9/21/24

From: Vincent Scott, CEO, Defense Cybersecurity Group, Inc.
To: Ms. Heather Kitchens, OSD DFARS
Ms. Leslie Beavers, DoD CIO
Ms. Stacy Bostjinak, DoD CMMC Program Office
Subj: Comments on the DFARS Case 2019-DO41 Assessing Contractor Implementation of Cybersecurity Requirements

1. Introduction

The following comments are submitted for your consideration. These reflect my active participation in the DoD Cyber Community in four ways.

First, as an implementer. I am the Chief Security Officer responsible for Cybersecurity; FSO; Internal Audit; and Governance, Risk, and Compliance (GRC) for a small/medium-sized defense contractor. I am responsible for implementing CMMC throughout this organization and directly interact with the challenge of making regulation a daily reality. I will likely be a future Senior Official.

Second, as a consultant. My company, Defense Cybersecurity Group (DCG), consults with a broad spectrum of clients. Our largest is a major research University. Our smallest is a 1-3 person micro company. We also have a range of clients in between, providing insights for organizations across the spectrums of size and type.

Third, I am one of 105 current, completely qualified CMMC Assessors. I have participated in multiple mock assessments and one Joint Surveillance Voluntary Assessment; when Lead Assessor qualifications are implemented, I will be one of less than 100 people who meet these qualifications.

Finally, as an instructor. I teach both CMMC Certified Professional and CMMC Certified Assessor courses.

I play actively in all four phases of the game today: implementing (as a responsible Senior Official), consulting, assessing, and teaching. This has resulted in excellent “in-the-trenches” experience with the impact of these regulations.

I am also a retired Naval Officer with a number of deployments to ground and at-sea combat operations. Please do not presume that these comments stem simply from a desire to limit costs or a lack of understanding of the requirements for our men and women on the pointy end. The professional cybersecurity/CMMC community members, many of whom share those experiences, are every bit as motivated for the defense of our nation as anyone.

2. Executive Summary

In order of importance, we recommend particular scrutiny on the following comments.

- As worded, this seems to eliminate the use of CUI enclaves and mandates that if a Level 2 environment is required then all *FCI and CUI* must be inside the L2 assessment/certification boundary. We recommend this be changed to align with the understanding up until this point that CUI enclaves are a valid approach: **Comment #9**

- We recommend the addition of a definition for "change in compliance status:" **Comment #8**

- We highly recommend eliminating the requirement for swearing to *continuous compliance into an unknowable future*. As stated in the 32CFR170 proposed rule comments, this potentially boxes every Senior Official into an unavoidable position of swearing to something that cannot be true, and making that individual potentially liable for personal, federal fraud charges. As worded, this language sets Senior Officials up to attest not only to the perfection of their information security at the time of assessment but to *swear that controls will not fail in the future*. This failure is virtually guaranteed to occur, especially when faced with maintaining 100% fidelity to a highly detailed control set across several years. This in our view creates a no-win situation for all defense contractors. We recommend the removal of the word "continuous" throughout: **Comment #11**

- As worded, this document fails to *require* certification assessments in any circumstance other than Level 3. We assert that the current language, when examined through the lens of symbolic logic, leaves it up to OSCs/OSAs whether to self-assess or seek a certification assessment. We understand this is not the DoD's intent and recommend modifications to close this gap so that, at Level 2, it is the responsibility of the *contracting officer* to specify whether a self or certification assessment is required: **Comment #13**

Comment #1

https://www.federalregister.gov/d/2024-18110/p-135

> "Since DoD does not track awards that may include FCI or CUI, DoD assumes the number of impacted awardees in Year 4 and beyond will be the average number of entities in the Electronic Data Access (EDA) system from fiscal year (FY) 2021 through FY 2023 with awards containing the clause at DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, or 29,543 entities, of which 20,395 (69 percent) are small businesses."

This assumption is incorrect as the clause applies to FCI *or* CUI. FCI is defined and applied to essentially all contracts under FAR Clause 52.204-21 Basic Safeguarding of Covered Contractor Information Systems. Further 4.1903 Contract clause states, "The contracting officer shall insert the clause at 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, in solicitations and contracts when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system." Therefore the inclusion of this clause in contracts should also be used to reflect the applicability of CMMC. Our understanding is that this clause is applied in every or nearly every contract.

Comment #2

https://www.federalregister.gov/d/2024-18110/p-140

> "For each of the information systems that will process, store, or transmit FCI or CUI, DoD assumes it will take offerors and contractors—
>
> - An estimated 5 minutes to post the results of the CMMC self-assessments in SPRS;
> - An estimated 5 minutes to complete the required affirmation in SPRS; and
> - An estimated 5 minutes to retrieve DoD UIDs in SPRS for the information systems that will be used in performance of the contract and to submit the DoD UIDs to the Government."

These assumptions are flawed and leave the vast majority of associated new work under this clause and impact unaccounted for. Posting the results of a CMMC self-assessment is only a tiny portion of the new requirements. Conducting a ***CMMC*** self-assessment is a new requirement and different from the previously existing SPRS self-assessment requirements as outlined in the new regulations. Currently, self-assessments are conducted as directed in DFARS 7019/7020 using the DoD Assessment Methodology (DoDAM). Under CMMC, CMMC self-assessments will be conducted using the new CMMC Scoping Guides, Assessment Guides, and the CMMC Assessment Process. These directives for how to conduct an assessment already run to nearly 1,000 pages and are substantively different than the DoDAM. You certainly cannot even read the rules under which you are supposed to conduct a self-assessment in 5 minutes.

