HITRUST

6175 Main Street
Suite 420
Frisco, TX 75034

855.HITRUST
(855-448-7878)
www.HITRUSTAlliance.net

November 30, 2020

VIA Regulations.gov

Under Secretary of Defense for Acquisition and Sustainment
United States Department of Defense
3010 Defense Pentagon Room 3E1010
Washington, DC 20301

Chief Information Security Officer
Office of the Under Secretary for Acquisition and Sustainment
United States Department of Defense
3010 Defense Pentagon
Washington, DC 20301

Re: HITRUST Comments on Docket DARS-2020-0034

Dear Under Secretary and Chief Information Security Officer:

HITRUST® applauds the Department of Defense (DoD) for recognizing the need to create an efficient and effective manner to evaluate vendors appropriately and consistently with its interim rule to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification (CMMC) framework.

We write to outline our recommendations for improving the administration of the CMMC Program. Our recommendations are informed by the many partners and organizations that leverage our solutions across several industries with interconnectedness with the DoD. Our primary recommendation is the value of reciprocity for widely adopted market-based certifications. Clear guidance should be given to the CMMC Accreditation Body (CMMC-AB) to further reduce the cost and administrative burden of compliance through leveraging current certification systems. As part of an effort to create efficiencies, it is important to allow organizations to leverage well-established certifications and attestations with an equal level of assurance and scope. Without recognizing this opportunity, the DoD is burdening itself and the defense supply chain ecosystem with additional and unnecessary assessment requirements and costs.

HITRUST was established in 2007 as a not-for-profit standards development and certification organization to champion programs that safeguard sensitive information and manage information risk for organizations across industries and throughout the supply chain.

In collaboration with information security and risk management leaders from the public and private sectors, HITRUST develops, maintains, and provides broad access to its widely adopted common risk and compliance management frameworks as well as detailed assessment and assurance methodologies. HITRUST has been a leader in delivering solutions to address the lack of a common understanding around the security and privacy controls needed to safeguard sensitive information and individual privacy for over a decade. These solutions include: (1) an industry-accepted information security and privacy control framework, the HITRUST CSF®, that incorporates multiple regulatory requirements, best practice

standards, and frameworks; (2) a standard, open, and transparent assurance process to provide accurate, consistent, and repeatable assurances around the level of protection provided by an organization; and (3) a broadly recognized certification of an organization's conformity to the requirements specified in the HITRUST CSF through the HITRUST CSF Assurance Program.

For example, the HITRUST CSF[1] already integrates, maps to, and—with the HITRUST MyCSF® platform—allows organizations to assess themselves against both NIST 800-171 and the several levels of the CMMC framework. Assuming all things being equal, the DoD's acceptance of a suitably scoped HITRUST CSF Certification with the necessary regulatory and other relevant risk factors helps organizations reduce the burden on the ecosystem and still provide the assurances that are required by the DoD.

The Value of Providing Reciprocity

Defense Industrial Base (DIB) members today face new challenges of managing risk, complying with a myriad of information security and privacy regulations, and providing related assurances to internal stakeholders, external partners, and regulators. The DoD has done a tremendous job through the CMMC Model of helping to focus the efforts of DIB members, providing a set standard and a means for organizations to demonstrate that they meet the standard through formal assessment and certification.

While the defense sector is unique in its needs, it also relies on many of the same service providers as other sectors. Take a top-named cloud service provider (CSP), for instance: whether a CSP has a direct contract with the DoD or not, those CSPs are likely to be entities upon whom most, if not all, of the DoD's prime contractors and subcontractors rely and therefore will be in scope/subject to CMMC accreditation requirements and consequently will most certainly seek to leverage their existing investments. These CSPs must comply with a myriad of security requirements and demonstrate a level of compliance to many stakeholders and regulators across every sector. This reality existed prior to the advent of the CMMC Model. The DoD should recognize this and leverage the value that reciprocity with other certifications can add to the DIB and its overall mission.

