Before the
Federal Acquisition Regulation Council
U.S. General Services Administration
Washington, DC

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

85 FR 61505
Docket ID: DARS-2020-0034

COMMENTS OF
INTERNET ASSOCIATION

Internet Association (IA) represents over 40 of the world's leading internet companies and supports policies that promote and enable internet innovation, including commercial cloud solutions. Our companies are global leaders in the drive to develop lower cost, more secure, scalable, elastic, efficient, resilient, and innovative cloud services to customers in both the private and public sectors. IA appreciates the continued engagement with industry and the opportunity to provide input on the changes being made to the Defense Federal Acquisition Regulation Supplement (DFARS) in order to implement the Cybersecurity Maturity Model Certification (CMMC).

IA maintains its strong support for the work being performed by the federal government to strengthen and secure our nation's infrastructure, protecting our most sensitive information and data from theft and espionage. Having developed many of the practices, policies, and procedures that are currently being used by the most secure organizations in the federal government and private sector, IA members have a clear understanding of why this effort is so important.

Our collective experience in securing information and communications technology (ICT) infrastructure around the nation, including for much of the Intelligence Community (IC) and the Defense Industrial Base (DIB), also provides IA members with a unique perspective on how to successfully implement enterprise- as well as industry-wide standards. This is why most of the existing best-in-class certifications and standards are developed and maintained with a heavy emphasis on industry engagement and involvement.

For these reasons, and to ensure the federal government makes use of the existing knowledge and best practices related to securing hardware, software, and managed services supply chains possessed by IA members, we request the reviewers consider the following requests for modification. Working together, we are confident national security interests will take precedence over unnecessary administrative burden and the financial and human resources that will otherwise be required to implement this rule.

There Has Been A Marked Lack Of Industry Engagement In Developing The CMMC. Cybersecurity is a discipline that responds to a constantly evolving environment on a global scale, and as a result, requires a certain degree of centralization of knowledge and standardization of language. This language, expressed primarily through proven and tested security controls, and the way in which it was developed

is what informs - or at least, should inform - the discussions surrounding CMMC today.

This need for a common language of security controls, developed and agreed upon by all stakeholders, is one hallmark of advancing the use of any form of technology to the general public, especially when that technology involves the use or transmission of data. This concept is not unique to cybersecurity. For example, in 2010, Naval Postgraduate School (NPS) Distinguished Professor of Computer Science (CS) Dr. Peter Denning found in his report entitled "Resparking Innovation in Computing Education" that spreading computer science literacy among the general public, not just practitioners, required a standard definition for computing.

Based on a similar concept to what Dr. Denning found in terms of requiring a universally accepted "definition" of the terms and concepts, on February 12, 2014, v1.0 of the NIST Cybersecurity Framework (CSF) was released to serve that role for cybersecurity. Currently on v1.1, released on April 16, 2018, the CSF builds on the collective lessons learned since the advent of storing data on computers. In fact, the legislature itself understood the need for a certain level of standardization. The law that inspired the formalization of the NIST CSF, the Cybersecurity Enhancement Act of 2014 (P.L. 113-274), specifically required that NIST "identify a prioritized, flexible, repeatable, performance based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks."

Because of industry engagement in its development, including extensive participation from IA members, these goals were achieved and the NIST CSF remains the standard and accepted approach adopted by the public and private sector today.

The development of the NIST CSF was not unique, as there has been a long history of this level of public and private collaboration leading to successful efforts in advancing technology. As early as 1959, when Rear Admiral Grace Hopper attended the Conference/Committee on Data Systems Language (CODASYL), the best and the brightest the nation had to offer from both the private and public sector have cooperated on developing these "repeatable" solutions that can be and have been applied across all sectors of the nation's economy. This important historical context demonstrates the long-standing tradition of collaboration by all interested stakeholders, including the DIB and the Government itself, in developing those "prioritized, flexible, repeatable, performance based, and cost-effective" solutions that drive innovation without compromising security.