Recommend revision of this section to reflect more realistic impact estimates. Start with the estimated time to read the new regulations both 32CFR170 and 48CFR and their associated mandatory documents under the CMMC process. This clause, not 32CFR170, adds the requirements for contractors to read and follow CMMC requirements. Some potential input in this estimate:

- Read the regulation. 879 pages counting the associated CMMC documentation. 1 Minute per page = 14.65 Hours.

Document	#Pages
32CFR170	254
DFARS Case 2019-D041	57
CMMC L1 Scoping Guide	7
CMMC L2 Scoping Guide	14
CMMC L1 Assessment Guide	52
CMMC L2 Assessment Guide	275
CMMC Assessment Process	47
CMMC Glossary	40
CMMC Model Overview	52

DoD Cyber FAQ incorporated by reference	81
Total	879

- Conduct of the CMMC Self Assessment in accordance with that required guidance. This is similar but not identical to existing DoDAM based assessments with additional scope and security protection requirements. CMMC is not simply assessing existing 171 as written. Estimate that in general, a CMMC self-assessment with evidence gathering at Level 2 takes 10 days with 4 people. 320 hours. Provide for 80% overlap with the DoDAM assessment and include an extra 64 hours to conduct the assessment.
- Conduct Scoping. Scoping under CMMC is an entirely new requirement as guided by the new CMMC scoping Guide. Although some of the specifics for this are covered in the new 32CFR170 proposed rule, this is the first time these requirements are mandated in contracts and therefore those expenses should be estimated here, including the time required to conduct the new work. New work under CMMC includes:
    - Conducting written scoping activities for the flow of CUI in the network and the documentation of all assets (as assets are defined in a broad and new way with a new specific to CMMC definition); estimate 100 hrs of qualified professional CMMC and business operations time.
    - Categorize all assets in accordance with CMMC scoping categories; varies by size of the organization but estimate 80 hours of IT professional time.
    - Gather evidence for CMMC assessments; estimate 160 hours of IT and compliance personnel time.

This leaves off the table technical changes, systems modifications, programmatic changes, and other activities needed to accommodate the greatly expanded scope of CMMC particularly for Security Protection Assets and External Service Providers.

_____

Comment #3

https://www.federalregister.gov/d/2024-18110/p-147

The proposed rule solicits input on the proposed costs of this table. This analysis is supported by the Regulatory Impact Analysis provided as a separate document here: https://www.regulations.gov/document/DARS-2020-0034-0195

We submit that this very very significantly underestimates the costs of this regulation. An alternative approach for costs to industry might be to assume that each company requiring a CMMC Level 2 certification will spend $100,000 in preparation for the assessment. This assumption is low but leading experts in the assessment field routinely state publicly that “CMMC is a six figure problem.” Using one of my companies as an example (a small-medium DIB contractor) we have spent approximately $700,000 in the last four years on CMMC program development and preparation. This is primarily concerned with

documentation and assessment requirements but also drives implementation and maintenance activities for the overall cybersecurity program including the security requirements of NIST SP 800-171. $100,000 in labor hours represents the subset of those hours spent strictly on assessment preparation. In addition to this estimate add $50,000 for hiring a C3PAO and conducting the assessment. Current cost models for CMMC assessment run between $25,000 and $75,000. This is driven by the qualifications of the individuals required to conduct the assessment in 32CFR170, and the labor hours of those highly skilled people to conduct the assessments in the manner directed by the DoD. Higher costs will be incurred for larger organizations with more locations. Again these numbers likely underestimate the total financial impact. These impacts are the direct result of the inclusion for a requirement to gain a CMMC certification as outlined in this regulation, not 32CFR170 which provides guidance on how these activities are to be conducted but does not mandate that activity for the DIB. The mandate is contained in this 48CFR case.

We will provide feedback on the total number of entities estimated in this proposed regulation to need a CMMC certification separately and instead use the very different numbers developed and published in the 32CF170 regulation, which although also likely low, will serve. Table 6 of 32CFR170 estimates that the total number of entities requiring a Level 2 certification will be 76,598. Focusing on the Level 2 certifications as by far the largest impact area, using the estimates outlined above, we conclude

Preparation	Assessment	#Entities	Total
$100,000.00	$50,000.00	76,598	$11,489,700,000.00

This represents assessment preparation and execution which will be repeated triannually. Spread over a 10 year period assuming that all entities are re-certified 3 times we conclude that the 10-year cost to industry will be **$34,469,100,000.00**. Over time these costs will be reflected in increased cost to the DoD in contract execution. Again we see this estimate as *conservative.*

We are in favor of an assessment regimen. It is required to move companies to better cybersecurity and better protection of DoD information. We must not delude ourselves that the cost of this regulation is 15 minutes. That serves neither the DoD nor the Defense Industrial Base (DIB) well.

_____

Comment #4

https://www.federalregister.gov/d/2024-18110/p-153

> "The rollout is intended to minimize both the financial impacts to the industrial base, especially small entities, and disruption to the existing DoD supply chain."

The phased rollout ultimately does not reduce or mitigate the financial burden on small entities. It does reduce the risk of supply chain disruption. Recommend removing the statement on reducing financial impacts.

