03 August 2027

TO: Honorable Kirsten A. Davies via Ms. Leanne Condren at whs.mc-alex.ad.mbx.eosd-psb-branch-mailbox@mail.mil and leanne.m.condren.civ@mail.mil

CC: See Supplement page 1

Subject: Reforming CMMC and Reducing Compliance Burden for the DIB

Dear Ms. Davies;

As the president of an authorized CMMC 3rd Party Assessment Organization (C3PAO) and a veteran, thank you for pausing the transition to CMMC Phase 2. The vast majority of our clients have been small businesses, and with only a handful of exceptions, none of our clients were ready to get certified out of the gate. The pause was the right thing to do. So is keeping the pressure on.

Peak InfoSec has been involved in Defense Industrial Base (DIB) DFARS Clause 252.204-7012 implementation efforts since our founding in 2016 when the requirements were based on NIST SP 800-53. While some DIB contractors believed in the mission and committed to implementing NIST SP 800-171, many we interacted with over the years looked at compliance as a business risk and chose to blatantly disregard their contractual obligations.

In our experience, the vast majority of the DIB did not begin to seriously implement NIST SP 800-171 until CMMC was introduced. Unfortunately, every time the Department of War "took a relook" or "re-assessed" CMMC, that majority of DIB companies chose to stop all CMMC efforts. We already know via our partners that this suspension is no different, and DIB cybersecurity is stopping and slipping backwards as a result of the current "suspension".

Many claim, and we agree with them, that, in general, compliance does not equal security. However, in our experience, third-party compliance review catalyzes organizations to implement security. Without that catalyst, there is no action that can overcome any business's focus on the bottom-line. CMMC is a catalyst that galvanized the DIB into finally implementing NIST SP 800-171 protections and onto a path to adopting mature, ingrained information security practices. The threat of an audit by DIBCAC followed by a False Claims Act charge has proven to be orders of magnitude less effective as a catalyst and is simply has not motivated the DIB to implement NIST SP 800-171.

In the following pages, we highlight many improvements your office can adopt which make it easier for the DIB to mature into a compliant state while also providing ways your office can reduce C3PAOs' operating and certification costs. There are significant areas when your predecessors, in an over-abundance of caution, took steps which added unnecessary complexity and increased the program's certification costs and reduced C3PAOs' agility. If your office implements our suggestions, we estimate that the cost of conducting a CMMC Level 2 Certification Assessment would decrease by 15-20%. By allowing C3PAOs to operate as fully independent ISO inspection bodies, including allowing surveillance assessments, will likely further reduce CMMC Level 2 Certification Assessment costs by another 10% over the typical triennial cycle while simultaneously improving DIB cybersecurity and resilience.

As an Air Force Program Manager and Enterprise Architect that worked within the Air Force CIO's purview, I also request that, when your task force and you are considering your options, you not discount the interconnected nature of the DoW and the DIB, or the fact that nation-state actors are creating, and injecting via the DIB, exploitable threats against our warfighters. This threat, and potential attack surface it creates, is vast and <u>will</u> be exploited against us.

Please let us know if you have any questions about our comments and suggestions. We truly stand by to help your office protect our warfighters and the DIB.

Very Sincerely,

Matthew Titcombe:A0109B300000191EC07A90E00000043

Digitally signed by Matthew Titcombe:A0109B300000191EC07A90E00000043
Date: 2026.08.03 11:05:44 -04'00'

Matthew A. Titcombe, CISSP, LCCA, CCI
President

PEAK INFOSEC
Trusted Guides For Your CMMC Journey

cmmc@peakinfosec.us | www.peakinfosec.com | (352) 575-9737
3001 N. Rocky Point Dr. E, Suite 200, Tampa FL 33607

Company Information	Point of Contact
Peak InfoSec LLC CAGE CODE: 7JCH4 D-U-N-S®#: 10-123-8375 Unique Entity ID (UEI): LLMDWL7VF4B6	Matthew A. Titcombe, President 3001 N. Rocky Point Dr. E, Suite 200, Tampa FL 33607 Office: 352-575-9737 (no Fax) Email: m.titcombe@peakinfosec.us

1. Identify the top five most prohibitive cost drivers, administrative burdens, or operational challenges your organization has experienced, or anticipates to experience, when attempting to comply with the CMMC framework and NIST SP 800-171 Rev 2.

As a veteran-led CMMC 3rd Party Assessment Organization (C3PAO), Peak InfoSec implemented and was assessed twice by the Defense Industrial Base Cybersecurity Assurance Center (DIBCAC); initially, when we were an organization of only two people, and then subsequently as a three-person company. This makes us a quintessential small business. As a small business C3PAO implementing NIST SP 800-171 Rev 2 as a part of the CMMC program, the top five "prohibitive cost drivers, administrative burdens, or operational challenges" we experience are:

A) The Use of FedRAMP Cloud Services [Prohibitive Cost Driver]:

With only a rare few exceptions, the price differences between commercial Cloud Service Providers (CSP) and their FedRAMP offerings range from two to five times the cost of the corresponding commercial offering. From a Total Cost of Ownership (TCO) perspective, the costs are higher because technical support is harder as there are differences between what the commercial and FedRAMP clouds may offer. This forces increased time to troubleshoot issues and work though disconnects when things break as commercial upgrades are pushed up to FedRAMP versions months, and sometimes years, later. The mandate to use FedRAMP also decreases the organization's security posture as more advanced, secure solutions are available on the commercial side that are not in the FedRAMP clouds. Organizations that piecemeal their solution using multiple vendors only exacerbate their initial licensing costs and increase their overall TCO even more.

B) DIBCAC Assessments [Administrative Burdens]:

As a C3PAO, the requirement in 32 CFR 170.9(b)(6)(i)[i] to have DIBCAC conduct an assessment is an administrative burden that is better served by having The Cyber AB conduct C3PAO assessments as a part of their authorization and accreditation processes. Akin to businesses having to grapple with significant changes, this stifles a C3PAO's ability to innovate, adopt controlled Artificial Intelligence (AI) mechanisms to streamline, and deal with market pressures to reduce costs. As a part of the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17020:2012(E), "Conformity assessment—Requirement for the operation of various types of bodies performing inspection," annual surveillance conducted by The Cyber AB, The Cyber AB can review our security changes annually versus once every three years done by DIBCAC. This would also save taxpayer funds while freeing up DIBCAC assessors to conduct DIB assessments and investigate potential False Claims Act (FCA) issues.

C) Tier 3 Background Screening [Prohibitive Cost Driver & Administrative Burdens]:

The requirement in 32 CFR 170.9(b)(3)[ii] that "all C3PAO company personnel participating in the Level 2 certification assessment process to complete a Tier 3 background investigation resulting in a determination of national security eligibility" is both a prohibitive cost driver and administrative burden. As explained below, it is quickly becoming an operational challenge due to labor pool limitations created by DoW.

