Information Technology Acquisition Advisory Council

June 14, 2021

CMMC Readiness Assessment

An Independent Assessment of The United States DoD's CMMC Program
In support of GAO's congressionally directed audit

Information Technology - Acquisition Advisory Council **June 14, 2021**

CMMC Readiness Assessment

An Independent Assessment of The United States DoD's CMMC Program
In support of GAO's congressionally directed audit

Why IT-AAC Did This Study

The Information Technology Acquisition Advisory Council (ITAAC) is a public/private partnership of concerned citizens, subject matter experts, public interest groups (SDO, NGO, EDU), private sector sponsors and government partners working together to serve as a catalyst for positive change and evolution in the Information Technology and Cybersecurity domains to meet the challenges of the 21st century.

The IT-AAC mission is to provide Congress, White House, and Executive Branch IT Leadership with a trusted collaborative entity that can provide transformative roadmaps and recommendations for streamlining the IT acquisition process to ensure critical mission elements that are highly dependent on IT (Info Sharing, Cyber-Security, E-Health, E-Gov, E-Biz, and Green IT) are effective. The IT-Acquisition Advisory Council is a 501(C)6 Public/Private Partnership that includes engagement with international governments (NATO/EU), academia, standards bodies, Fortune500 communities of practices and leading national security authorities.

This CMMC Readiness Assessment provides GAO Audit team with significant insights into key challenges and opportunities and offers recommendations to enhance DoD's efforts to increase cybersecurity practices and effectiveness within its Defense Industrial Base.

These findings and recommendations have applied Evidenced-Based Research for its basis of assessment. The CMMC-COE desires to assist in improving both SMB preparation and supporting NATO DIB partners.

Executive Summary

The National Defense Authorization Act for Fiscal Year 2021 (NDAA 2021) directed GAO to conduct a comprehensive audit of DoD's Cybersecurity Maturity Model Certification (CMMC) Program Office and its newly established CMMC-Accreditation Body (CMMCAB.org). GAO has sought input from all key stake holders, including those representing most of the DIB (NDIA), as well as leading cyber standards bodies, international innovators, and leading national security SMEs (IT-AAC). To improve the protection of CUI/FCI data, DoD established a new maturity model, building on NIST 800-171 processes, called the Cybersecurity Maturity Model Certification (CMMC). CMMC evolved from the prior self-attestation provision (DFAR 252.204-7012) to a required set of controls and practices.

IT-AAC is offering comments, findings, and recommendations in six areas of review:

1. Engagement with CMMC program office during CMMC development and/or rollout, including RFI responses, transparency, DFARS clarity, approach to improving DIB Cyber Resilience.
2. Experience conducting assessments of information system cybersecurity and/or consulting companies on improving information system cybersecurity, whether using NIST or some other criteria.
3. Clarity of oversight and governance mechanisms, including security requirements and efforts to ensure consistency of assessments.
4. Quality and availability of resources (e.g., training courses or materials) to support assessment organizations.
5. Perspectives on current CMMC structure and/or implementation timeline.
6. CMMC and its relationship with the DIB's global supply chain partners.

Having launched the CMMC-Center of Excellence in June of 2020, building out IT-AAC's international partnership network, the IT-AAC was able to pull together stake holder inputs from across the tens of thousands of SMBs, leading SDOs/NGOs, and gain insights from our NATO allies who offered objective insights on CMMC strengths and weaknesses. Key recommendations from IT-AAC's comprehensive review are as follows;