Comment #5

https://www.federalregister.gov/d/2024-18110/p-156

CMMC Level	Percentages	Small entities	Large entities	Total entities
Level 1 Self-assessment	63	12,849	5,763	18,612
Level 2 Self-assessment	2	408	183	591
Level 2 Certificate	35	7,138	3,202	10,340
Total Entities	100	20,395	9,148	29,543

The estimates stated here differ significantly from the estimates supplied in 32CFR170 no doubt because different methodologies were utilized in developing them. We recommend that the DoD, with two rules published nearly simultaneously synchronize the estimations for the exact same impact; primarily the number of companies that will require a CMMC level 2 certification assessment. The use of the Electronic Data Access system based data underestimates the number of entities that will require a certification. Since this regulation covers both Level 1 entities for self-certification for Federal Contract Information (which should include all DoD Contractors with rare exceptions) this should reflect the entirety of the DIB. Most significantly this does not account for subcontractors as the government only has visibility on prime contractors. In 2022 five contractors digested 1/3 of the DoD Budget (See CRS report The US Defense Industrial Base: Background and Issues for Congress https://crsreports.congress.gov/product/pdf/R/R47751). These large prime contractors then in turn support thousands of subcontractors.

Additionally, this fails to account for the fact that CMMC has expanded the scope of certification beyond DoD contractors and subcontractors. The new regulation **now requires, as new and expanded requirements** the CMMC certification of External Service Providers (ESP). The majority of the DIB are small entities and these entities depend extensively on ESPs for their IT support. An estimate of the number of ESPs that require certification should also be included in the size estimate and added to the estimate from the 32CFR170 which also did not include this impact.

Using the DoD Small Business Strategy referenced below we could state that roughly 75% of the DIB is made up of small and medium sized businesses. In 2020 the DoD stated in the Federal Register for the publication of DFARS 7019/7020/7021 that:

> Based on information from the Federal Procurement Data System (FPDS), the number of unique prime contractors is 212,657 and the number of known unique subcontractors is 8,309. RIN 0750-AK81.

Taking the total of 220,966, and realizing that the number of unique subcontractors is massively under estimated, we can calculate that approximately 165,725 SMB's are in the DIB. Let us further estimate

that on average one MSP services 25 DIB contractors, and that 80% of SMB's utilize an MSP or MSSP in as part of their IT enterprise. We submit that both assumptions are conservative. This in turn estimates then that: (165725-SMBS*.8)/25=5303 additional MSPs that will also require CMMC self assessment/certification.

_____

Comment #6

https://www.federalregister.gov/d/2024-18110/p-161

> "DoD invites comments from small business concerns and other interested parties on the expected impact of this proposed rule on small entities."

The DoD has from the earliest days of this regulation taken the position that CUI requires the same level of protection wherever it travels. In fact in the comment response from the earliest versions of 7012, the DoD cast derision on the very concept that CUI might require different protections based on the size and capabilities of the contractor instead opting for a one-size-fits-all approach. One standard for a contractor based cybersecurity system regardless of the size or capabilities because the sensitivity of CUI did not change. The amount of risk to the DoD does change, however. A breach of Mom and Pop's machine shop is much less likely to have a significant impact than a breach of one of the major defense suppliers.

The DoD is requiring the same security system for Mom and Pop's Machine Shop as you are on the mega-corporation contractors. So, Mom and Pop's machine shop needs the same cybersecurity as Raytheon or LMCO? An interesting view asserted by an agency that spends billions on Cybersecurity and adheres to its own standards and controls at a lower rate than they will now be demanding of the DIB as reported by the GAO. If with billions in budget dollars for cybersecurity the DoD is only 70-79% implementing the CMMC controls, then what is the burden on Mom and Pop's Machine Shop? That this regulation will require 100% perfect implementation perpetually with no deviations? A standard with which no DoD system has ever accomplished? We invite the DoD authors of this regulation to find a single DoD system under ATO anywhere in the department that has been implemented with zero POAMs in effect and has maintained that status over the lifecycle of its operation. Our conversation with numerous professionals in the space working on Federal ATOs consistently report that they have never *seen* an ATO without a POAM. Add into this, as required under CMMC, an ATO with no POAMs, no waivers of requirements, no tailored out requirements, and zero Not Applicable requirements which is effectively the standard required in CMMC. The DoD has set a higher standard for the DIB than it has set for itself, and the cost/impact on small businesses will be enormous.

See Comment #12 for additional input on the impact on small businesses.

_____

Comment #7

https://www.federalregister.gov/d/2024-18110/p-164

> "Public reporting burden for this collection of information is estimated to average 5 minutes (0.8333) per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information."

The picayune nature of this estimate is breathtaking. As outlined in our recommended estimations in comment #2 and comment #3 we indicate much better the potential public reporting burden. As stated in comment #2, since this explicitly includes the "time reviewing instructions" we respectfully submit that no living human can review 889 pages of instructions contained in the extended CMMC documentation, which is required to comply with this regulation by reference and is uniquely required of contractors through this contracting clause, in some subset of 5 minutes. Each response will require at a minimum:

- Reviewing Instructions. At a minimum, this will entail at least 14.65 hours at one minute per page. This of course greatly underestimates the time required to study and understand these regulations and their implications. Some professionals in the space have spent years studying these documents. My reading and study for understanding and implications for what must be done for this 57-page regulation alone exceeds 40 hours. Recommend an estimate of 80 hours for reviewing instructions.
- Searching existing data sources. DCG has experienced, on numerous occasions, the evaluation of 110 controls and 320 assessment objectives. We are doing this in some form every week. With the gathering of evidence to support the evaluation of those controls the full run-through of 110/320 normally takes a full-time effort of two weeks with 2 evaluators and at least 2 supporting members from the evaluated organization. This is normally spread out over a longer period for self-assessments, generally 6 weeks. Estimate 80 hours each for four qualified personnel resulting in an estimated overall effort of 320 hours. This is not an overestimate. Our team has come to refer to this as "the grind," because of its nature and that there is just no circumventing the process.
- Gathering and maintaining the data needed. Gathering the data was laregley covered in the above estimate of searching existing data sources, the maintaining of a current body of evidence requires further ongoing work. Estimate 1 hour per week annually for a single person; 52 hours annually.
- Completing and reviewing the collection of information. Estimate one hour quarterly for supervisory personnel; 4 hours.
- Submitting the results of this effort to the DoD in the form of an annual self-affirmation will require 8 hours of initial work gaining access to the required DoD system initially (determining how to submit for the needed accounts, submitting for those accounts, follow-up to ensure the creation and activation of those accounts) and then submitting the approved affirmation annually; 2 hours including time for the senior official to review and approve results; 10 hours

- Total for all points: estimated **466** hours.

_____

Comment #8
https://www.federalregister.gov/d/2024-18110/p-179

Definition of "Current" and definition of "Change."

Current is defined as:

> "(1) Not older than 1 year for Level 1 self-assessments, with no changes in CMMC compliance since the date of the assessment;
> (2) Not older than 3 years for Level 2 certificates and self-assessments, with no changes in CMMC compliance since the date of the assessment;
> (3) Not older than 3 years for Level 3 certificates, with no changes in CMMC compliance since the date of the assessment; and
> (4) Not older than 1 year for affirmations of continuous compliance with the security requirements identified at 32 CFR part 170, with no changes in CMMC compliance since the date of the affirmation."

Change is not explicitly defined.

This definition of current is in this case attached to the 204.7501 clause but is used consistently throughout. We submit that the concept of "no changes" in the definition of "current" over any period greater than a single day is not aligned with the reality of IT system operation in the DoD's own systems nor those inside the DIB. This concept of "no changes" is also carried through the current 32CFR170 and our comments are similarly reflected in our input on that regulation. To recap however and to again reinforce the enormous disconnect between DoD regulatory thinking and the reality of IT system operations…

The DoD regulatory authors should study the requirements of IT system operation to include the very real concept that absolutely zero IT systems, anywhere are static. The concept shared in 32CFR170 that affirmations may be updated, "with no changes in CMMC compliance since the date of the assessment" may as well include, "as long as the OSC observes at least one living Unicorn." The IT system that went utterly unchanging for a year is a fantasy creature that does not exist. The pursuit of this fantasy creature should be dropped from the entirety of the regulation.

This reality in turn will mean that some attempt must be made to set a level of change that triggers a reaffirmation, and a level of change that triggers a reassessment, possibly a thorny challenge that the regulation authors seek to avoid. As currently worded (and further feedback and recommended changes will be outlined under a separate comment for that section of 7021) only a re-affirmation is triggered under a "changes of compliance status." The principle question then is what is a change of compliance status exactly?

In some ways, I am trepidatious about requesting clarification on this point. In the past clarifications have in general moved the bar towards "even less doable" than the ambiguous predecessor. The argument has been made to leave it ambiguous and then define it as industry sees fit. That leaves a

great deal of risk on the table for future FCA allegations however, even with the repudiation of the Chevron doctrine.

We recommend the addition of a "change in compliance status" definition as follows:

> Change in Compliance Status - Minor changes and updates to covered systems are a normal part of IT operations and anticipated under the security requirements of NIST SP 800-171. Changes of compliance status consist of revocation of certification status by the accrediting body, certificate expiration without renewal, significant expansion of the system boundary such as part of the merger and acquisition of formerly separate business entities where their IT system is incorporated into the system boundary, changes to system protection capabilities that significantly degrade system security, and OSA Basic Assessments conducted under DFARS 252.204-7020 that results in an SPRS score of lower than 88.

Consider this proposed definition in the light of the following real-world case study.

I serve as the Chief Security Officer for a small DIB contractor of less than <$50M in revenue and <500 employees. Small per SBA definitions but not micro. We have been running a fully funded 171 compliance program for over 5 years. This includes meeting the required continuous monitoring for that time frame and includes actively worked hours on CMMC/171 compliance every week. We have a compliance program the envy of many companies 10x our size.

Every year for the last 5 years we have run our own Mock Assessment as a part of our self-mandated annual Basic Assessment process i.e. these assessments follow the CMMC Assessment Process as closely as possible while also meeting the requirements of the DoD Assessment Methodology mandated in DFARS 7019/7020. Although the current regulation does not mandate an annual self-assessment we see an annual self-assessment/mock-assessment as a good way to meet the 171 requirement for periodic review of control effectiveness where CMMC has defined periodic as not longer than annually.