The way in which the CMMC was developed and is currently being implemented, however, has not followed this established best practice of cooperation and collaboration.

This is true of the rule change itself, which was published as an Interim Rule, depriving the Government of the opportunity to take the time necessary to incorporate valuable feedback into the final text that will ensure this is "done right" rather than "done fast". This is also true of the way in which the existing pilot programs are being run, behind closed doors and with hand-picked participants. In fact, the pilot programs are indicative of the significant missed opportunities that have come from this lack of collaboration with industry. They were not only too few in number, but they also failed to provide substantive updates to the model itself. This lack of development is apparent in the relatively minor changes that took place between v0.6 and v1.0 of the CMMC. In fact, this approach has thus far left the

Government unable to obtain incredibly useful and continuous input from the very organizations in the DIB that will be directly impacted by this rule.

The rule should be changed to mandate communication and engagement between members of the DIB, DoD, the CMMC Accreditation Body (CMMC-AB) or subsequent organization, and other relevant stakeholders, on a regular basis and in a significant manner, especially before making any substantive changes. This will ultimately provide the type of technical and administrative feedback necessary to ensure the important goals of this rule change will be achieved, mitigating the human and financial costs associated with implementation, and ensuring innovative solutions can continue to be provided by new and experienced members of the DIB.

Reciprocity With Existing Standards And Certifications Is Essential To Effective Implementation. Most likely a product of the lack of industry engagement and collaboration, it is telling that the word "reciprocity" or "reciprocal" are not mentioned anywhere in the rule's text. Rather, in justifying the decision to issue an Interim Rule, DoD states that CMMC is a framework being developed as "an important first step" in the general effort to secure the DIB (*see* Determination to Issue a Final Rule).

It is essential to recognize that the CMMC is not the "first step" (*see Id.)* and it does, in fact, "duplicate, overlap [and] conflict" with existing rules (*see* VIII.E.). Even further to the point, the Federal Government has already been working with industry to develop a standard and reusable security certification that indicates an organization's ability to maintain the cybersecurity standards required to safely and securely store federal information - the Federal Risk and Authorization Management Program (FedRAMP). Established in 2011, FedRAMP announced 200 authorized products in September of 2020, representing almost a decade of effort and billions of dollars of private - and public - sector investment in cybersecurity.

FedRAMP is not the only program or standard for which industry and governments have had to spend - and therefore, per advice of the DoD itself, charge the taxpayer by building the expense into their rate - billions of collective dollars, all in the name of compliance.

While others within the DIB have to comply with differing families of standards, IA members are complying with NIST SP 800-53, DoD Cloud Computing Security Requirements Guide (SRG), the Committee on National Security Systems (CNSS) Instruction No. 12533 (CNSSI 12533), ISO/IEC 27000, ISA/IEC-62443, and a variety of the DoD's Security Technical Implementation Guides (STIG). Adding in the 20 new standards that will be introduced when SP 800-172 is finalized and the variety of unique processes being implemented through CMMC without accounting for reciprocity with these previous compliance requirements does not provide DoD with the ability to avoid duplication of "efforts from each assessment, or any other DoD assessment" (*see* Background).

The lack of industry engagement has also impacted the nuances of the rule itself. For example, while existing guidance from DoD, as outlined in DFARS 252.204-7012(b)(2)(ii)(D), provides for a FedRAMP Moderate baseline, there is nothing in the rule that would stop the CMMC-AB or some other subsequent body from raising the Impact Level (IL) requirement to IL4 or IL5 without any technical justification or industry input in doing so. Industry engagement would have provided the drafters with a mutually acceptable process for making such decisions while continuing to achieve the goals of the rule.

One such process would be to make the CMMC framework a NIST SP 800-53 "controls overlay" for Supply Chain Risk Management rather than an entirely new framework. CMMC duplicates security controls already in NIST SP 800-53 Rev. 5 and in the NIST CSF. Since the authors of CMMC mapped the CMMC controls to NIST 800-53, the groundwork has already been laid to simplify this for industry and make this a "controls overlay" rather than an entirely new model, achieving the intended goals of this rule change with minimal disruption.