- DoD can SMB CMMC implementation burden by leveraging mature capabilities of established cybersecurity non-profits, standards and accreditation bodies. Standing up a new AB entity with inexperienced volunteers was mistake and should be rethought.
- As DFARS flow down from Primes to subs already, consider empowering these relationships to bolster cyber hygiene for SMBs who lack expertise and resources.
- Establish a whole of government cyber reference architecture by leveraging existing standards bodies and Public/Private Partnerships
- CyberSecurity standards should remain in the control of DoD CIO and NIST. The CMMC PMO may also need a new home where deeper cybersecurity skills exists.
- Automation is key to sustainable cyber resilience; including continuous monitoring, sensor nets, and establishing a shared secure enclave that will reduce cost and risks.
- DOD should consider leveraging the CMMC-COE to support International DIB partners, innovators and SMBs prepare, remediate and modernize to meet CMMC and related Cybersecurity Standards. This allows the AB to focus on 3PAOs and Certification needs without OCI.
- The new Cyber EO directs DOD to work with Industry NSC, NATO and Civil Agencies to establish a broad Cybersecurity Reference Architecture that allows dynamic mapping of threats to proven technical solutions.

TABLE OF CONTENTS

.....2

1 CMMC, an Introduction to DIB CyberSecurity 4

1.1 GAO CMMC Audit Methodology 5

2 OUSD A&S CMMC PMO 5

2.1 Engagement with CMMC program office during CMMC development and/or rollout 5

2.2 Recommendations for improving CMMC Program Office Engagements.....6

3 CMMC Certification 7

3.1 The Current Certification Methodology for Auditors, Trainers and Registered Consultancies lacks rigor and fails to address international demands. 7

3.2 Recommendations for improving effectiveness and efficiency of companies conducting assessments of information system cybersecurity and/or consulting 7

4 CMMC Oversight and Governance 8

4.1 Clarity of oversight and governance mechanisms, including security requirements and efforts to ensure consistency of assessments 8

4.2 Recommendations for improving Clarity of oversight and governance mechanisms, including consistency of assessments 9

5 CMMC Support Contractors; SEI CERT, JHAPL, CMMC-AB 9

5.1 Quality and availability of resources (e.g., training courses or materials) to support assessment organizations. 9

5.2 Recommendations for improving Quality and availability of resources (e.g., training courses or materials) for Assessment Organizations. 10

6 CMMC Implementation timeline.....10

6.1 Perspectives on current CMMC structure and/or implementation timeline.....10

6.2 Recommendations for improving CMMC structure and/or implementation timeline.....11

7 CMMC Support of Global Supply Chain: NATO 12

7.1 How CMMC is addressing Global Supply Chain Partners (i.e., NATO). 12

7.2 Recommendations for improving Global Supply Chain Partners (i.e., NATO) 12

8 Critical Success Factor for achieving and improving DIB Cybersecurity Maturity 13

8.1 Summary of IT-AAC recommendations for improving Global Defense Supply Chair Cyber Resilience: 13

IT-Acquisition Advisory Council (IT-AAC)
John.weiler@IT-AAC.org 703-863-3766

1 CMMC, AN INTRODUCTION TO DIB CYBERSECURITY

The aggregate loss of Controlled Unclassified Information (CUI) from the Defense Industrial Base (DIB) sector increases the risk to our national economic security. To reduce this risk, the United States Department of Defense (DoD) must continue working with the DIB and Cyber Communities of Practice to enhance its protection of CUI in the DoD unclassified networks.

The DOD CIO in 2015 commissioned NIST promote innovation and industrial competitivene the DIB with NIST, issuing special publication (SP) 800-171 to store, process, or transmit Controlled Unclassified Information (CUI) and provide adequate security to protect the covered defense information (the NIST SP 800-171 standards are based on the Federal Information Security Management Act of 2002 (FISMA) moderate level requirements).

After determining that self-attestation was not reliable, in early 2018, OUSD A&S established a Cybersecurity Program Office and contracted initially with JHAPL to build out 800-171. Later on, SEI CERT was contracted to establish an auditable maturity model called CMMC, issuing its first public release of CMMC v.04 in early September 2019. Soon after, the PMO conducted multiple industry interchanges before issuing an RFI seeking industry insights on how it could rely on a 3rd-party to manage accreditation and certification of this mandatory standard. With over 50 proposals responding to this RFI, the PMO widely expected that DOD would leverage an existing standards body that would embrace this new "standard" and establish a robust certification and accreditation operation. Instead, the new PMO decided it would direct the creation of a new entity called the CMMC-Accreditation Body that would be stood up by a team of volunteers, including the IT-AAC's executive director, John Weiler.