As a Cost of Services Sold (COSS), the latest estimates from the CMMC Assessor & Instructor Certification Organization (CAICO) indicate 2,040 individuals completed their Tier 3 background investigations done by DoW and are now qualified to be a CMMC Certified Assessor (CCA), Lead CCA (LCCA), or CMMC Certified Professional (CCP). Likewise, the CAICO estimates that ~600 individuals are awaiting their Tier 3 background investigations. This includes individuals who already possess an active Top Secret/Sensitive Compartmented Information (TS/SCI) clearance. Anecdotally, the wait times for the Tier 3 to complete are 12-18 months!!! Presuming all 600 of these individuals are eligible, then DoW is denying 22.7%[iii] from being in the workforce to conduct assessments. To get scale, DoW must remove all blockages to get more labor into the labor pool. Furthermore, the shortage of assessors is driving up COSS that are passed onto our clients. In a recent hiring effort by Peak InfoSec, we had a 1% offer rate because Peak InfoSec was forced to pass by a significant number of highly qualified candidates because DoW had not completed their Tier 3 review. This reduces the supply of qualified CCAs and LCCAs, which is resulting in authorized CCAs and Lead CCAs commanding increased salaries. The

limited number of assessors is further complicated by the fact that a significant portion of assessors are not assessing as they are focusing on consulting or in-house work per a recent survey by The Cyber AB.
With demand going up for NIST SP 800-171 compliance due to both CMMC and the forthcoming FAR CUI rule, and the labor pool being limited, costs will increase for C3PAOs and firms that help clients implement NIST SP 800-171 security controls. These COSS must, inherently, be passed onto the DIB.

D) DoW Generated Bureaucratic Overhead for C3PAOs [Prohibitive Cost Driver & Administrative Burdens]: In addition to 32 CFR 170.9(b)(3) and 32 CFR 170.9(b)(6)(i) specified above, the following parts of 32 CFR 170 create unnecessary cost drivers and administrative burdens that increase the overall COSS related to conducting CMMC Level 2 Certification Assessments:

- 32 CFR 170.9(b)(12)[iv]: The requirement that an "Assessment Team must include at least two people: a Lead CCA, as defined in § 170.11(b)(10), and at least one other CCA" further exacerbates the labor problems caused by the Tier 3 backlog issues. While we understand the need to maintain a two person-rule to avoid any perceived conflicts of interest, the requirement negates any benefits a C3PAO can also gain by using a CCP to fulfill this role while also using the opportunity to train up-and-coming CCAs as a part of our ISO/IEC 17020:2012 requirements[v]. This requirement fundamentally makes the CCP certification useless for a C3PAO and forces the C3PAO to use a significantly more expensive labor category.
- 32 CFR 170.9(b)(13)[vi]: The requirement that "Any individual fulfilling the quality assurance function must be a CCA and cannot be a member of an Assessment Team for which they are performing a quality assurance role" pushes the C3PAO to have three of the most expensive personnel involved. Furthermore, under ISO/IEC 17020:2012 para 6.1.5, this requires the CCA fulfilling this role to be fully trained and qualified by the C3PAO to both conduct assessments and serve as the Quality Assurance (QA). Under normal ISO practices, the QA role is filled by the organization's QA function that manages the overall assessment process established by the C3PAO. Given that the person conducting/serving in the QA role is not making conformity determinations, this role does not need to be a CCA.
- 32 CFR 170.9(b)(8), 32 CFR 170.9(b)(17), and 32 CFR 170.17(a)(1)(i): eMass uploads have become a significant burden. DoW consistently requires that C3PAOs provide information (e.g., the names of subject matter experts being interviewed by the C3PAO) that exceeds the information specified in 32 CFR 170.17(a)(1)(i). In addition, the required information is considered confidential by our clients and must be protected per our Non-Disclosure Agreements (NDA) with the clients. Despite continued requests to coordinate with The Cyber AB and C3PAOs, eMASS program has continued to make ad hoc changes to their templates without communication or notice. This forces C3PAOs to spend additional time and labor hours dealing with unexpected disconnects, updating data models, and addressing confidentiality conflicts caused by DoW.
- 32 CFR 170.9(b)(18)[vii] and 32 CFR 170.17(a)(1)(i)(E)[viii]: The requirement to have C3PAOs "issue Certificates of CMMC Status to OSCs … that include, at a minimum, all industry CAGE codes associated with the information systems" has become a bureaucratic nightmare for C3PAOs. Foremost, C3PAOs assess information systems–not CAGE codes. Even for small businesses, the relationship between CAGE codes and information systems can get convoluted as one small business may be part of an interrelated set of small businesses. C3PAOs are now forced to help guide clients through CAGE code conflicts, a subject about which most C3PAOs are not experts. Every time the client provides a C3PAO inaccurate information, we are forced to regenerate a new Certificate and update the assessment information submitted to CMMC eMASS. This is an administrative burden and cost driver that was not forecast in the program rule.

E) The Cyber AB's CMMC Assessment Process (CAP) [Prohibitive Cost Driver, Administrative Burdens, & Operational Challenge]: When CMMC was originally conceived, the CAP was created because The Cyber AB was supposed to be the Certifying body and C3PAOs were "just" providing recommendations. DoW's decision that C3PAO's must be ISO/IEC 17020 based inspection bodies shifted to the C3PAOs the requirement to establish and follow an internally defined procedure. This is especially evident in ISO/IEC 17020:2026[ix]. The current CAP is still tied to CMMC 1.0 paradigms. While useful as an informative reference for new C3PAOs, the current CAP[x] places operational mandates that constrict the innovative nature of a C3PAO to respond to market pressures and drive down our costs and prices.

2. Which specific security controls has your organization found to deliver the most tangible uplift of cybersecurity and actual risk reduction?
Contrary to DoW's perception, our initial 3rd party DIBCAC assessment in 2022 created the most uplift. While we were compliant with the requirements, the initial preparation work guided us and helped us to find flaws in our

PEAK INFOSEC
Trusted Guides For Your CMMC Journey
cmmc@peakinfosec.us | www.peakinfosec.com | (352) 575-9737
3001 N. Rocky Point Dr. E, Suite 200, Tampa FL 33607

thinking. As a result, it took less than four days to complete our initial interviews and tests with DIBCAC. In addition, because we maintained our environment, provided ample evidence to DIBCAC to explain our expected behavior, and were prepared to demonstrate actual behaviors as required by NIST SP 800-171A, our second re-assessment interviews and tests by DIBCAC in 2025 completed in eight and a half hours.
Aside from the security requirements identified in the next question, the remaining NIST SP 800-171 security requirements are foundational to us implementing actual zero-trust mechanisms to protect ourselves against potential nation-state level attacks.

3. Conversely, which specific regulatory requirements or security controls create the highest administrative overhead and financial burden with the least measurable improvement to your actual cybersecurity posture?
As stated previously, FedRAMP creates a significant financial burden and actually reduces our ability to implement enhanced security controls due to the lag for the capabilities to get to the FedRAMP clouds.
The NIST SP 800-171 Rev 2, 3.12.4, "Develop, document, and periodically update system security plans…" has become a bureaucratic documentation nightmare that is bogging down small businesses. Even in our dealings with DIBCAC, if something wasn't "just perfect" and "all of the i's dotted and t's crossed" in the System Security Plan (SSP), many DIBCAC assessors' and CCAs'/Lead CCAs' inclination is to mark the organization as not met. This wastes countless manhours on maintaining paperwork when NIST's intention is to allow documentation plus interviews to define the expected behavior.[xi]
Given that in NIST SP 800-171 Rev. 3, NIST either withdraws or heavily consolidates the majority of the Maintenance family, we found the entirety of the Maintenance domain to be of limited value. Given the proclivity of all businesses to use Remote Monitoring & Management (RMM) applications, only NIST SP 800-171, Rev 2, 3.7.5[xii], "Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete" should remain.
With the heavy adoption of perimeterless architectures, NIST SP 800-171 Rev 2, 3.4.7, "Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services" is a bureaucratic and administrative nightmare to develop and maintain, especially for small businesses.

