Raytheon Technologies
880 Technology Park Drive
Billerica, MA 01821
United States

October 29, 2020

Defense Acquisition Regulations System, Department of Defense (DoD)
Washington, DC 20301-3060

Subject: DFARS Case 2019-D041, *Assessing Contractor Implementation of Cybersecurity Requirements*

Raytheon Technologies (RTX) greatly appreciates DoD's past and continuing collaboration between the Department and broader Defense Industrial Base (DIB) during the development and enhancement of the Cybersecurity Maturity Model Certification (CMMC) framework. We share the Department's goal of safeguarding Covered Defense Information (CDI) throughout the DIB supply chain. Additionally, we support the approach the DoD has taken for Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) assessments, which acknowledges that contractors may have program-specific system security plans that inherit the protection requirements from enterprise system security plans. However, we note that the interim rule as written poses potential implementation and interpretive difficulties, and our recommendations and comments are included below.

I. GENERAL COMMENTS

Duplicate Assessments: In the Preamble to the interim rule, as well as in 204.7302(a)(5) and 204.7501(c), DoD indicates that NIST SP 800-171 DoD Assessments, CMMC assessments, and other DoD assessments "*will not duplicate efforts where assessments are comparable, except in rare circumstances when a re-assessment may be necessary*." However, DoD does not indicate which assessments and levels are comparable. For example, if a contractor achieves a CMMC level of 3 or higher, would the contractor also be required to have a NIST SP 800-171 DoD Assessment, whether at a Basic, Medium, or High level? If so, this would presumably duplicate efforts since DoD has indicated that a CMMC level 3 certificate demonstrates implementation of all NIST SP 800-171 security requirements and more. Relatedly, Section VII.B *"Objectives of, and Legal Basis for, the Rule"* states the following: "This rule establishes a requirement for contractors to have a current NIST SP 800–171 DoD Assessment **and** the appropriate CMMC level certification prior to contract award and during contract performance." This statement, read in conjunction with DoD's statements that assessments will not duplicate efforts, further creates confusion as to the relationship between the CMMC and NIST assessment requirements. In order to avoid duplicate efforts for comparable assessments and provide clarity to contractors, RTX recommends DoD not only specify which assessments and levels are comparable, but also expressly provide for reciprocity between assessments.

Supply Chain: In section C, *"Description of an Estimate of the Number of Small Entities to Which the Rule Will Apply"*, states that the basic assessment requirement is expected to be phased in over a three-year period. This is the only reference to this requirement being phased in and creates significant ambiguity as to how it might be phased in and when individual organizations might be impacted. Additionally, as written, the rule does not detail DoD's phase

Raytheon Technologies
880 Technology Park Drive
Billerica, MA 01821
United States

in plan for DFARS 252.204-7020(g) (2) or 252.204-7021(c)(2). Prior to this rule, subcontractors subject to implementation of NIST SP 800-171 security requirements were not required to undergo DoD assessments, and as a result, it is likely that many of those subcontractors, which comprise a significant portion of the DIB, will not have completed a Basic NIST SP 800-171 DoD assessment or possess a CMMC certificate when the rule becomes effective on November 30, 2020. Without a defined phase in period allotting time for subcontractors to comply with these requirements, once the rule becomes effective, contractors will be challenged to perform new contracts that utilize existing subcontracts, and will also face limitations when entering new subcontracts. Finally, larger contractors may have thousands of subcontractors. A large percentage of them may handle CDI. Thus, the requirement in DFARS 252.204-7020(g)(2) for contractors to ensure subcontractors have at least a basic assessment for all covered contractor information systems relevant to the offer before making an award to a subcontractor is a significant and complex task. This task requires a great deal of "education" and administrative efforts to ensure compliance, even assuming all subcontractors comply with the adequate security requirement of DFARS 252.204-7012. Therefore, RTX recommends clarification as how the Basic Assessments requirements will be phased in and that the DoD create a longer transition period (beyond November 30)—particularly since the 252.204-7019 provision and 252.204-7020 clause have with no CMMC-like limits on the number of solicitations and contracts they appear in, and there is continued uncertainty on whether the requirements of the interim rule will change by before November.