Under direction of the PMO, the new CMMC Advisory Board (CMMC-AB) was kicked off on November 19, 2019. In early 2020 Ellen Lord, OUSD A&S, signed an MOU with this Maryland based non-stock corporation that gave it exclusive authority over all CMMC certification and accreditation activities. Months later, the MOU was replaced with a sole source, no-cost contract that expanded DOD's control of the AB and increasing its ability to dictate inherently governmental functions. It would not be until February 2021 that the AB would file with the IRS for non-profit 501C3 status. The AB struggled with governance and transparency since its inception, leading Congress to require a full GAO audit in the 2021 NDAA. DOD also sought an independent Industry Advisory Council outside of the AB.

This report is the IT-AAC's response to GAO's request for input from key stakeholders. The IT-AAC's mission is to provide policy recommendations and guidance on issues impacting governments and industry in Information Technology, Cybersecurity, and acquisition. To facilitate this the IT-AAC engages with NATO allies, Standards Bodies, Cyber Innovators, and many small/medium businesses. Working with its partners, the ITAAC provides guidance for Industry and Government on how to prepare for these emerging cybersecurity and supply-chain protection and resilience requirements. IT-AAC believes that by engaging with cybersecurity experts and through the adoption of modern automated cybersecurity controls it will be possible to secure the DoD supply chain. The best practices and recommendations we suggest here will help address the aggregate loss of CUI and provide competent support for SMB's and the DIB.

IT-Acquisition Advisory Council (IT-AAC)
John.weiler@IT-AAC.org 703-863-3766

1.1 GAO CMMC Audit Methodology

GAO has been tasked with completing a congressionally directed audit of the CMMC program, and has tapped both NDIA and IT-AAC to gain insights from the widest range of DIB stakeholders. GAO's audit methodology includes a multidimensional review of both the CMMC PMO and its Accreditation Body in terms of transparency, governance, effectiveness and trustworthiness. IT-AAC's response is organized into GAO's study areas;

1. Engagement with CMMC program office during CMMC development and/or rollout, including RFI responses, transparency, DFARS clarity, approach to improving DIB Cyber Resilience.
2. Experience conducting assessments of information system cybersecurity and/or consulting companies on improving information system cybersecurity, whether using NIST or some other criteria
3. Clarity of oversight and governance mechanisms, including security requirements and efforts to ensure consistency of assessments.
4. Quality and availability of resources (e.g., training courses or materials) to support assessment organizations. DAU has already initiated training for Acquisition professionals.
5. Perspectives on current CMMC structure and/or implementation timeline.
6. How CMMC is addressing Global Supply Chain Partners (i.e., NATO).

The IT-AAC represents a wide range of cybersecurity stakeholders including: Small Medium Businesses (SMB), International Standards Bodies (SDOs), NATO DIB suppliers, and cybersecurity innovators/solution providers. IT-AAC has made significant investments to complement the work of the PMO, AB and SEI CERT, and stood up the CMMC Center of Excellence (CMMC-COE.org) to leverage the significant investments of IT/Cyber standards bodies and industry communities of practice that would collectively serve as a resource for SMBs and Innovators seeking a role in the CMMC ecosystem. The following sections reflect the significant insights of the IT-AAC public/private partnership and its international CMMC-COE affiliates.

2 OUSD A&S CMMC PMO

2.1 Engagement with CMMC program office during CMMC development and/or rollout

In the early days of CMMC concept development, the OUSD A&S PMO was deliberately inclusive and collaborative with key stake holders and industry groups, gaining buy in from leading standard bodies, Defense Trade Groups and other NGOs supporting the public sector. DoD held numerous industry days and issued a broad request for information that many responded to in good faith.