4. Describe how your organization utilizes existing commercial cybersecurity capabilities, platforms, managed services, or any other additional strategies or initiatives to safeguard data, improve operational resiliency, and reduce cybersecurity risk, and how the DoW might better recognize or accept these commercial solutions within a compliance or risk framework.
Peak InfoSec uses Microsoft's FedRAMP High Office 365 and supporting infrastructure in Microsoft's Government Community Cloud-High (GCCH) tier. We also use CISCO DUO FedRAMP Moderate tool for our Multi-Factor Authentication functionality. As an organization that does not handle client FCI or CUI and given that 32 CFR Part 170 does not stipulate the usage of FedRAMP clouds for C3PAOs, we are only using FedRAMP clouds to reduce the risk of DIBCAC finding us non-compliant because neither vendor has a commercial body of evidence that meet NIST SP 800-171 security requirements or a Customer Responsibility Matrix. This underlies the administrative and prohibitive cost burdens DoW is creating by mandating FedRAMP or an unachievable demonstration of evidence.
If DoW continues to impose additional safeguarding requirements on CSPs above those in NIST SP 800-171 as required under 32 CFR 2002, DoW should look to embrace GovRAMP, ISO 27000 series, and other third-party validated CSP frameworks under 32 CFR 170.20, standards acceptance. However, given that ISO 2700x, GovRAMP, and other frameworks contain fundamentally different requirements, we suspect that it will be difficult for DoW to accept these standards.

5. a. Regarding Phase I self-assessments, what specific administrative or technical challenges does your organization face in maintaining, verifying, and reporting compliance, and how could this process be fundamentally streamlined?
This question seems to be narrowly focused on the effort spent reporting compliance to the Supplier Performance Reporting System (SPRS). As an organization that submits its self-assessments, we frankly spend more time logging into SPRS to change our password than it takes to report our self-assessment. Why? Because we are compliant and maintain our compliance.
DoW also presumes in this question that the DIB is compliant with NIST SP 800-171. It isn't. The time and effort to self-assess is an iterative loop for non-compliant companies to implement NIST SP 800-171 security requirements and undergo culture changes. This is an area where DoW must separate the NIST SP 800-171 implementation, which includes both continuous[xiii] and periodic self-assessment[xiv] of security requirements, from the NIST SP 800-171 3rd Party Assessment of the organization's implementation. In our experience with over a hundred firms of all

PEAK INFOSEC
Trusted Guides For Your CMMC Journey
cmmc@peakinfosec.us | www.peakinfosec.com | (352) 575-9737
3001 N. Rocky Point Dr. E, Suite 200, Tampa FL 33607

sizes, implementing technology is the easy part. Getting the organization to commit to the change, pay for the jump to FedRAMP mandated services, adapt processes, and adjust their culture are the real time and cost drivers. This is the fundamental internal organizational challenge of an organization implementing NIST SP 800-171 controls and why it normally takes 12-18 months. Likewise, this is something DoW simply does not understand as DoW has never implemented the Security Requirements in a business. Still further, adopting culture change is not something that can be streamlined; it takes time for organizational culture to change.

5. b. Have your self-assessments led to a more dynamic cyber posture approach, or are they performed only for compliance purposes?

This question indicates DoW assumes that businesses understand what NIST SP 800-171 security requirements are. Our leadership team has been conducting NIST SP 800-171 assessments since 2018. In all that time, it has become abundantly clear that organizations of all sizes, and especially small businesses, do not understand the security requirements. Instead, they make numerous, significant misinterpretations that lead to false indicators of success. In our experience, only cursory assessments are performed and the results pencil-whipped into fulfilling compliance reporting. Put more simply, without oversight, organizations will rationalize what they are doing as meeting the security requirements when in fact they have entirely failed to meet many of the requirements.

6. What specific, actionable policy changes or regulatory reforms should the CMMC Reform Task Force recommend over the next 60 days to drastically reduce costs and barriers to entry for small, medium, and non-traditional businesses without degrading the protection of federal data?

The follow recommendations to the CMMC Reform Task Force are first bound by the following key Law, Regulatory, or Government Wide Policies (LRGWP) that the DoW does not have the authority to contravene:

- Executive Order 13556 -- Controlled Unclassified Information[xv]
- 32 CFR Part 2002[xvi]

The following recommendations also presume the Office of Department of War CIO and the Under Secretary of War for Acquisition & Sustainment re-instate 3rd party assessments of a DIB organization's implementation of NIST SP 800-171. Given the complexity of the DIB and that NIST SP 800-171 includes resiliency requirements in the Non-Federal Organization controls, we do not try to address this area as it would be best determined via other Acquisition mechanisms or additional regulations.

A) Empower your Department Acquisition Executives & Requirement Owners (AE/RO)

- DESCRIPTION: Both the Offices of Department of War CIO and the Under Secretary of War for Acquisition & Sustainment do not and should not claim to understand the types of sensitive information being provided to small businesses based on anecdotal evidence. Understanding the sensitivity and criticality of information for each and every program in the DoW lies with the AE/ROs and their respective Program Management Offices (PMO). This is especially true when considering the interconnectedness of the DoW information systems and Acquisition Category (ACAT) Level 3 or higher[xvii] Programs of Record (PoR). Properly training DoW personnel on what constitutes CUI and how to avoid giving contractors CUI when access to it is not needed to fulfill a lawful government purpose would drastically reduce costs and barriers to entry for small, medium, and non-traditional businesses without degrading the protection of federal information. For example, in a base-level, non-ACAT level contract to have a small business paint a building, the painting contractor should not be expected to handle CUI if the AE/RO properly abstracted out the non-CUI information (i.e., the square feet of surface to be painted) from the CUI (i.e., the critical infrastructure components of the building plan), thus avoiding the need for CMMC Level 2 Certification for the painting contractor. Similarly, DoW should not require 3rd party certification at the point of innovation.

  However, it is important to recognize that business size is not an indicator of whether a company will be handling CUI. For example, a separate small business may be handling Unclassified Controlled Nuclear Information – Defense (CUI//SP-DCNI)[xviii] or other forms of CUI that now become an exploitable piece in the interconnected nature of DoW under an ACAT Level 3 or higher program. The risk profile for determining whether a CMMC Level 2 Certification by a C3PAO or even CMMC Level 3 assessment should be made only by the AE/RO for that program as a formal acquisition decision.

  It would be incredibly difficult for either the Offices of Department of War CIO or the Under Secretary of War for Acquisition & Sustainment to make that level of a risk-decision carte blanche on behalf of the entire DoW. A one-size-fits-all risk profile approach simply does not work given the complexity of the DIB and the sensitivity of information provided to the DIB.