The benefit from this is clear in that it will allow industry to "build" or "enhance" the existing framework established by 800-53 rather than starting from scratch with unclear requirements. Similar to the Low, Moderate, and High baselines in NIST SP 800-53, CMMC could have control overlays for Levels 1, 3, 4, and 5. For industry, this would greatly simplify security compliance and reporting while directing resources towards the "new" risks related to relevant supply chains. Simply, industry and Government would spend their limited time and dollars towards developing "real security" and not more paperwork.

Formality Of Communications And Oversight Must Be Codified Based On Current Experiences. Operationalizing DIB-wide implementation of CMMC will require a formal and professional organization and approach. To date, the DoD has partnered with the CMMC-AB, a non-profit organization that has been run by volunteers since it first self-formed in January of 2020. In that relatively short period of time, due to a number of issues and concerns with certain actions taken by the CMMC-AB as well as general burnout of the participants resulting from the immense time and energy commitment required, there has been nearly a complete turnover of the organization's Board of Directors as of the submission of these comments.

Not only is the current delegation of authority to this group of private sector individuals unsustainable, it has proven to create an unnecessarily opaque and difficult process for obtaining the necessary information required to make the appropriate information security investments. Much of this is due to the group's own actions, and the lack of any way in which to hold them accountable. In fact, more information has been obtained from social media (e.g., LinkedIn posts from DoD officials and CMMC-AB members, a privately-run Discord server utilized by at least one CMMC-AB Board member to engage with industry, etc.) and a variety of webinars hosted by private sector organizations rather than from the official websites or channels of the DoD.

This is alarming, as the CMMC-AB is the organization that will have the authority to "accredit and oversee multiple [CMMC] third party assessment organizations (C3PAOs) which in turn, will conduct on-site assessments of DoD contractors throughout the multi-tier supply chain" (*see* Scale and Depth).

With the rule change scheduled to be implemented on November 30, 2020, the CMMC-AB is apparently at about 52 approved C3PAOs, with only 12 listed on the CMMC-AB Marketplace before the page was taken down several weeks prior to submission of these comments. With over 200,000 contractors that will be subject to CMMC, with a significant portion of them subject to CMMC Level 3 Certification, there is an immediate need for vetted and verified C3PAOs.

By way of comparison, FedRAMP, which as was previously stated hit 200 certifications in nine years, has a federally-funded program management office (PMO) with 37 3PAOs on their marketplace, of which 22 have done at least 1 assessment. For the CMMC-AB to achieve 200,000+ certifications in less than five years with only a total of 52 assessors expected to be ready by the end of 2020, there is a gargantuan

task ahead of the DoD.

Outsourcing this task to a group of private citizens, all of whom have business interests of their own, operating under a no-cost contract from the DoD, is not only an ineffective approach, but one that could be potentially catastrophic.

In order to ensure the proper administration of a program that requires on-site visits and access to some of the most sensitive information about how a contractor's cybersecurity posture is maintained, the DoD must engage with the DIB in order to establish a PMO within DoD.

This will result in the CMMC-AB becoming a formal and professional body that has an appropriate level of funding and cleared personnel with the requisite oversight, as well as a body that incorporates and iterates on work that has already been performed by the variety of teams involved in developing and verifying compliance with existing standards across the Federal Government.

Harmonization With Existing And Proposed Frameworks Must Be Addressed. Harmonization of the requirements introduced by this rule change with the universe of other relevant standards is essential and necessary for its success. This applies to the numerous existing and proposed frameworks, requirements, and policies that impact information security.