Unexpectantly, OUSD A&S did not consider the many industry proposals responding to DOD's 2019 RFI. In these comments, questions were raised as to the quality of market research and the business case DOD decided used to create a brand-new AB entity. Soon after the launch of the CMMC-AB in November 2019, access to the DoD PMO became challenging. The PMO sought to limit who from the AB could engage the PMO, while forcing industry to work exclusively with the AB. Efforts to reach

IT-Acquisition Advisory Council (IT-AAC)
John.weiler@IT-AAC.org 703-863-3766

the two contractors hired to build out the CMMC "standard", JHAPL and SEI CERT were also constrained, creating not only a bottle neck, but also undermining transparency in decision making.

During the first six month of operation, the CMMC AB leadership was only granted two meetings with the PMO, and the PMO also restricted AB access to DOD's support contractors SEI CERT and JHAPL. By June of 2020, a six of the founding board members resigned following the removal of two AB officers accused of violating ethics rules associated with an attempted "pay to play scheme" to raise funds that was apparently approved by the PMO but not the full board.

The appointment of four individuals into the PMO office who further lacked experience in Cybersecurity, Third-Party Risk Management, On-Site Assessments, or Maturity Models also raised concerns among members of the AB.

Despite shortcomings, many of the AB members continued to dedicate large portions of their time to this important goal. Questions addressed to the PMO by the AB regarding timing, scope and funding models were rarely answered. While the AB struggled with gaining access to the PMO, it was clear that the PMO was communicating with potential CMMC Prime contractors as well as trade associations. This left the SMB, standards bodies, NATO allies, and innovators on the outside and without a voice.

OUSD A&S PMO knew the DFAR would need to be supplemented, and many hoped for a comment period prior to issuing an interim DFARS ruling. Instead, the PMO skipped the comment period and issued an emergency DFARS without industry input. This approach drew much condemnation from various groups and resulted in over 200 comments on the ruling. To date, the PMO has yet to respond to either the initial 2019 RFI nor the comments on the interim DFARS ruling.

DoD has outsourced many of the responsibilities of engaging industry to the CMMC-AB. The AB has established a set of CMMC working groups that would allow external stake holders to engage in policy and standards decision making. The AB also started a monthly Town Hall, often with 3rd parties who had a vested interest in future implementations. Unfortunately, most of these were one-way communications with and the AB has failed to respond to many industry questions.

The IT-AAC represents many DIB CyberSecurity stake holders, including several former AB members, and therefore can provide the GAO, Congress, and Pentagon leaders with unique and relevant perspectives on collective industry challenges with the current implementation strategy seeking to improve DIB CyberSecurity. In an effort to address some of these shortcomings, the IT-AAC launched the CMMC Center of Excellence (CMMC-COE.org) to meet the needs of underserved stake holders including Small Medium Businesses, Cybersecurity NGOs & SDOs, NATO allies and emerging innovators. Reliance on a single NGO entity to manage all aspects CMMC ecosystem has proven to be a root cause and must be addressed.

2.2 Recommendations for improving CMMC Program Office Engagements

Staff in the CMMC PMO must have proper cybersecurity training and/or experience. As the owners of the foundational standard are DoD CIO and NIST, it would be logical to return management of the

CMMC standards to the DoD CIO where the needed expertise in SCRM resides. SEI CERT support would shift from OUSD A&S to DoD CIO with little disruption.

IT-AAC applauds the DoD CIO work on complementary SCRM frameworks, which are necessary extensions to the CMMC standard in response to recent SolarWinds, MSFT Exchange, and Colonial Pipeline breaches. Though some have suggested the CMMC standard change to meet these constantly evolving threats, this would not be advised as it would undermine any training or DIBCAP certification efforts already underway. What is needed is a larger CyberSecurity Reference Architecture that supports a Whole of Government approach, vs a one size fits all approach. DOD must partner with the full range of stakeholder NGOs and SDOs and not limit communications to just Primes.

3 CMMC CERTIFICATION

3.1 The Current Certification Methodology for Auditors, Trainers and Registered Consultancies lacks rigor and fails to address international demands.