PEAK INFOSEC
Trusted Guides For Your CMMC Journey
cmmc@peakinfosec.us | www.peakinfosec.com | (352) 575-9737
3001 N. Rocky Point Dr. E, Suite 200, Tampa FL 33607

- ACTION: The Office of Department of War CIO and CMMC PMO should reinstate CMMC Level 2 (C3PAO) with the requirement for AE/ROs to make the risk determination of if and when a CMMC Level 2 (C3PAO) assessment is required.
- ACTION: The Under Secretary of War for Acquisition & Sustainment or their authorized delegate should publish a memorandum requiring base-level and sustainment AE/RO's to complete a risk analysis for their requirement(s) to determine whether their contracts should require a CMMC Level 2 Certification Assessment by a C3PAO. All ACAT Level 3 or higher PoRs should be required to include CMMC Level 2 (C3PAO) in their contracts when the DoW CIO reinstates Phase 2.
- BENEFIT: This properly places risk-acceptance with the AE/RO and allows flexibility while still taking rigorous steps to protect the more sensitive forms of CUI that exist in the DIB based on ACAT levels.

B) Remove the FedRAMP Moderate of Higher Requirement

- DESCRIPTION: The FedRAMP Moderate authorized or equivalent requirement creates an onerous and cost-prohibitive requirement. DoW's inclusion of the FedRAMP requirement for all small business contractors that may handle CUI engenders duplicative costs to set up, migrate, and maintain because most small businesses start in the commercial CSPs.
- ACTION: The Under Secretary of War for Acquisition & Sustainment should publish a class deviation which amends DFARS Clause 252.204-7012(b)(2)(ii)(D) from "…the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/documents-templates/) and …" to "…the Contractor shall require and ensure that the cloud service provider meets security requirements published in the current version of NIST SP 800-171".
- ACTION: The Under Secretary of War for Acquisition & Sustainment or authorized delegate should initiate steps to formally amend DFARS Clause 252.204-7012(b)(2)(ii)(D) language as described above.
- ACTION: The CMMC PMO should notify The Cyber AB to publish a Management Decision directing all C3PAOs and their assessors to disregard the FedRAMP scoping requirement for External Service Providers (ESP) and to instead require NIST SP 800-171.
- BENEFIT: This aligns DoW with Executive Order 13556, which requires NARA and the federal agencies to establish an 'an open and uniform program" for sharing CUI and 32 CFR 2002 which requires that non-federal systems that handle CUI be evaluated against NIST SP 800-171 and no other federal information security program (like FedRAMP or NIST SP 800-53). It also lowers costs for both the DIB and for the DoW.

C) Create a Graduated Plan of Action & Milestone (POA&M) Approach

- DESCRIPTION: The current 32 CFR 170.21(a)(2)[xix] POA&M approach is contrary to actual internal DoW and industry best practices. The current practice of meeting all the critical 5-point, moderate 3-point, and 1-point requirements plus having a score above 88 from the range of -203 to 110 per 32 CFR 170.21(a)(2), is onerous and restrictive to all businesses and even internal DoW PoR within the classified eMASS. DoW should replace the current POA&M section in 32 CFR 170.21(a)(2) with language that allows for a graduated, 3rd-party validated, implementation of POA&Ms. Prior to CMMC, POA&Ms were simply never closed out as DFARS Clause 252.204-7012 fundamentally only requires a SSP and a POA&M to be eligible to have a DoW contract. Reporting scores in SPRS has no assurance the DIB organization is actually doing what they say. A graduated approach, akin to normal ISO practices for handling major findings, would allow a DIB company to get to the basic threshold established by DoW and then validated by a C3PAO. The C3PAO then works with the DIB company as they continue making progress implementing all NIST SP 800-171 requirements and adapting to new technical requirements. A suggested basic threshold would be implementation of all 5-pointers in the Access Control, Configuration Management, Identification & Authentication, Physical Security, System & Communications Protection Maintenance, and System & Information Integrity families. Likewise, the suggested period for full compliance would be two years and the organization would have to undergo C3PAO reviews every 180-days. This latter part is normal for businesses initially getting other ISO certifications by ISO inspection bodies.
- ACTION: The Office of Department of War CIO and the CMMC PMO should publish a class deviation memorandum for 32 CFR 170.21(a)(2) with new language while publishing a revision to 32 CFR 170.21(a)(2).
- BENEFIT: This removes the exceedingly high threshold for organizations whether conducting self-assessments or needing to be CMMC Level 2 certified by C3PAO. Within the commercial sector, this approach commonly lowers the overall compliance costs and spreads it out over multiple years, especially once the DIB company matures its cybersecurity practices.

D) Expand the Mentor/Protégé Program

cmmc@peakinfosec.us | www.peakinfosec.com | (352) 575-9737
3001 N. Rocky Point Dr. E, Suite 200, Tampa FL 33607

- DESCRIPTION: The DoW should expand the Mentor/Protégé program, especially in areas where the small business is handling sensitive CUI, as determined by the AE/RO. As a part of this expansion, DoW should allow for C3PAO assessment costs to be covered by the program.
- ACTION: The Under Secretary of War for Acquisition & Sustainment should direct the Deputy Assistant Secretary of War for Industrial Base Growth to expand the Mentor/Protégé program to include efforts required for the protégé to demonstrate via 3rd party assessment that their environment meets NIST SP 800-171 security requirements.
- BENEFIT: This increases resources available to the mentor firm to help their small business protégés. This is especially more important with the larger PoRs which are more likely to handle sensitive CUI.

E) Direct Cessation of On-site Assessment Requirements:
- DESCRIPTION: For a small business that has on-premises infrastructure, the current CAP requires all C3PAOs to conduct a physical site survey. Removing the physical site survey and replacing with a virtual one will reduce small business certification costs by $3,000-5,000 per site.[xx] This will also make C3PAOs more efficient, which can help us to reduce our overall COSS too.
- ACTION: The Office of Department of War CIO and CMMC PMO should publish a memorandum to The Cyber AB and all C3PAOs indicating that the DoW accepts the risk of not conducting a physical site survey for all small businesses that self-certify that they meet Small Business Administration sizing criteria and can demonstrate they are registered in SAM.gov as a small business for their NAICS.
- BENEFIT: This immediately reduces the costs to small businesses that need to get CMMC certified while increasing C3PAO efficiency and throughput.

F) Remove the requirement for Customer Responsibility Matrices (CRM) for CSPs
- DESCRIPTION: 32 CFR 170.19(c)(2)(ii)[xxi] requires a CRM where "The use of an ESP, its relationship to the OSA, and the services provided need to be documented in the OSA's SSP and described in the ESP's service description and CRM, which describes the responsibilities of the OSA and ESP with respect to the services provided." While appropriate when the organization is using an Information Security or Technology provider for managing its operating environment, requiring CRMs for CSPs is currently a waste of effort by all involved. Why?
  For FedRAMP CSPs, organizations are given the FedRAMP CRM, which was written under NIST SP 800-53 and for when the Federal Government is the customer. Since these CRMs are not written for non-federal systems or based on NIST SP 800-171, these CRMs are convoluted and arcane for small businesses to decipher. The CSPs that get certified as FedRAMP equivalent also have a NIST SP 800-53 based CRM and may have a NIST SP 800-171 based one. For CSPs that do not handle CUI, FedRAMP is not required. This increases complexity as most of these CSPs will never create a CRM, let alone one for NIST SP 800-171. This creates a bureaucratic, non-standardized, unmeasurable nightmare for the organization and C3PAO that wastes time and money on what is truly a paper chase by both the DIB company and C3PAO. Ultimately, DoW does not have the authority to regulate the interactions of private entities (contractors and CSPs). Further, the CRM requirement creates significant burden, and DoW has not estimated the financial impact of this additional regulatory requirement for contractors nor has DoW provided any evidence that CRMs provide value to the federal government or contractors. Removing this requirement would significantly streamline the implementation of NIST SP 800-171 requirements, reduce barriers to entry, and reduce costs.
- ACTION: The Office of Department of War CIO and CMMC PMO should publish a memorandum to The Cyber AB directing the immediate cessation of the requirement for CRM reviews for CSPs.
- ACTION: After receiving the memorandum, the Cyber AB should publish a Management Decision to all C3PAOs directing the immediate cessation of the requirement for CRM reviews for CSPs.
- BENEFIT: This is a zero-cost change that immediately reduces costs for the DIB and the COSS by C3PAOs when conducting assessments.