With all due deference to regulators and policy makers, security, risk management, vendor management, third-party assurance, and compliance are not unique to any organization or industry. The DoD does not and cannot make these decisions in a vacuum even though the regulatory and contracting process implies that it does. These same issues manifest themselves elsewhere and, more importantly, have been solved elsewhere. With all due respect to the architects of the CMMC Program, the DoD owes it to themselves and their community to leverage existing solutions. The DoD should harness the products and solutions that enable it to fully integrate assessment models and standards that allow the DoD the insight to make customized, procurement-specific risk decisions.

Reciprocity with other certifications acknowledges the maturity, investment, and commitment organizations put into achieving those certifications. Every certification program that is scalable, reliable, consistent, accurate, and transparent in determining and communicating the scope of an entity's security posture and maturity should be genuinely considered and leveraged. Streamlining Federal cybersecurity requirements requires looking at systems and approaches other than CMMC that work and harnessing their success for CMMC. Recognizing strong, sufficiently scoped approaches that organizations are already performing frees up time and resources for entities to focus on mission tasks and objectives. This would be true for the CMMC-AB as well as the DIB members who have already achieved certifications with other programs.

[1] https://hitrustalliance.net/product-tool/hitrust-csf/

Specific Recommendations

1. Citing the financial impacts to the DIB, the Department developed a five-year phased rollout strategy to implement the CMMC program requirements. This runs contrary to the justification of the CMMC Model and the more than $1 trillion that malicious cyber activity is estimated to cost the U.S. economy over the next decade. The need for these requirements is now and the Department should strongly consider accelerating the implementation of the program across the entire DIB.

2. The rule does not clarify whether the CMMC-AB is required to conduct any meaningful quality assurance (QA) review of the work of CMMC Third-Party Assessment Organizations (C3PAOs). Further QA requirements should be outlined and clarified for the C3PAOs to meet and the AB to measure their performance. The AB must be required to perform a meaningful QA function in order to meet the DoD's stated objectives. QA is essential to ensuring consistency of experiences for assessed entities as well as guaranteeing that the DoD can rely on the assurances provided to make meaningful decisions, regardless of which C3PAO was engaged.

3. Equal to the quality assurance standards referenced above is the adjudication process of whether a contractor can appeal or challenge the results of a C3PAO's assessment. Without further clarity regarding the standards upon which this could take place, this presents a weakness in the program to ensure the integrity of the assessments. Such appeals are inevitable (especially during the first assessment). Without clear guidance from the DoD regarding the adjudication process, the CMMC-AB will be burdened with a process that it will assuredly find difficult to respectfully address in a timely manner.

Significant Alternatives

The Department asserts that they provided a "[d]escription of any significant alternatives to the rule which accomplish the stated objectives of applicable statutes and which minimize any significant economic impact of the rule on small entities." The Department has fallen short of this regulatory requirement and should describe in detail any significant alternatives to the rule which accomplish the stated objectives of:

> (1) the ability to assess at a corporate level a contractor's implementation of NIST SP 800-171 security requirements, as required by DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting; and
> (2) assurances that a DIB contractor can adequately protect sensitive unclassified information at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain.

The Department has authorized the CMMC-AB to manage and complete these tasks when there are other organizations that are qualified to do so in operation. Without surveying the market to the extent and breadth necessary to evaluate its strengths and capabilities, the rule falls short of the DoD's obligation to ensure that it would adequately meet the needs of the CMMC Program without undue negative impact upon small entities. A proper examination of these requirements is vital for the Department to properly state that they are following the most economic and effective path when it comes to CMMC implementation. The Department should justify why they chose the current implementation path rather than the many viable market alternatives, or possibly manage the program completely within the Department. Merely asserting that the Department considered alternatives falls short of the obligation to justify a program that has this level of economic impact and plays a vital national security role.

HITRUST

6175 Main Street
Suite 420
Frisco, TX 75034

855.HITRUST
(855-448-7878)
www.HITRUSTAlliance.net

Conclusion

The DoD has made great strides with the CMMC Program in a short amount of time. We share the ultimate goal of the CMMC Program to leverage the best approaches and methodologies in the marketplace.

Thank you on behalf of our many partners and organizations for the opportunity to address these concerns directly with the Department. If you have any questions and/or concerns, please do not hesitate to contact me at carl.anderson@hitrustalliance.net or 469.269.1206.

Sincerely,

s/
Carl A. Anderson
Chief Legal Officer and SVP for Government Affairs