Experience matters most. The current approach developed by the OUSD A&S PMO and implemented by the CMMC-AB has been characterized as a "pay-to-play" scheme by multiple press outlets and industry partners. Today, the PMO and the AB have been more focused on maximizing number of auditors (3PAOs), Trainers (LPPs) and Registered Consultancies (RPOs).

Currently, the only criteria for being included in the CMMC AB Marketplace is a costly registration fee and completing an online training course. Some companies entering in the AB's marketplace are highly qualified, having existing NIST 800-171 and/or FEDRAMP support offerings. However, feedback from many DIB contractors tell a troubling story of incompetence and flawed recommendations on possible cyber tools suites that lack any approval process.

There are emerging industry efforts (CMMC-COE) to provision DIB supply chain entities who operate within the NATO alliance but operate outside the US. By failing to support in country resources and tools to attain CMMC compliance preparation or certification for these organizations, the Global Supply Chain for DoD is directly compromised. The SOW with the AB disallows US based 3POAs and RPOs to operate outside the US, which is why the CMMC-COE was established. Unfortunately, without support from the PMO who has also restricted interaction with the AB the CMMC-COE will not be able to fulfil this requirement.

3.2 Recommendations for improving effectiveness and efficiency of companies conducting assessments of information system cybersecurity and/or consulting

IT-AAC and its CMMC-COE has already initiated multiple mechanisms for improving the efficiency and effectiveness of CMMC auditors, consultants and solution providers serving both US and NATO allies, some of which are already operational and only need DoD recognition.

The IT-AAC recommends building on the work of DAU, Capital Tech University, CompTIA. itSM, and other CMMC-COE partners who have made significant investments to fill the gaps left by the limited online training provided by the CMMC-AB and PMO office. Training content must also be modified to address tangential cybersecurity risks exposed by SolarWinds and MSFT Exchange Hacks. Capital Tech University, itSM, and CompTIA have a Global Reach and would welcome additional partners to scale up to the significant demand.

DCMA/DIBCAC has the expertise to audit future 3PAOs but cannot scale today without the support of leading Cybersecurity experts, institutions and related trade groups. DCMA self-attests that they can conduct one (1) CMMC Level 3 assessment on a candidate C3PAO once every 6-8 weeks. With hundreds of C3PAOs in the queue awaiting their turn for assessment, this lack of scalability will only lead to tremendous first-mover advantages for the few who get certified first. Today, IT-AAC, NDIA and AFCEA have launched their own awareness programs outside the current CMMC-AB offerings. As each of these entities already have official DoD agreements, it would be wise for DoD to offering some standardization on these training programs to ensure quality and access.

4 CMMC Oversight and Governance

4.1 Clarity of oversight and governance mechanisms, including security requirements and efforts to ensure consistency of assessments

Currently there has been very little oversight or governance exercised by the PMO since launching the Accreditation Body. Numerous claims of conflicts of interests, self-dealing and mismanagement have gone unaddressed, resulting in numerous DoD IG filings and negative press seeking some level of accountability. https://rmf.org/2020/10/12/cmmc-ab-proposes-pay-to-play-program/

In congressional testimony, the PMO has claimed the cost of CMMC on the DIB will have a limited budget impact by setting up industry run certification program. Yet, the allowable cost provision in the DFARS rule that allows contractors to be reimbursed for the additional cost of CMMC compliance could reach up to $60bn over the next five years, with a significant portion of the cost covered by tax payer funds. PMO estimates that CMMC level 1 would only cost a few thousand dollars, evidence gathered from early adopters are suggesting a ten fold increase, and major impediment to SMBs. A recent IPC report explains these challenges; https://emails.ipc.org/links/IPC-CMMC-Report-June2021.pdf

A review of the CMMC-AB marketplace, along with some marketing programs reveals a free-wheeling market that is driven more by greed than by national security interests. Multiple AB board members are offering various CMMC capabilities including training, mentoring, preparation and technical solutions. Each board member was required to sign an ethics agreement that appears to be completely ignored by some. This undermines the public trust and raises the risk for DoD as well as the DIB who may not be equipped to judge the relative quality or efficacy of those in the CMMC-AB marketplace. Current AB vetting of registered 3PAOs and RPOs are done without effective oversight or quality control, leading to numerous false claims by companies who lack proven expertise.