We do so with the intent to "be as hard as possible" and exacting in terms of regulatory compliance perceiving the DoD's compliance regimen to be enormous, complex, and utterly unforgiving. For two of the five years we have engaged an outside assessment organization to conduct the assessment. Every year we score ourselves less than 110. Every year for different reasons and interpretations. In some cases, that has been chasing the evolving interpretations and updates to CMMC. In other cases, it was just pointed out that in the view of the assessor, our approach was not adequate or sufficient for a specific assessment objective in some ways. Our scores have been somewhat oddly consistent 91 or 92 every year based on completely different controls and AOs. Realize that based on the scoring system this still means 98% of the assessment objectives were assessed as Met. Missing a portion of one assessment objective, as the evaluation is currently constructed, results in losing all points for the entire control. For example in this year's Mock Assessment, we received a Not Met, for AT.L2-3.2.2 *Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities*. This is a 5-point control. The assessor determined that one of the cybersecurity personnel was insufficiently knowledgeable on what constituted "Lawful Government Purpose" for CUI handling and therefore assessed 3.2.2. as Not Met. The other aspects of this control such as having an identified list of specific training for all IT and cybersecurity personnel, listing and completing certification

requirements, and documented evidence that the training is complete as a part of an established evidence locker were all met. Yet we lost 5 points for a small portion of the overall requirement. This also would have constituted an autofail for a CMMC certification purposes as directed in 32CFR170. This serves as a great example supporting our previous statements about CMMC becoming a brutally high and unforgiving standard. One example of an assessor seeing it differently can result in a destroyed business. That is all it takes as written. Further, this could effectively make a CISO or CEO liable to personal criminal fraud charges having sworn unending perfect compliance into the future. See Comment #11 for further on this.

Every year we undertake to correct any identified deficiencies within 90 days and normally complete those in much less time than that.

In our view this is a good process of review and correction, and how the 171 security requirements in general are designed to work. This is *extremely* consistent with the security requirements as laid out in 171. This is exactly the kind of process they were envisioning. NIST was not, rightly, envisioning any system to maintain unending perfection in controls implementation.

Once the identified weaknesses are corrected, we then report our updated SPRS score of 110 as a point in time. This is the type of program that the DoD wants to encourage, not burden those programs doing it right with every change or weakness identified triggering mandatory reporting to the contracting officer. The DoD's continued pursuit of ever more assurance and ever more perfection in execution is far beyond counterproductive at this point.

We submit that the definition above would meet the DoD's intent of being informed when they need to be, without burdening the contracting officer and the OSA with counterproductive reporting for what is a "moderate" and reasonable security program. As written the regulation could be read to mean that any change to the system triggers a reporting requirement. Putting the contracting officer on as an info addee for every system update, every patch, and every modification would provide an undue burden on the OSC/OSA, and be utterly useless to the DoD. Although all reasonable security personnel would see the "any change" standard as ridiculous and clearly not the intent, the Department of Justice in pursuing an FCA claim might not, and likely would not (we have some information on this in practice as well). The DOJ reads these regulations quite literally and at times with little understanding of IT operations, take the same view thus resulting in extreme and unwarranted legal and compliance risk for the OSC/OSA.

_____

Comment #9

https://www.federalregister.gov/d/2024-18110/p-185

> "(a) The CMMC certificate or CMMC self-assessment level specified in the contract is required for all information systems, used in the performance of the contract, that will process, store, or transmit Federal contract information (FCI) or controlled unclassified information (CUI)."

And from the 204.7503 section

https://www.federalregister.gov/d/2024-18110/p-190

> "(i) The results of a current CMMC certificate or current CMMC self-assessment at the level required by the solicitation, or higher, for each DoD unique identifier (DoD UID) applicable to each of the contractor information systems that will process, store, or transmit FCI or CUI and that will be used in performance of the contract posted in the Supplier Performance Risk System (SPRS) (see 32 CFR 170.15 through 170.18); and"

This could be interpreted to mean that if a CMMC L2 is specified in a contract that all FCI information would be required to operate at Level 2, which is not a requirement for that information type as outlined in FAR and DFARS. We believe it is the DoD's intent to allow for multiple systems per contract, as they have estimated an average of 5 systems in this proposed regulation, and some of those systems might be FCI, ie Level 1 specific. We recommend this language be adapted as follows:

> (a) The CMMC certificate or CMMC self-assessment level specified in the contract for specific is required for all information systems, used in the performance of the contract, that will process, store, or controlled unclassified information (CUI). Information systems processing Federal Contract Information (FCI) and not CUI require a CMMC Level 1 self-assessment.

and for the second

> (i) The results of a current CMMC certificate or current CMMC self-assessment at the level required by the solicitation, or higher, for each DoD unique identifier (DoD UID) applicable to each of the contractor information systems that will process, store, or transmit CUI and that will be used in performance of the contract posted in the Supplier Performance Risk System (SPRS) (see 32 CFR 170.15 through 170.18). Systems processing FCI and not CUI require a CMMC Level 1 self-assessment.

This would result in the ability of a contractor that only does some DoD work to continue to use its existing and compliant business systems for the processing of FCI and build an enclave at the higher security requirement level for CUI. This is, we believe, both an important option to control cost and one that has been under construction broadly in the DIB based on existing guidance.

If the intent was to require all FCI handling to occur within the CUI-certified boundary, then this is largely unexecutable across the DIB and represents another significant expansion of requirements. This is not, "We are crying it will cost too much," but cannot be done for any price. Why. Because business systems are largely cloud-based. Not FedRAMP cloud-based. We can keep the CUI out of them, but designating some FCI, and requiring it arbitrary and unmarked use be restricted is just not executable for any amount of money across much of the DIB. I know. I have been working with a broad range of companies on their systems and operations. The DIB needs these companies and many of them are NOT DoD solely focused. Requiring them to break their business processes for a subset of information that is unmarked and even more mysterious than CUI will not work. We need the enclave concept for CUI to be intact. It is literally the only possible path forward for many of your critical manufacturers. As I elaborate on later,

this is another expansion of the requirements, subtly laced into the regulation if the intent is as written. And counterproductive.