Identification of Covered Defense Information: A key issue that industry continues to struggle with when implementing the DFARS 252.204-7012 rule is the lack of guidance from DoD customers on how precisely to identify "Covered Defense Information" (CDI). This lack of guidance further complicates industry's ability to comply with 252.204-2019 and 252.204-7020, since the scope of the DoD NIST assessments requirement in those clauses is focused on "*covered contractor information systems*" as defined in DFARS 252.204-7012, which in turn hinges on the definition of "*covered defense information."* The definition of "*covered defense information*" in turn references controlled unclassified information that may not be marked or identified by the customer but is *"collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract."* We urge DoD to provide clear guidance to contractors on how to identify CDI and provide clear marking requirements.

Alignment with DFARS 252.204-7012: DoD leaves in place 252.204-7012, which includes among other things a definition for CDI and requirements for external cloud service providers to align with FedRAMP Moderate requirements. At the same time, we understand DoD is moving toward the use of the term "DoD Controlled Unclassified Information" (DoD CUI) and potentially providing some level of reciprocity between the FedRAMP and CMMC frameworks. The move to this new approach without clarifying whether and how it changes the old approach can lead to confusion and wasted resources. In the last several years, the DIB has been encouraged to leverage cloud services to reduce program costs, but the lack of reference to any FedRAMP reciprocity in the CMMC clause leads to confusion. In order to help avoid confusion and wasted resources, RTX recommends quick action to accept the current FedRAMP baselines for CMMC certifications or a decoupling of the requirements to allow FedRAMP to regulate cloud offerings without being assessed for CMMC certification.

Raytheon Technologies
880 Technology Park Drive
Billerica, MA 01821
United States

Furthermore, RTX recommends that DoD provide clarity and guidance on how 252.204-7012 should be read in conjunction with the new provision and clauses.

COTS and Micro-purchase Threshold: The reference to Commercial-off-the-Shelf (COTS) in the new provision and clauses does not tie directly to an official definition. RTX recommends DoD provide the definition for COTS in the rule or in a definitions section. In addition, in the Preamble DoD indicates that it does not intend to apply the 252.204-7019 provision or the 252.204-7020/7021 clauses to acquisitions at or below the micro-purchase threshold. In order to fulfill DoD's intent regarding micro-purchases, RTX recommends DoD revise 204.7304(d) and (e), 204.7503(a) and (b), 252.204-7020(g), and 252.204-7021(c)(2) and instruct contracting officers and contractors that the provision and clauses do not apply to acquisitions that are at or below the micro-purchase threshold. In addition, we suggest citing in the rule the regulatory source that determines the micro-purchase threshold.

II. DFARS 252.204-7019 & 252.204-7020

Overall Efficacy of "Basic Assessments": The "Basic Assessment" Requirement, which requires among other things the input of self-attested summary level scoring in SPRS, adds significant additional administrative burdens even for contractors that have already implemented NIST SP 800-171 or undergone a Medium or High DIBCAC Assessment and creates significant uncertainties—all without a clear explanation of how this will improve a bidder's cybersecurity posture. Notably, the "Basic Assessment" requirement seems to be a different way to ask contractors to "self-attest" to their security, which is a strategy that the DoD has already stated did not work in the DFARS 252.204-7012 context and did not improve the cybersecurity posture of the DIB. Therefore, we respectfully request that DoD reconsider the requirement for contractors to submit "basic" self-assessments, or in the alternative, make the NIST DoD assessment requirement easier to implement as described in these comments.

CAGE Codes: The interim rule requires contractors to list in basic assessments a list of CAGE Code supported by each System Security Plan (SSP). Yet large contractors have hundreds of facility CAGE Codes and many more contracting CAGE Codes. Furthermore, CAGE Codes could have a one-to-many and many-to-one relationship (e.g., one CAGE code could reference multiple dozens of systems, and one system could be related to a large number of CAGE codes). For large contractors, with hundreds of facilities across the US and abroad, use or reliance on CAGE Codes to meet a NIST SP 800-171 DoD assessment requirement for individual information systems can be very confusing from a practical standpoint and concerning from a legal liability standpoint. RTX recommends that the DoD utilizes another type of unique identifier (e.g., DUNS), that will be easier to manage and will align with the DoD's strategic approach to the CMMC and NIST assessments.