4.2 Recommendations for improving Clarity of oversight and governance mechanisms, including consistency of assessments

DoD needs a better assessment guide that is supported by automation and artificial intelligence (AI). This challenge is way too critical to leave to human error or incompetence. At this juncture, it is widely believed that DIB cybersecurity readiness will not improve under current CMMC-AB certifications. Funds being spent on CMMC certification would be better spent on Zero Trust and compliance automation. There are already several continuous monitoring solutions on the market today. These continuous monitoring solutions could easily allow a CMMC Level 1 assessment to take place almost virtually for most of the companies in the DIB. The cost of these virtual assessments could be covered by the DoD or, since their individual cost is quite low, covered by the DIB company. With most DIB companies expected to achieve CMMC Level 1, these technological solutions will expedite the process of moving the DIB as an entirety up to CMMC Level 3. DOD needs to embrace the work of well established and proven non-profits like CREST-APPROVED, Comptia, Parava, SEI CERT and other CMMC-COE partners offering to scale CMMC and support the SMB community.

5 CMMC Support Contractors; SEI CERT, JHAPL, CMMC-AB

5.1 Quality and availability of resources (e.g., training courses or materials) to support assessment organizations.

The current CMMC framework is clear, well documented, and reflective of a solid standard targeting the control of CUI and FCI data. Yet, neither SEI CERT nor JHAPL have been tasked with training or preparing 3PAOs who will be performing most of the audits (DCMA is the other source). Missing from the concept of operations are quality controls, audit guides, case studies and automation tools that can improve quality and consistency of implementation. This shortcoming is clear when looking at the number of 3PAOs who have passed the required DCMA audit (only 2 at the time of this writing).

OUSD A&S PMO has met with well-established Accreditation Bodies including A2LA and ANSI ANAB, but nothing has been put in place to improve the ability of 3PAO's to achieve DCMA accreditation. When modeling the number of contractors and rate of training/certification of 3PAOs, the best-case scenario forecasts completion of DIB compliance well past 2030.

Regarding organizations supporting preparation, or RPOs, the quality controls and potential conflicts of interests are much graver. ISO guidelines prohibit any accreditation body from running both preparation and certification programs. The ISO standard requires a completely different entity to focus on preparation and automation of the pre-audit activities. It is estimated that 80% of all costs are in the preparation and technical remediation activities, which are out of scope of the SOW signed between DoD and the CMMC-AB.

IT-AAC recognized this preparation and remediation gap when setting up the CMMC-COE's International Public/Private Partnership. As DoD claimed it supported a self-organizing non-profit, the

evidence suggests it seeks to tightly control all activities despite the negative consequence of providing the CMMC-AB with both preparation and certification power . Examples include:

- Assigning the creation and maintenance of the CMMC Assessment Standard to the CMMC-AB in signed and agreed to MOU – only later in the replacement SOW, DOD take back control of the "standard". Clearly, DOD PMO did not embrace a truly independent body, and sought greater control that would stifle operations and innovation.
- Asking for an ISO certified, independent accreditation body in both the RFI and MOU – then demanding oversight of AB finances, contracts, etc. when executing the replacement SOW. At this writing, it is still unclear how the AB will achieve ISO certification, and mitigate conflicts of interests arising from its attempt to control and "certify" both audit and preparation contractors, creating a serious conflict of interests that ISO will not approve.

5.2 Recommendations for improving Quality and availability of resources (e.g., training courses or materials) for Assessment Organizations.

DoD should be promoting alternative CMMC resources as this will contribute to high quality, better security, and availability of CMMC products and services. Several organizations have initiated CMMC/NIST 800-171 training programs in cooperation with the IT-AAC and its CMMC-COE. This will benefit the US SMB market, as well as NATO allies and their DIB suppliers.