G) Remove the Tier 3 Background Investigation Requirement
- DESCRIPTION: Per 32 CFR 170.9(b)(4)[xxii], DoW can establish "the Tier 3 background investigation equivalence for use with the CMMC Program only" and direct the C3PAOs to conduct the equivalent background investigations. This would form the standard C3PAOs are required to follow per ISO/IEC 17020:2012 and The Cyber AB accreditation requirements.
- ACTION: The Office of Department of War CIO and CMMC PMO should publish a memorandum to The Cyber AB, CAICO, and all C3PAOs directing the immediate use of the Tier 3 background investigation equivalence by C3PAOs for "all C3PAO company personnel participating in the Level 2 certification assessment process" in lieu of the current process.

- BENEFIT: This is a zero-cost change that simplifies operations for The Cyber AB, CAICO, and C3PAOs while immediately unleashing a larger workforce pool. This will reduce the cost of assessors as the labor pool can grow faster, which will reduce the DIB small business' cost to get certified.

H) Remove or empower the CMMC Certified Professional (CCP) Certification:
- DESCRIPTION: 32 CFR 170.9(b)(12)[xxiii] and 32 CFR 170.9(b)(13)[xxiv] forces C3PAOs to use the most expensive labor categories for all CMMC Assessment-related work. The net effect is the CCP has become a useless certification for C3PAOs. We have yet to conduct an assessment for which it makes economic sense to include a CCP as part of an Assessment Team.
  Furthermore, the CCP certification creates a barrier to entry that only increases the individual's cost to get certified and places them in limbo when they cannot be effectively used by C3PAOs. DoW should issue a class deviation directing The Cyber AB and CAICO to cease all efforts on the CCP and only have the CCA and Lead CCA as the assessor-related certifications under the CMMC program. If DoW would prefer to retain the CCP as an assessor-related certification, then we recommend that DoW take the following Actions:
- ACTION: The Office of Department of War CIO and CMMC PMO should publish a Class Deviation and a memorandum to The Cyber AB directing an interim change to 32 CFR 170.9(b)(12) to read "[C3PAOs shall:] Meet the requirements for Assessment Team composition. An Assessment Team must include at least two people: a Lead CCA, as defined in §170.11(b)(10), and at least one other CMMC Certified individual.
- ACTION: The Office of Department of War CIO and CMMC PMO should take steps to amend 32 CFR 170.9(b)(12) with the language suggested above.
- ACTION: Upon receipt of the memorandum, DoW should require The Cyber AB to publish a Management Decision reflecting the revised language.
- BENEFIT: By empowering the CCP to be a full-blown participant under the supervision of a Lead CCA, this allows the C3PAOs to reduce costs by being able to use a lower cost labor pool in an assessment.

I) Remove the Overstaffing Burden of CCAs for C3PAOs:
- DESCRIPTION: As stated previously, 32 CFR 170.9(b)(12) and 32 CFR 170.9(b)(13) create an onerous burden on C3PAOs that limits our ability to innovate and leverage the best skill sets for the actual requirements. For example, the requirement that the "individual fulfilling the quality assurance function must be a CCA" has no correlation to industry best practices. This function is actually best served by the C3PAO's quality assurance function, as mandated for accredited C3PAOs under ISO 17020:2012. Since the function does not involve a review of the technical aspects of the assessment, the function does not need to be done by a CCA or Lead CCA. The function can be performed by someone with proper quality assurance training from the C3PAO. Furthermore, having someone who is just a CCA may not matter as the person(s) doing this role must also be empowered to affect quality assurance changes in the organization if deviations are found.
- ACTION: The Office of Department of War CIO and CMMC PMO should publish a Class Deviation memorandum to The Cyber AB directing an interim change to 32 CFR 170.9(b)(12) to read "[C3PAOs shall:] Meet the requirements for Assessment Team composition. An Assessment Team must include at least two people: a Lead CCA, as defined in §170.11(b)(10), and at least one other CMMC Certified individual."
- ACTION: The Office of Department of War CIO and CMMC PMO should publish a Class Deviation memorandum to The Cyber AB directing an interim change to 32 CFR 170.9(b)(13) to read "Implement a quality assurance function that ensures the accuracy and completeness of assessment data prior to upload into CMMC eMASS. Any individual fulfilling the quality assurance function cannot be a member of an Assessment Team for which they are performing a quality assurance role. A quality assurance individual shall manage the C3PAO's quality assurance reviews as defined in paragraph (b)(14) of this section and the appeals process as required by paragraphs (b)(19) and (20) of this section and in accordance with ISO/IEC 17020:2012(E) (incorporated by reference, see §170.2) and ISO/IEC 17011:2017(E) (incorporated by reference, see §170.2)."
- ACTION: Upon receipt of the memorandum, The Cyber AB must publish a Management Decision reflecting the revised language.
- BENEFIT: This administrative change frees up the C3PAO to use appropriately trained and qualified staff to conduct the QA function without requiring the function to be performed by expensive personnel. This will lower the COSS to the DIB organization.

J) Make the CMMC Assessment Process (CAP) Informative:
- DESCRIPTION: Given the CAP is a holdover from the CMMC 1.0 construct, it has outlived its usefulness as a document that is micromanaging C3PAOs from both DoW and The Cyber AB. While an informative version is needed for new C3PAOs, The Cyber AB should not dictate the process or steps a C3PAO should follow.

This limits our ability to operate, innovate, and lower costs. Mandated requirements belong in The Cyber AB's R2001: C3PAO Authorization Requirements[xxv] and R2002: C3PAO Accreditation Requirements[xxvi] documents.

- ACTION: The Office of Department of War CIO and CMMC PMO should publish a memorandum to The Cyber AB directing The Cyber AB to make the CAP an informative document only.
- ACTION: Upon receipt of the memorandum, The Cyber AB must publish a Management Decision stating all C3PAOs are to consider the CAP as a informative document until the next version is published.
- BENEFIT: This administrative change frees up C3PAOs to innovate and not be constrained by processes that are not applicable to evolving approaches needed to support small business certifications at the lowest price.