Scope of Assessments: The requirement for the NIST SP 800-171 based, DoD directed assessments to cover "each covered contractor information system that is relevant to the offer, contract, task order, or delivery order" leads to major interpretive difficulties particularly for contractors with multiple information systems. Especially for larger contractors, a DIBCAC High or Medium Assessment as well as a Basic Assessment may involve an assessment of a contractor's use of an "inheritance model" by which a large number of program-specific system security plans inherit protection requirements from an enterprise system security plans. It is

Raytheon Technologies
880 Technology Park Drive
Billerica, MA 01821
United States

unclear how the assessment requirement would be met in such scenarios. Therefore, we recommend that DoD indicate how it will allow contractors with such inheritance models to describe their enterprise SSP/inheritance model and provide a score for this inheritance model process. Such guidance would better enable contractors with such inheritance processes to meet the DoD assessment requirement by utilizing their Medium or High DIBCAC assessments, or craft new Basic Assessments, that take into account such processes. Notably, such guidance would also greatly promote the DoD's stated goals in the Preamble to 1) enable strategic assessments at the corporate- or entity-level rather than at the program or contract level, thereby reducing cost to both DoD and industry, and 2) reduce duplicative or repetitive assessments rather than addressing implementation of NIST SP 800-171 on a contract-by-contract approach.

Criteria for Medium and High Assessments: In 252.204-7020(a), DoD sets forth the definitions of Basic, Medium, and High Assessments, which are the levels corresponding to the level of confidence in the assessment. DoD also sets forth in the Preamble the number of Basic, Medium, and High assessments it anticipates will occur over a three (3) year period. However, DoD does not specify the criteria for selecting which contractors will be subject to Medium or High Assessments. RTX recommends that the DoD provide such criteria to allow contractors to assess whether they can reasonably expect to incur associated time and costs.

Source Selection: The use of a single, summary Basic Assessment score, without further context on what led to the score, may easily lead to a false impression of a good or bad cybersecurity posture. This concern is heightened by the possibility that these potentially misleading scores might be used as source selection criteria. We strongly recommend that DoD provide more details on whether and how these summary scores will be interpreted and acted upon by the DoD. In addition, it is possible that poor application of the DoD Assessment Methodology by less proficient industry organizations would lead to inaccurate representations of summary scoring. We recommend that the Department also provide clear liability details or a grace period to help reduce industry fear of legal liability when trying to do their best and meet this new requirement.

Three-year Validity Period: The rule indicates that the validity period for a self-assessment is three years but the -7019 provision and -7020 clause state that the validity period is "…not more than 3 years old ***unless a lesser time is specified in the solicitation***". The two statements are in conflict, the misalignment between the two would introduce uncertainty. We recommend the provisions and the rule include criteria as to when a lesser time might be necessary, as it will drive additional cost and effort.

Non-U.S. Contractors: 252.204-7020(c) requires contractors to provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800-171 DoD Assessment, and 252.204-7020(g)(1) requires contractors to insert the substance of 252.204-7020 in all subcontracts and other contractual instruments excluding those solely for the acquisition of COTS items. We note the particular challenges that will accrue with non-U.S. suppliers that may have local legal (e.g., export control) and security restrictions that would restrict their ability to accept such a flow-down clause and allow U.S. representatives access to their facilities and systems, and expect many non-U.S. suppliers will

Raytheon Technologies
880 Technology Park Drive
Billerica, MA 01821
United States

strongly push back on this requirement for these reasons. RTX recommends that DoD provide guidance on this point.

Email Assessment Reporting: The rule makes note that contractors can send their Basic Assessments to a Navy email address via an encrypted email. However, there is no information in the rule or on the SPRS web site how to obtain the appropriate certificate necessary to send an encrypted email. RTX recommends the DoD provides directions on the process to obtain the appropriate certificates on the SPRS web site or via other mechanism. Additionally, we recommend a standalone email address for submitting assessments for entry into SPRS rather than the general SPRS support email.