NDIA, CompTIA, and other IT-AAC public/private partners are rolling out an international program designed to address the knowledge and expertise gaps. IT-AAC is also in discussions with NATO NCI and ENISA to improve global cybersecurity standards coordination and collaboration. On the quality front, IT-AAC has teamed up with the internationally recognized accreditation body CREST-APPROVED, that is highly regarded in the cybersecurity certification space. IT-AAC recommends an adaptation of the CREST-APPROVED framework to support CMMC and ensure higher quality standards. OUSD A&S Small Business Office should also Project Spectrum participation to include a less restrictive set of stake holders. The contracting process should be transparent and take advantage of existing cybersecurity Public/Private Partnerships.

6 CMMC IMPLEMENTATION TIMELINE

6.1 Perspectives on current CMMC structure and/or implementation timeline

The significant struggles in rolling out the CMMC program suggests a misalignment of resources within OUSD A&S, and diminishes the role of both DOD CIO and NIST. The cybersecurity expertise required of the PMO necessitates a move to an entity with deep cybersecurity expertise. The DoD CIO

IT-Acquisition Advisory Council (IT-AAC)
John.weiler@IT-AAC.org 703-863-3766

office would be the most logical place or Intergovernmental Domains like the U.S. Department of Commerce (NTIA/NIST) or DHS CISA.

The outsourcing of CMMC to a newly formed entity creates unneeded complexity and additional oversight that has caused a disruption in securing the DoD supply chain. With only two 3PAOs certified by DCMA, the timelines for achieving widespread CMMC compliance will stretch into 2030 at an estimated cost of some $60 billion. In addition, a once every three-year audit gives no assurance of true cyber resilience. This is not a productive, efficient, or effective strategy for Zero Trust and Continuous Monitoring. This was a key take away from the RAND report on DIB CyberSecurity published in late 2020; https://www.rand.org/pubs/research_reports/RR4227.html

6.2 Recommendations for improving CMMC structure and/or implementation timeline

The IT-AAC concurs with the views of the Honorable Frank Kendall III, as explained in a Forbes Magazine Op-ed on CMMC that DoD's sole source contract with the non-stock CMMC-AB corporation should be cancelled for cause, with inherently governmental functions brought back in to the Government. Minimally, DoD should limit the CMMC-AB operations on establishing and mentoring 3PAOs per ISO guidelines and the initial MOU and with its own charter. This will allow other viable cybersecurity public interests concerns to fill the gaps, meet market needs and accommodate both international partners and SMBs who are not equipped to meet the demands of CMMC compliance. Frank Kendall's Forbes article on CMMC can be found; https://www.forbes.com/sites/frankkendall/2020/04/29/cyber-security-maturity-model-certificationan-idea-whose-time-has-not-come-and-never-may/?sh=7bede32f3bf2

The current strategy for rolling out CMMC certification will not scale to address the hundreds of thousands of small businesses that need to achieve and maintain the CMMC standard. Furthermore, DoD's assertion that companies are already following either the lower level DFARs cybersecurity clause or NIST SP 800-171 clause – and will therefore require little to no investment to achieve the correct CMMC Level certification – does not account for the lack of 3PAO's available to perform certification, or the cost of the certification itself. If this gap is too large to span – many companies will simply opt out of Defense contract work – further reducing the overall resilience of the DIB and DoD's access to market innovation. Several industry groups have received push back from DOD when seeking to establish programs for their stake holders, including IT-AAC with its launch of the CMMC-COE. DOD should be embracing these efforts to scale and support SMBs, which today has not been the case. Here is a powerful report from a consortia of universities concerned with the cost of CMMC in its current form; https://www.aau.edu/key-issues/aau-associations-urge-defense-department-consider-consequences-cmmc-implementation.