_____

Comment #10

https://www.federalregister.gov/d/2024-18110/p-187

> "for example, when there are indications of issues with cybersecurity and/or compliance with CMMC requirements."

This provision is extremely broad and potentially touches on the pursuit of unicorns as outlined in Comment #8. In my experience, there is not a single day that passes without some issue with cybersecurity or CMMC compliance. This is the reality of cybersecurity operations. Cybersecurity is something we do on a daily and continuing basis. Likewise, CMMC compliance is a constant effort. In real systems, compliance is in the process of continuously degrading. I liken this to being inside a house where the roof is constantly collapsing. Security and Compliance is constantly making the rounds and shoring up the falling ceiling. Stop working and very quickly the roof is no longer keeping out the rain. This is exactly why the NIST SP 800-171 control 3.12.3 "Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls." This constant work is required as security controls constantly degrade over time. Recommend striking this phrase from the regulation entirely. There are existing reporting requirements for incidents under DFARS 7012.

_____

Comment #11

https://www.federalregister.gov/d/2024-18110/p-191

> (ii) A current affirmation of continuous compliance with the security requirements identified at 32 CFR part 170 in SPRS for each DoD UID applicable to each of the contractor information systems that will process, store, or transmit FCI or CUI and that will be used in performance of the contract.

As previously submitted under 32CFR170 the affirmation of *continuous* compliance, where compliance is defined as complete and perfect implementation of all 110 Controls/320 Assessment Objectives over time and indefinitely into the future, is in reality not possible. An affirmation is the equivalent of a legal oath and this regulation directs that contractor senior officials swear that they will always be compliant *into the future* under the threat of federal criminal fraud charges should they fail. Absolutely everyone will fail. It is not possible in any functioning and adapting IT system to maintain unending perfect compliance with the NIST 800-171 standard. The change is too frequent. Things change. Systems break. People do things. Would any authorizing official swear an oath that the system as ATO'd will remain in unending compliance into the future? Under threat of federal criminal charges for failure? When the actions of any number of other people might cause a weakness or break in one of the controls? Certainly not and they would know with any experience at all that things constantly fall out of compliance and need correction.

Recommend dropping the word "continuous" from the entirety of these regulations. Assessment of compliance can be conducted periodically but no guarantees can be made or should be reasonably expected about the future. In fact the reverse is true. You can guarantee that any system actually in use will fail to meet some assessment objective at some point for some reason. Also, consider this under the light of future DoJ indictments. As written this guarantees that every contractor will fail and in the event of an investigation the Senior Official could be subject to a fraud indictment… for failing in the impossible task of maintaining perfection into an unending future. As written this will become within a few years the go-to mechanism for every contracting officer to punish or terminate any contractor for any reason at will because swearing compliance into an unknown future will have a 100% failure rate. In turn, the unintended consequences for this on corporate operations will drive organizations to great lengths to avoid the regulation, hide cyber incidents, create pristine separate networks that are never used, and halt any future cyber incident reporting because although not reporting is a violation of the regulation, reporting an incident becomes a path to potential personal indictment on federal criminal fraud charges.

_____

Comment #12

https://www.federalregister.gov/d/2024-18110/p-150

> "DoD does not expect this proposed rule, when finalized, to have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601, *et seq"*

Per the DoD's request for feedback on the impact on small businesses, these expectations are completely incorrect.

The DoD Small Business Strategy from 2023 states:

> "It is imperative for the Department to focus on small business. These innovative companies account for 43 percent of all high-tech jobs in the U.S. and generate sixteen times more patents than large firms. Small businesses spur innovation, represent most new entrants into the Defense Industrial Base (DIB), and through their growth represent the next generation of suppliers with increasingly diverse capabilities. Small businesses are agile and often can implement change more quickly than larger firms. In Fiscal Year (FY) 2021, **small businesses made up 73 percent of all companies that did business with DoD and 77 percent of the research and development (R&D) companies** that did business with DoD." https://media.defense.gov/2023/Jan/26/2003150429/-1/-1/0/SMALL-BUSINESS-STRATEGY.PDF

Small businesses make up an outsized portion of the DIB and most small businesses live below what has been dubbed as the "cybersecurity poverty line." We define this line as the point at which *gross* income is less than the required funding to fully implement the controls of NIST 800-171. Roughly we estimate this as companies below 100 employees and less than $6.5M in annual gross revenue.

Additionally, almost all of these small businesses use what 32CFR170 proposed rule has defined as an External Service Provider (ESP), and *expanded* the definition of covered entities and systems to include the requirement for a CMMC certification of these providers as a pre-requisite for the OSC/OSA's own

CMMC certification or CMMC Self Assessment at level 2. The vast majority of these ESPs are unaware of these requirements. The DoD has undertaken no effort to communicate with these communities of the new impending, expensive certification requirements. There are a very limited number of companies, perhaps fewer than 10, that currently are aware of an actively pursuing CMMC L2 certification readiness. That number is growing but it is a tiny fraction of the capacity needed to provide these services to the DIB at any price. As the implementation of CMMC at the small business level is relatively very expensive, and many ESPs are small businesses too, the cost of these certification-ready companies is quite high in comparison to the rates small businesses are paying for these services today. As an example, in soliciting three of these companies for the implementation of a compliant network for a company needing a network supporting 20 office workers, the results were on average $200K for initial implementation, and $200K per year to maintain that network. They also exceeded the capability of the small business to bear those costs and remain in business. They elected to delay full implementation pending the final rule.