K) Get Rid of CMMC eMASS and its admin burden:

- DESCRIPTION: The DoW's CMMC eMASS creates a significant labor burden on a C3PAO that is passed onto the client as a part of the COSS. For the simplest type of Certification Assessment, the time spent working within CMMC eMASS makes up about 25% of the overall COSS.
  While that may seem surprising, a core issue is that the CMMC eMASS application is subject to changes without any notification to C3PAOs. This forces us to look through and troubleshoot data formatting issues when data is submitted to CMMC eMASS. This is further exacerbated by DoW tying CMMC eMASS and SPRS by CAGE Codes. When an Organization Seeking Certification (OSC) gives us the wrong CAGE Code information, it gets rejected and C3PAOs are not informed. This then forces the C3PAOs' staff to work with the OSC to resubmit the information to CMMC eMASS. The information submitted to CMMC eMASS is further restricted by the C3PAO's confidentiality requirements, which is forcing us to not share all of our specific notes with DoW as the DoW does not have an inherent need to know OSC information that is otherwise part of a business-to-business transaction.
- ACTION: The Offices of Department of War CIO and the CMMC PMO should shut down CMMC eMASS and save the taxpayer funds for an application that benefits the warfighter.
- ACTION: The Offices of Department of War CIO and the CMMC PMO should modify The Cyber AB's contract to require The Cyber AB to establish a DoW searchable database of certifications issued by C3PAOs or for the C3PAOs to establish an independent certification validation mechanism. This would also allow the CMMC program to be easily embraced by federal agencies other than DoW.
- ACTION: Under Secretary of War for Acquisition & Sustainment should direct Contracting Officers to require a copy of all identified OSCs' certificates as a part of the Request for Proposal submission and then validate as needed.
- BENEFIT: Reducing the onerous and bureaucratic reporting process that is manually intensive with an industry provided one will reduce the COSS to small businesses, save the taxpayers monies by not continuing to use CMMC eMASS, and make C3PAOs more efficient.

7. What specific, actionable policy changes or regulatory reforms should the CMMC Reform Task Force recommend over the next 60 days to drastically improve operational resilience against cyber-attacks at your organization?

A) Mandate Jointly Created Security Classification Guides (SCG) for each PoR:

- DESCRIPTION: The biggest challenge the DIB faces is a lack of clarity with the DoW. The challenge is neither understands CUI because CUI starts as requirements in DoW that get developed and delivered via the DIB, where the bulk of the derived CUI exists. This conundrum requires DoW AE/ROs and the Primes to work together to create Security Classification Guides that allow the DIB to develop and deliver CUI down to portion marked aspects that can be built without having to pass down CUI to the micro-small businesses that make up the bulk of our manufacturing base.
- ACTION: Under Secretary of War for Acquisition & Sustainment should direct all AE/ROs and their Contracting Officers to require portion marking of CUI and to develop SCGs that allow for appropriate decontrolling of information that no longer contains CUI as permitted under DFARS 252.204-7012(m).
- BENEFIT: This will allow the DIB to effectively protect CUI where confusion exists currently. This allows the DIB to optimize delivering warfighter capabilities without over-encumbering small manufacturers.

B) Better train DoW Acquisition Executives/Requirement Owners and Contracting Officers:

- DESCRIPTION: While we agree with reducing the CUI training for the vast majority of the DoW, DoW and Defense Acquisition University (DAU) actually need to increase CUI training for personnel in the Acquisition workforce. One of the greatest complaints from the DIB is that Acquisition workforce doesn't understand CUI. This leads to the Acquisition workforce overmarking items as CUI when they aren't. This actually occurred during our DIBCAC assessment as a C3PAO where DIBCAC declared our assessment schedule as General Proprietary Business Information (CUI//SP-PROPIN), which was not the case per the cited

LRGWPs[xxvii]. This lack of understanding of CUI within the DoW creates significant burdens because DIB companies are required to protect information that isn't CUI as-if it is CUI until clarified, and most DoW personnel take offense to such "challenges".[xxviii] When a contractor is brave enough to challenge a CUI designation, the contractor almost never gets a response. This is partly due to the primes and the Acquisition workforce taking CYA actions, since DoW's policies do not currently impose penalties on overdesignation of information as CUI. Enhancd CUI training will also help the DIB with base-level sustainment contracts by educating the Acquisition workforce how to not disseminate CUI to the DIB when they could easily and properly redact and decontrol information.

- ACTION: The Under Secretary of War for Acquisition & Sustainment should direct DAU to work with commercial sector experts that understand CUI, such as Peak InfoSec or the CUI Institute personnel, to develop enhanced CUI education for specific roles in DoW. The commercial sector should be involved in developing this training for the Acquisition workforce because the commercial sector has better visibility into the real-world scenarios that unfold when CUI is jointly used by, and disseminated between, the DoW and commercial entities.
- BENEFIT: Having a properly trained Acquisition workforce that understands CUI beyond the generic biennial training is critical to the success of DoW actually protecting its information in the DIB.

C) Remove the use of CMMC Asset Categories for Scoping

- DESCRIPTION: Contrary to the DoW's beliefs, DIB contractors tend to use the Contractor Risk Managed Asset (CRMA) and Specialized Asset categories as areas to dump whole swaths of their business' assets. This effectively allows the contractor to avoid having those assets assessed and, at least in their perception, exempts them from having to apply NIST SP 800-171 security requirements to those assets. This undercuts operational resilience within the small DIB firms because they are leaving their manufacturing assets more exposed to cyberattacks, such as the cyberattack on Iran's centrifuge's via Stuxnet[xxix]. This also undercuts operational resilience and protecting manufacturing assets when needed to support the warfighter. In reality, fundamental information security principles like least privilege/functionality, applying zero-trust principles, and network segmentation are foundational aspects needed to protect operational resilience, which are also facets under NIST SP 800-171 Rev 2 and 3.
- DoW also has not been delegated the authority to regulate Security Protection Assets or Security Protection Data. This is confirmed in part by Paragraph 9 of ISOO Notice 2020-04[xxx], which states in pertinent part "Agencies may assess only systems and components that an entity uses to store, process, or transmit CUI, and they assess the systems for performance of requirements in the relevant contract or agreement" (emphasis added). Although NIST SP 800-171 indicates that "The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components", neither Executive Order 13556 nor 32 CFR 2002 delegate to NIST any authority to regulate the components that provide security protection[xxxi], and NIST cannot therefore delegate any authority to DoW or any other entity. Instead, the assets in scope for a CMMC certification assessment should simply be defined as assets that store, process, or transmit CUI ("CUI Assets"), and any assets not physically or logically isolated from CUI Assets.
- ACTION: The Offices of Department of War CIO and the CMMC PMO should issue interim scoping guidance that removes the Security Protection Asset, CRMA, and Specialized Asset categories and direct all entities assessing to follow NIST SP 800-171 scoping guidance.[xxxii, xxxiii]
- BENEFIT: This simplifies scoping for organizations, reduces, conflicts during assessments over interpretations, and protects operational resilience against cyberattacks.

We would like to offer the following suggestions to the Office of Department of War CIO and the Under Secretary of War for Acquisition & Sustainment:

A) Clarify your messaging

- DESCRIPTION: DoW and the CMMC/DIB ecosystem have overfocused on the term "CMMC" and, as a result, have comingled implementation of NIST SP 800-171 requirements with *any* 3rd party assessment of the organization's implementation. This has led to a perception battle that may have also mislead the DoW CIO and SBA into believing a NIST SP 800-171 3rd Party Assessment by a C3PAO costs upwards of $600,000.[xxxiv] While CMMC may be the program name, DoW should move away from associating the program's name to the desired security requirement implementation and self-/3rd party assessment requirement.
- ACTION: The Offices of Department of War CIO and the CMMC PMO should change the 32 CFR Part 170, CMMC Model, and other supporting documentation to move away from "CMMC Level 2" to NIST SP 800-171" terminology as the levels are outdated notions from CMMC 1.0.