III. DFARS 252.204-7021

Level 4 and 5 Alternative: The Interim rule includes a discussion of alternative methods of implementing CMMC Levels 4 and 5 that would require contractors to meet only a portion of the controls required by those levels based on defined thresholds. We urge the DoD to strongly consider these alternative methods. The alternative methods would significantly reduce the cost to implement Level 5 by reducing the number of controls and will align the rest with the company's cybersecurity strategy. In addition, a non-standard implementation of practices across the DIB avoids a single implementation blueprint and supports defense against the Advanced Persistent Threats (APTs). Furthermore, only 18 of 41 practices at Levels 4 and 5 directly mitigate threats identified by DoD Cybersecurity Analysis and Review (DoDCAR). The other 23 practices are administrative in nature, only provide support, or enhance lower level Practices. Overall, implementing the alternative threshold practice model (Flex Option) discussed at Levels 4 and 5 would bring critical thinking and risk management back to the CMMC model, significantly reducing cost and assessment complexity. It also would not require a change to the model or practices themselves, but rather a simpler change in assessment methodology. RTX recommends the (Flex Option) for these levels be reconsidered and a focus be placed on those Practices that more directly mitigate cyber threats.

Plan of Action & Milestone (POA&M): A POA&M is a plan that describes specific measures to be taken to correct deficiencies found during a security assessment. POA&M are a normal occurrence during the lifecycle of an information system and it is unreasonable for the Department to disallow POA&Ms as a part of the CMMC framework. Further, initiatives in the federal government, such as the Open Security Controls Assessment Language (OSCAL), will support improvement in tracking and reporting POA&M status to ensure POA&Ms are closed in appropriate timeframes. We recommend the Department reconsider the use of POA&Ms for the CMMC framework.

Phased Rollout of CMMC: The 204.7503(a) provision indicates that until September 30, 2025, inclusion of a CMMC requirement in a solicitation must be approved by OUSD (A&S). What is not clear is how the contractor will know that a solicitation was approved by OUSD (A&S) if a contractor receives a CMMC requirement prior to September 30, 2025. RTX recommends that DoD identify, by marking or otherwise, solicitations approved to contain a CMMC requirement.

Disputing C3PAO Assessment: In the Preamble, DoD describes the process for disputing the outcome of a C3PAO assessment. First, the contractor requests that the dispute be

Raytheon Technologies
880 Technology Park Drive
Billerica, MA 01821
United States

adjudicated by the CMMC-AB, though it is unclear whether the CMMC-AB is compelled to grant such requests. Second, if the request is granted, the CMMC-AB will provide a preliminary report, and if the contractor does not accept its findings, the contractor may request an additional assessment to be conducted by the CMMC-AB staff. Again, it is unclear whether the CMMC-AB is compelled to grant such a request. Since CMMC certification at the required level is a pre-condition to contract award, DoD should set forth limitations on time for resolution and associated costs. Further, DoD should indicate how it will provide oversight of the process since contractors could disagree with the CMMC-AB's findings. RTX recommends providing clarity on what recourse contractors will have if they disagree with CMMC-AB adjudications of appeals to C3PAO assessments.

Flowdown of Certification Requirements: The rule requires that contractors know which CMMC level is "appropriate for the information being flowed to the subcontractor" and verify that the subcontractor is appropriately certified. RTX recommends that DoD not only specify the CMMC level required for contract award, but also specify the CMMC level required for subcontract award and/or performance. While DoD has indicated that contractors handling CUI will need a Level 3 certification, we note again the continued industry confusion regarding identification of CUI/CDI, and thus recommend that DoD provide clear guidance on certification level requirements for subcontractors.

Continued Proliferation of Requirements by Agencies. Finally, we are greatly concerned that even with the onset of the new -7019 provision and -7020, and -7021 clauses, there may continue to be a proliferation of additional security requirements from various DoD agencies with their own security requirements. Such proliferation would lead to significant inefficiencies and add to the already substantial costs that the new CMMC and DoD NIST Assessments regime will require. We urge DoD to provide guidance to its agencies and services to honor the spirit of this rule, which is partly to provide the means for DoD to improve the cyber posture of contractors in a way that is cost-effective and efficient for both DoD and its contractors, rather than requiring disparate security requirements on an agency-by-agency, contract-by-contract basis.

Thank you for soliciting and considering our comments.

Jeffrey C Brown

Digitally signed by Jeffrey C Brown
Date: 2020.10.29 14:11:29 -04'00'

Jeff Brown
Vice President and Chief Information Security Officer
Raytheon Technologies