October 14, 2024

Comments regarding Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)

We appreciate the opportunity to provide comment on the proposed rule. Upon review, the Guernsey team would like to provide the following comments/questions.

Confusing Wording Regarding CMMC Level and Applicable Systems

252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements (b)(2) - 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).

It is assumed that the intention here is to ensure that the required CMMC level is maintained for in-scope assets throughout the contract, however the wording seems to indicate that the level required by the contract is required for all systems handling FCI or CUI. The scope of a Level 2 assessment does not include FCI, and many FCI systems are out of scope for that assessment. For a contract that requires Level 2, that scope and the full 110 security requirements should only apply to assets in scope for the assessment.

It is recommended that this section be reworded to required continued compliance with CMMC level required by the contract for assets in scope for the applicable level. It could also specifically state that Level 1 must always be maintained for FCI assets.

Request for Clarification on Data Processing

252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements (b)(3) - 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.

The generic use of the term “data” here seems far too broad. There is likely significant amounts and types of data processed, stored, or transmitted by contractors that has nothing to do with the contract. More specifically, FCI may be processed, stored, or transmitted on systems that are not in scope for a Level 2 assessment.

It is recommended that this section be removed. If the intent is to ensure only systems included in the assessment scope be used to process, store, transmit, or protect CUI, then this should be addressed by requirements to maintain certification level as well as report changes to security posture or scope (see additional comments below).

Overly Generic and Potentially Redundant Reporting Requirement

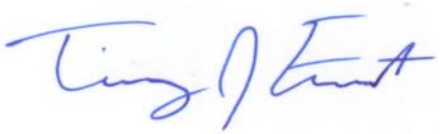
252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements (b)(4) – Notify the Contracting Officer within 72 hours when there are any lapses in

information security or changes in the status of CMMC certificate or CMMC self-assessment levels during performance of the contract.

"Any lapses in information security" is too broad and generic, leading to confusion, potential over reporting. In the case of a security incident potentially involving CUI this will also require reporting duplicating the requirements of 252.204-7012. Additionally, it does not seem reasonable to require the contracting officer, who is assumed to not be a cybersecurity analyst, to handle such reports.

It is recommended that the requirement to report a lapse/change in security be removed. It seems more reasonable to require reporting of a change in CMMC scoping along with the requirement to report a change in certificate or assessment level.

With highest regards,



Timothy Fawcett, CISSP, CCA
Vice President, Director of Cybersecurity Consulting
C.H. Guernsey & Company