PEAK INFOSEC
Trusted Guides For Your CMMC Journey
cmmc@peakinfosec.us | www.peakinfosec.com | (352) 575-9737
3001 N. Rocky Point Dr. E, Suite 200, Tampa FL 33607

- ACTION: The CMMC PMO should direct the CMMC eMASS PMO, presuming DoW rejects our previous suggestion to shut down CMMC eMASS, to rename the CMMC tab for CMMC Level 2 to NIST SP 800-171.
- ACTION: The Offices of Department of War CIO and the CMMC PMO should direct The Cyber AB and CAICO to train to the new model. Presuming the DoW CIO retains commercial 3rd party assessments of the DIB, The Cyber AB should also affect changes to the Certificate template used by C3PAOs.
- BENEFITS: This simple clarification will help to separate NIST SP 800-171 "non-negotiable" costs incurred by the DIB expected to be done by the DOW CIO[xxxv] from NIST SP 800-171 implementation costs versus 3rd party assessment costs, whether generated by the Department of Justice (DoJ), DIBCAC, or C3PAOs.

B) Incentivize the DIB to Implement NIST SP 800-171
- DESCRIPTION: Given our cover letter recommendation to extend CMMC Phase I though 10 November 2028, DoW needs to reward and recognize the DIB members that have not invested "in vain"[xxxvi] while other members of the DIB have avoided the costs of implementing NIST SP 800-171 security requirements and some have lied about the implementations. The last phase of the ProSCI ADKAR model[xxxvii] is "Reinforcement" which seeks to ensure that the change is sustained over time. To reinforce their commitment and incentivize the rest of the DIB to follow suit, the DoW should increase their opportunity to win contracts because they have demonstrated their commitment to protect the government's information.
- ACTION: The Under Secretary of War for Acquisition & Sustainment should direct all AE/ROs and their contracting officers to provide greater weight as a Technical Evaluation Criteria for all DIB contractors that can demonstrate 3rd party NIST SP 800-171 compliance via a DIBCAC or C3PAO assessment.
- BENEFIT: Positive reinforcement will incentivize the DIB to keep implementing NIST SP 800-171 security protections. Failing to do so increases the probability that the DIB increasingly "blow-off" NIST SP 800-171 compliance requirements as DoW continues to flip-flop on CMMC and the probability of being audited by DIBCAC is near 0%[xxxviii]. This is considered a business risk and with the likelihood being so low, most of the DIB will continue to ignore NIST SP 800-171 security requirements until something incentivizes them. And those that have heeded DoW's call will increasingly look at lowering their investments to maintain their security posture.[xxxix]

C) DoW Small Business Innovation Research (SBIR) & Small Business Technology Transfer (SBTT):
- DESCRIPTION: The DoW should introduce the requirement to begin implementing NIST SP 800-171 security requirements where an organization is involved in the DoW SBIR/SBTT program. Should the organization proceed to Phase III, the DoW should require NIST SP 800-171 3rd party assessment over a graduated timeline using the prior recommendations for POA&Ms and the Mentor/Protégé. If possible, DoW should look to fund the implementation of NIST SP 800-171 security requirements in Phase II.
- ACTION: The Under Secretary of War for Acquisition & Sustainment should direct the Office for Small Business Innovation to limit NIST SP 800-171 implementation requirements to begin in SBIT/SBTT Phase II and for 3rd party assessment to being in Phase III by not sharing CUI in Phase 1.
- BENEFIT: Incentivizing small businesses to provide innovations to the DoW while building in NIST SP 800-171 security practices into their business model early reduces everyone's costs at the earliest point in a potential new system's lifecycle. But integrating NIST SP 800-171 security requirements, items like secure coding and a Software Bill of Materials (SBOM) are natural results of the existing requirements.

D) Treat this like ISO 9000:2026, AS9100E, and other common certs:
- DESCRIPTION: The current model forces triennial certification cost spikes because the 3rd party assessing organization and the DIB organization must treat the assessment like a brand-new assessment every time. This same cost spike also occurs whenever the DIB company makes a significant change, merges with or acquires another entity, etc. The current model does not normalize these costs, nor does it allow for ongoing validation that the DIB firm is doing what they should. Defense Counterintelligence Security Agency (DCSA) recognized the need for ongoing monitoring as a part of their Facility Clearance (FCL) and Foreign Ownership, Control or Influence (FOCI) reviews. Likewise, DoW recognizes the value in ongoing monitoring for every program that requires an Authorization To Operate (ATO) under eMASS. Allowing C3PAOs to conduct annual surveillance assessments allows DIB organizations to lower their certification cost after their initial assessment. Furthermore, most of the DIB is already used to this approach as it is consistent with other DoW-required industry certifications like ISO/IEC 9000 and ASE 9100. If CMMC eMASS is allowed to persist, its functionality must be enhanced to track this surveillance, as well as "delta" assessments.
- ACTION: The Offices of Department of War CIO and the CMMC PMO should direct The Cyber AB to allow C3PAOs to conduct surveillance assessments and should update CMMC eMASS to recognize them.
- BENEFIT: This lowers the overall certification costs for the DIB that require NIST SP 800-171 3rd party assessments. This also serves as a reinforcement mechanism under the ADKAR model.

COURTESY COPIES

Courtesy Copies of this memorandum were provided to:

- United States Senator Richard Blumenthal (Connecticut)
- United States Senator Chris Murphy (Connecticut)
- United States Congressman John Larson (Connecticut – 1st)
- United States Senator Risk Scott (Florida)
- United States Senator Asheley Moody (Florida)
- United States Congressman Gus Bilirakis (Florida – 12th)
- United States Senator Todd Young (Indiana)
- United States Senator Jim Banks (Indiana)
- United States Senator Chris Van Hollen (Maryland)
- United States Senator Angela Alsobrooks (Maryland)
- United States Congressman Jamie Raskin (Maryland – 8th)
- United States Senator John Fetterman (Pennsylvania)
- United States Senator Dave McCormick (Pennsylvania)
- United States Congresswoman Madeleine Dean (Pennsylvania - 4th)
- United States Congresswoman Nancy Mace (South Carolina – 1st)
- United States Senator Mark Warner (Virgina)
- United States Senator Tim Kaine (Virgina)
- United States Congressman Eugene Vindman (Virgina – 7th)
- United States Congressman James Walkinshaw (Virgina – 11th)
- John L. Vatian, Assistant Chief Counsel, Financial Services and Banking, SBA Office of Advocacy
- Matthew Travis, The Cyber AB
- Todd Gagnon, ISACA/CAICO

PEAK INFOSEC
Trusted Guides For Your CMMC Journey

cmmc@peakinfosec.us | www.peakinfosec.com | (352) 575-9737
3001 N. Rocky Point Dr. E, Suite 200, Tampa FL 33607

ENDNOTES

[i] 32 CFR 170.9(b)(6)(i), "The assessment will be conducted by DCMA DIBCAC." (https://www.ecfr.gov/current/title-32/part-170#p-170.9(b)(6)(i))

[ii] C.f., https://www.ecfr.gov/current/title-32/part-170#p-170.9(b)(3)

[iii] 600 individuals pending Tier 3 divided by 2640 (2040 currently cleared individuals plus 600 individuals pending Tier 3) equals 22.7%

[iv] C.f., https://www.ecfr.gov/current/title-32/part-170#p-170.9(b)(12)

[v] ISO/IEC 17020:2012, para 6.1.5, The inspection body shall have documented procedures for selecting, training, formally authorizing, and monitoring inspectors and other personnel involved in inspection activities.