The largest part of this problem, which is potentially not obvious, is that the costs of implementation and ongoing compliance do not *scale down* past a certain minimum size. I estimate this as roughly at the 250-employee point where this begins to become a problem. Below that as the company size and total cash flow shrinks, the compliance implementation costs do not proportionally scale down eating an ever-increasing share of revenue. The point at which this becomes truly unsustainable for the business varies. Ultimately these companies cannot do work for the DoD at a loss. However patriotic, the day comes when you cannot pay your employees. The variation in turn makes the potential impact to the size of the DIB difficult to calculate. This impact is interconnected with the number of L2 Certification and Self-Assessments that will be required. We submit that the 32CFR170 estimates, which are substantially larger than those contained in this rule, underestimate the number of companies that will require L2 certification or self-assessment but are better. Based on the DoD's handling of CUI, and the broad uncertainty of what is CUI both inside and outside of government, we anticipate that most contracts will entail the potential of CUI handling and in turn, require L2 certification or self-assessment. **Potentially over 50% of the DIB Small Business Community will be forced out of the DIB, or out of business**. Regardless high cost, and high attrition due to those costs **will** most definitely have "a significant economic impact on a substantial number of small entities." NDAA 2020 Section 1648 (c)(3) has largely been ignored directing that the Secretary shall "consider tailoring" for SMB.

_____

Comment #13

https://www.federalregister.gov/d/2024-18110/p-190

> "(i) The results of a current CMMC certificate or current CMMC self-assessment at the level required by the solicitation, or higher, for each DoD unique identifier (DoD UID) applicable to each of the contractor information systems that will process, store, or transmit FCI or CUI and that will be used in performance of the contract posted in the Supplier Performance Risk System (SPRS) (see 32 CFR 170.15 through 170.18); and"

And in the 7021 clause itself https://www.federalregister.gov/d/2024-18110/p-220

"(b) Requirements. The Contractor shall—
(1)(i) Have a current CMMC certificate or current CMMC self-assessment at the following CMMC level, or higher: _____ [Contracting Officer to fill in the required CMMC level];"

As written this seems to leave the contracting officer with three options for CMMC level; Level 1, Level 2, or Level 3. It does not specify certificate or self-assessment. At Levels 1 and 3 this does not matter as both of those have singular specified mechanisms to achieve the required compliance level; self-assessment and DIBCAC assessment. At Level 2 however, the most crucial and widespread, the option exists for either a certification or a self-assessment without specification. As worded this would mean that the OSC/OSA would exercise the option of whether or not to seek a certification or execute a self-assessment. As we understand things, this is not the DoD's intent. The intent has been since CMMC has been conceived to require certification assessments for the majority of contractors at Level 2. If the DoD has altered that intent and instead intends to allow all contractors to self-assess at Level 2 in all cases, then the CMMC ecosystem will cease to function in short order. There will not be a sufficient number of Level 2 certification assessments to support just the Level 3 certification requirements to support ecosystem membership. This would also fundamentally undermine the raison d'être for the entire certification program as a means to verify DIB compliance.

Recommended modification of this follows:
"(b) Requirements. The Contractor shall—
(1)(i) Have a current CMMC assessment at the following CMMC level, or higher: _____ [Contracting Officer to fill in the required CMMC level and for Level 2 self or certification assessment];"

_____

Comment #14
https://www.federalregister.gov/d/2024-18110/p-191

Recommend drop the word "continuous" for reasons stated in Comment #11

_____

Comment #15
https://www.federalregister.gov/d/2024-18110/p-195
Recommend drop the word "continuous" for reasons stated in Comment #11

_____

Comment #16
https://www.federalregister.gov/d/2024-18110/p-198

Recommend drop the word "continuous" for reasons stated in Comment #11

_____

Comment #17
https://www.federalregister.gov/d/2024-18110/p-208

Recommend drop the word “continuous” for reasons stated in Comment #11

_____

Comment #18

https://www.federalregister.gov/d/2024-18110/p-213

Adjust the definition of current, and add the definition of changes to compliance as outlined in Comment #8

_____

Comment #19

https://www.federalregister.gov/d/2024-18110/p-219

Recommend adjusting the language around CMMC Level requirement specification as outlined in Comment #13

_____

Comment #20

https://www.federalregister.gov/d/2024-18110/p-224

> (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;

“Lapses in information security” are too broad a reporting requirement. This is also another ***expansion*** of the overall requirements. Nearly anything could be construed as a lapse in information security. If someone holds the door open for a fellow employee in violation of policy requiring them to badge in, then that now becomes an offense reportable to the DoD. Any number of things that are daily parts of real operations are potentially lapses in information security. Every time an employee clicks the link, it is a lapse of information security. Etc. Etc. Leave the current definition of incident reporting as it stands in DFARS 2523.204-7012 and drop the reporting requirement for “lapses.”

Recommend revision as follows
(4) Notify the Contracting Officer within 72 hours when there are any changes in CMMC compliance status during performance of the contract;

Utilizing the supplied definition of changes in compliance status as recommended in Comment #8.

