional Instructor
MBA, CISSP, CISA
Kieri Solutions