As has already been described, the existing CMMC-AB has been incredibly difficult to obtain public information from, whether in relation to its administration or how it intends to interpret the CMMC itself through the C3PAOs. In the event of a disputed decision by a C3PAO, the CMMC-AB is given the authority to adjudicate the dispute (*see* CMMC Framework). However, what happens if a decision made by this group that is dependent on fees from the C3PAOs themselves makes a decision that does not satisfactorily resolve the dispute? Who has the authority to hear that appeal? The rule change as well as the current no-cost contract are silent on this issue, reasonably resulting in a scenario where this group of non-government employees, who must keep their day jobs in order to survive, will be the gatekeeper of who is and is not permitted to be within the DIB.

An even more likely scenario, considering the different pace at which existing standards are developed and updated, is a conflict between CMMC and a compliance regime that is introduced after CMMC goes into effect. For example, a Board Member of the National Credit Union Administration (NCUA), as recently as their October 15 Board meeting, expressed a desire to obtain supervisory authority over third-party service providers used by credit unions, including cloud service providers (CSPs). These CSPs, who will be required to abide by the regime implemented by the NCUA, will almost certainly be required to abide by CMMC as well as FedRAMP and SRG. If there is a difference in how a particular control is supposed to be implemented in SP 800-171 as interpreted by CMMC, SP 800-53 as interpreted by FedRAMP and SRG, and whatever standard as interpreted by NCUA, which regime should the contractor comply with? Who has the authority to make the final decision that could result in an innovative solution being unavailable to the DoD? The rule change is silent on this issue, again, reasonably resulting in a scenario where the CMMC-AB will be the gatekeeper of who is and isn't permitted to be within the DIB.

Even in terms of administrative issues, this lack of harmonization among the variety of cybersecurity requirements can cause very real and very expensive issues. For example, FedRAMP is currently working

with NIST to develop and implement the Open Security Controls Assessment Language (OSCAL) in order to automate their process. If the CMMC-AB and their C3PAOs are for some reason unable to support OSCAL, will a contractor be able to use the output of their work in OSCAL to obtain reciprocity for the equivalent controls or will the CMMC-AB and the C3PAOs require the contractor spend the money and time necessary to perform the same work manually? Once again, the rule change is silent on this issue.

Through industry engagement as well as by establishing reciprocity with widely-adopted existing standards, such as FedRAMP or the NIST CSF, many of these questions would be answered - and they would be based on widely-accepted standards with existing methods for review in the event of conflict.

There are a number of options available to the Government in terms of using an internal body, staffed by cleared Federal employees and contractors that will be able to perform this work. They can address these questions and others, and do so using authoritative bodies and information that exists today. The DoD should use one of these options - and can do so relatively easily after engaging with industry to determine which would be the most effective and efficient for all impacted by this rule change.

In Conclusion: Implementation Of CMMC Should Be Scaled Appropriately, Over Time, Ensuring The Final Model Is Representative Of Real-World Threats And The Practices Required To Mitigate Them. Our members' livelihoods depend on being secure - but they also depend on being compliant. As is widely understood by now, cybersecurity is an ever-evolving space and private sector best practices have to immediately adapt to new and real threats. It is worth repeating: most of the existing best-in-class certifications and standards are developed with a heavy emphasis on industry engagement and involvement.

The CMMC, unfortunately, has not followed this tried-and-tested method for developing a standard. Doing something fast does not equate to doing something right, and in the situation we find ourselves in today, we cannot afford to fail. Staying on the course this rule change has been on would exacerbate the problems it is attempting to address.

It is not too late to change course, however. The DoD can benefit from its own previous experiences as well as those of others in this space. With relatively minor changes and a certain degree of serious industry engagement, the implementation of CMMC can be put in the hands of a formal and professional body that recognizes the immense amount of work that has already been undertaken, allowing it to build from that position of collective strength. This approach will ensure the entire DIB, not just those involved in developing compliance regimes, use the very same methodologies that have resulted in the existing cybersecurity frameworks and policies that have been proven to work with known and emerging threats.

IA appreciates this opportunity to provide feedback on DFARS Case 2019-D041. We look forward to continuing to work with DoD staff to implement this rule such that the intended objectives are achieved.