[vi] C.f., https://www.ecfr.gov/current/title-32/part-170#p-170.9(b)(13)

[vii] C.f., https://www.ecfr.gov/current/title-32/part-170#p-170.9(b)(18)

[viii] C.f., https://www.ecfr.gov/current/title-32/part-170#p-170.17(a)(1)(i)(E)

[ix] ISO/IEC 17020:2026, sub-clause 7.2.5: The inspection methods or procedures shall address:
a) the inspection techniques to be used and, where appropriate, the measurements to be taken, including adequate information on the equipment and facilities to be used; NOTE An inspection scheme can include the methodology to evaluate the uncertainty of the measurement processes.
b) activities for which the inspector's judgement may rely on the use of technology;
c) inspection planning and sampling, where the absence of such instructions can jeopardize the effectiveness of the inspection process;
d) when sampling is relevant to the validity of the outcome of inspection activities, the inspection body shall establish a sampling plan and method; where appropriate, sampling plans should be based on statistical methods; additionally, records of sampling shall be maintained, including details such as the method used, date and time, personnel involved, and any deviations from the plan, to ensure traceability;
e) information supplied by any other party (including the client) as part of the inspection process, and how the integrity and the validity of such information shall be verified to the extent appropriate for the intended use of this information;
f) inspection results from artificial intelligence or digital developments;
g) the use of safety equipment and the rules or instructions for performing inspections in a safe manner;
h) where applicable, the criteria to make the decision on conformity of the inspection item;
i) which particular equipment has a significant influence (if any) on the result of the inspection and when relevant, under which conditions (such as environmental).

[x] C.f., https://cyberab.org/Portals/0/CMMC%20Assessment%20Process%20v2.0.pdf?ver=fEk1pUK1Fg26fVtopxv_DA%3d%3d

[xi] NIST SP 800-171A, para 2.1, "The examine method is the process of reviewing, inspecting, observing, studying, or analyzing assessment objects (i.e., specifications, mechanisms, activities). The purpose of the examine method is to facilitate understanding, achieve clarification, or obtain evidence. The interview method is the process of holding discussions with individuals or groups of individuals to facilitate understanding, achieve clarification, or obtain evidence."

[xii] NIST SP 800-171, Rev 3, 03.07.05 Nonlocal Maintenance

[xiii] NIST SP 800-171 Rev 2, 3.12.3, Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

[xiv] NIST SP 800-171 Rev 2, 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

[xv] C.f., https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information

[xvi] C.f., https://www.ecfr.gov/current/title-32/part-2002

[xvii] C.f., https://aaf.dau.edu/aaf/mca/acat/

[xviii] C.f., https://www.archives.gov/cui/registry/category-detail/ucni-dod

[xix] C.f., https://www.ecfr.gov/current/title-32/part-170#p-170.21(a)(2)

[xx] This is an estimate based on labor plus travel costs.

[xxi] C.f., https://www.ecfr.gov/current/title-32/part-170#p-170.19(c)(2)(ii)

[xxii] 32 CFR 170.9(b)(4), "Require all C3PAO company personnel participating in the Level 2 certification assessment process who are not eligible to obtain a Tier 3 background investigation to meet the equivalent of

a favorably adjudicated Tier 3 background investigation. DoD will determine the Tier 3 background investigation equivalence for use with the CMMC Program only." https://www.ecfr.gov/current/title-32/part-170#p-170.9(b)(4)

[xxiii] 32 CFR 170.9(b)(12), "[C3PAOs shall:] Meet the requirements for Assessment Team composition. An Assessment Team must include at least two people: a Lead CCA, as defined in § 170.11(b)(10), and at least one other CCA. Additional CCAs and CCPs may also participate on an Assessment Team."

[xxiv] 32 CFR 170.9(b)(13), "[C3PAOs shall:] Implement a quality assurance function that ensures the accuracy and completeness of assessment data prior to upload into the CMMC instantiation of eMASS. Any individual fulfilling the quality assurance function must be a CCA and cannot be a member of an Assessment Team for which they are performing a quality assurance role."

[xxv] C.f., https://cyberab.org/Portals/0/Documents/R2001-C3PAO%20Authorization%20Requirements%20JAN2026.pdf

[xxvi] C.f., https://cyberab.org/Portals/0/Documents/ISO17020/R2002-C3PAO%20Accreditation%20Requirements%20JAN2026.pdf

[xxvii] C.f., https://www.archives.gov/cui/registry/category-detail/proprietary-business-info.html

[xxviii] 32 CFR 2002.50(d), "Until the challenge is resolved, authorized holders should continue to safeguard and disseminate the challenged CUI at the control level indicated in the markings." (https://www.ecfr.gov/current/title-32/part-2002#p-2002.50(d))

[xxix] C.f., https://en.wikipedia.org/wiki/Stuxnet

[xxx] C.f., https://www.archives.gov/files/cui/documents/20200616-cui-notice-2020-04-assessing-security-requirements-in-non-fed-info-systems.pdf

[xxxi] C.f., 32 CFR 2002.14(g) and (h) which limit the applicability to only "information systems that process, store, or transmit CUI."

[xxxii] NIST SP 800-171 Rev 2, para 1.1, "The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components."

[xxxiii] NIST SP 800-171 Rev 3, para 1.1, "The security requirements in this publication are *only* applicable to components of nonfederal systems that process, store, or transmit CUI *or* that provide protection for such components."

[xxxiv] C.f., https://www.sba.gov/article/2026/07/13/sba-commends-us-department-wars-suspension-cmmc-phase-ii-small-defense-contractors

[xxxv] "Safeguarding covered defense information remains a non-negotiable legal requirement to deliver critical digital capabilities to our war fighters.", DoW CIO Kirsten Davies, timestamp 00:01:21, https://vimeo.com/manage/videos/1213075635/ef68cebbf5

[xxxvi] "Your investments were not in vain.", DoW CIO Kirsten Davies, timestamp 00:01:01, https://vimeo.com/manage/videos/1213075635/ef68cebbf5

[xxxvii] C.f., https://www.prosci.com/methodology/adkar

[xxxviii] C.f., https://www.linkedin.com/posts/jfarr1_i-understand-this-post-is-going-against-the-activity-7486504007302131712-bYhU/

[xxxix] This approach is consistent with other commonly experienced reinforcement mechanisms in the United States. Police use the threat of tickets, fines and potentially jail time to negatively reinforce people should drive safely while the auto insurance industry gives safe driver discounts.

PEAK INFOSEC
Trusted Guides For Your CMMC Journey
cmmc@peakinfosec.us | www.peakinfosec.com | (352) 575-9737
3001 N. Rocky Point Dr. E, Suite 200, Tampa FL 33607