Philosophically consider the addition of new expanded reporting requirements as represented by the inclusion of the “lapses” clause here. **The continuous movement to expand the scope and requirements of these regulations is counterproductive.** The DoD messaging on this to both senior executives in industry and senior officials in the Department has been and continues to be the assessment of a moderate level of cybersecurity that every company should be doing in their own defense anyway, and does nothing other than assess the implementation of controls that have been

required in contracts for nearly the last 10 years. Sounds quite reasonable except as written in these regulations that is not what is being done. This is not helpful. Well-meaning perhaps but ultimately extremely counterproductive. Every one of these "little" things tacked on distracts, and more importantly diverts resources away from, doing what we really need to do; raise the bar on cybersecurity in the DIB. Reporting requirements, evidence gathering, assessing… all of that is just **overhead.** It pulls resources away from doing the real work of cybersecurity for which there is now and always will be a limited supply. Minimize the overhead, dont maximize it. We have to have some of that to build in the needed accountability mechanism, but not one more word or requirement than is vital for the core mission. Because every one of those additional good idea tack-ons takes effort away from doing cybersecurity in a zero-sum resources game.

You asked in the header for feedback on, "whether this collection of information is necessary for the proper performance of the functions of DoD, including whether the information will have practical utility;" This ever-increasing expansion is not useful and the reporting of lapses represents no utility for the DoD. It is written apparently without consideration that every single word costs millions of dollars in execution and potentially, …potentially harms the very cybersecurity programs that the Department wants these regulations to engender by adding additional distractions from the core business of raising cybersecurity across the DIB. Increased reporting requirements do nothing to improve cybersecurity.

_____

Comment #21

https://www.federalregister.gov/d/2024-18110/p-225

https://www.federalregister.gov/d/2024-18110/p-226

Recommend drop the word "continuous" for reasons stated in Comment #11

_____

Comment #22

https://www.federalregister.gov/d/2024-18110/p-231

> (d) Subcontracts. The Contractor shall—
>
> > (1) Insert the substance of this clause, including this paragraph (d), and exclude paragraphs (b)(5) and (c), in subcontracts and other contractual instruments, including those for the acquisition of commercial products and commercial services, excluding commercially available off-the-shelf items, when there is a requirement under the subcontract or similar contractual instrument for a CMMC level; and
> >
> > (2) Prior to awarding a subcontract or other contractual instrument, ensure that the subcontractor has a current CMMC certificate or current CMMC self-assessment at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor.

Based on the discussion section here the above language on flow down seems inconsistent with:

> "Furthermore, CMMC certification requirements must be flowed down to subcontractors at all tiers when the subcontractor will process, store, or transmit FCI or CUI, based on the sensitivity of the unclassified information flowed down to each of the subcontractors in accordance with the proposed CMMC 2.0 requirements to be established at 32 CFR part 170 (see 88 FR 89058)."

The discussion importantly adds the phrase, “based on the sensitivity of the unclassified information.” This phrase should be added to the substantive rule language.

_____

Comment #23
https://www.federalregister.gov/d/2024-18110/p-236

> (b)(1) *Cybersecurity Maturity Model Certification (CMMC) level.* The CMMC certificate or CMMC self-assessment level required by this solicitation is: _____ *[Contracting Officer insert: CMMC Level 1 self-assessment; CMMC Level 2 certificate or CMMC self-assessment; or CMMC Level 3 certificate].* This CMMC certificate or CMMC self-assessment level, or higher, is required prior to award for each contractor information system that will process, store, or transmit Federal contract information (FCI) or controlled unclassified information (CUI) during performance of the contract.

Aligned with the same reasoning for the clause language from Comment #13, recommend revision to:

> “(b) Requirements. The Contractor shall—
> (1)(i) Have a current CMMC assessment at the following CMMC level, or higher: _____ [Contracting Officer to fill in the required CMMC level and for Level 2 self or certification assessment];”

_____

Comment #24
https://www.federalregister.gov/d/2024-18110/p-79

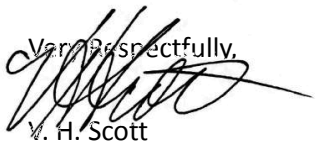
> Comment: Many respondents commented that clarification is needed regarding whether CMMC applies to fundamental research.
> Response: Fundamental research, as defined in National Security Decision Directive (NSDD) 189, is published and broadly shared within the scientific community and, as such, cannot be safeguarded as either FCI or CUI; **however, if fundamental research has the potential to become CUI, it would be subject to the requirements of CMMC.**

This is a completely unreasonable expectation without basis in 32CFR2002. Organizations cannot be expected to have a crystal ball to determine if, at some point in the future, the DoD might decide that some piece of information is CUI. It is either to be designated as CUI on creation as specified in the contract or it is not. There are no regulatory options for “we might want to make up our mind at some point in the future.” This expectation places an undo and unreasonable burden on contractors, particularly research institutions in conducting fundamental research. Recommend deletion of the entire bold phrase.

_____

3. We appreciate the DoD’s desire to pursue a higher level of cybersecurity across the DIB and firmly concur that an accountability process based on assessments is the way to drive that improvement. We also continue to note that the pursuit of perfection in implementation without variance is not achievable and submit that worse, it will drive degraded rather than enhanced security for DIB companies. The DoD

has succeeded in presenting a huge compliance risk to the DIB. When that risk is so great that it drives activities that degrade rather than enhance security though it becomes a potentially very expensive break on cyber maturity. We submit that the DoD is well into braking territory with the combination of 32CFR170 and this contract clause.



Very Respectfully,

V. H. Scott