IT-Acquisition Advisory Council (IT-AAC)
John.weiler@IT-AAC.org 703-863-3766

7 CMMC SUPPORT OF GLOBAL SUPPLY CHAIN: NATO

7.1 How CMMC is addressing Global Supply Chain Partners (i.e., NATO).

As noted earlier, the current CMMC implementation plan is significantly deficient in its accommodation of International DIB partners, leading some members of the Five Eyes to abandon CMMC altogether. A recent memo by the UK MOD details how, in its role as the UK designated Security Authority, the MOD requires US defense contractors which supply the UK and US to request modifications to the US DoD contracts under DFARS. This has the potential to jeopardize CMMC oversight of the UK DIB because CMMC does not make provisions for allies to implement the framework. The failure to address reciprocity of cyber security between the US and partner nations for the CMMC program highlights its ineffectiveness in regard to the international supply chain.

US partner nations adopt different cyber security standards, usually ones which are of a lower standard than NIST SP 800 – 171. The US, by requesting that other nationas adopt NIST standards, will create a 2-tiered approach to cyber security which needs to be considered and managed by the DoD, either though reciprocity or by making clear that DoD is the customer requiring these standards. This action would push nations to further adopt these standards as a commercial compliance decision. The UK MOD memo can be found here; https://www.gov.uk/government/publications/industry-security-notices-isns/compliance-with-cyber-security-requirements-from-other-nations

Our global adversaries will attack the softest target they can identify. If that target happens to be in another country, it is all too easy for an adversary to target them since cyberspace has no national boundaries.

7.2 Recommendations for improving Global Supply Chain Partners (i.e., NATO)

The IT-AAC, and its global network of CMMC-COE affiliates has established in-country offices to serve, and support expanded implementation of CMMC across our NATO alliance. To be effective, DoD should consider the following actions to continue international DIB participation;

1. Leverage the CMMC-COE NATO partner network that has established in country resources to ebable training and mentoring of non-US suppliers.
2. Work to broaden the recent Executive Order that directs agencies to embrace Public/Private Partnerships to enhance Cybersecurity standards on an international basis. CREST-Approved has already made programs in this space available.
3. Leverage the existing IT-AAC partner network to further CMMC reciprocity discussions with UK MOD, NATO NCI, ENISA, and related initiatives.
4. Support international CMMC/Cybersecurity training programs being developed by Capital Tech University and CompTIA who already have global reach.

IT-Acquisition Advisory Council (IT-AAC)
John.weiler@IT-AAC.org 703-863-3766

8 CRITICAL SUCCESS FACTOR FOR ACHIEVING AND IMPROVING DIB CYBERSECURITY MATURITY

Looking at the goals of CMMC, revisiting the original concept of operations is helpful as a guidepost in creating an updated entity that would be primarily focused on compliance and certificate issuance.

DoD has made important investments in improving DIB Cybersecurity with the implementation of NIST 800-171, 800-53, and more recently 800-161. Creating an auditable cybersecurity maturity model was desirable as these process investments addressed the shortcomings in self-assessment and self-attestation. However, the rush to put CMMC into operations resulted in challenges that now must be addressed for the desired original outcomes and goals can be realized. The primary challenge is change management and collaboration, and the IT-AAC believes the original end-state is still achievable under the right PMO leadership. Most in industry agree and seek an effective governance model to achieve holistic compliance CMMC mission objectives.

During the past 12 months, most agree that the previously sole-source contract with an entity that has small staff support, limited experience, and poor infrastructure created newer problems, without addressing the desired outcome. It is recommended that DoD reconsider its approach to education, preparation and CMMC certification, and this updated approached not be exclusively controlled by a single body called the CMMC-AB.

This CMMC Readiness Assessment offers high-impact change management recommendations that OUSD A&S, DoD OCIO, and NIST can consider achieving increased significant return on investment and cost savings in the near term. This recommendation focuses on actionable items in areas of process improvement, workforce development effective management and leadership, as well as perceived cultural impediments that can be addresses to drive greater cybersecurity resilience in the U.S. Defense Industrial Base and NATO allied countries.

The June Copy of NDIA's National Defense Magazine was dedicated to CMMC program and is a valuable reference for GAO's Audit effort. This is one of many hard hitting articles and is a must read; https://www.nationaldefensemagazine.org/articles/2021/5/28/industry-hopes-cmmc-review-leads-to-tweaks

DOD must embrace its many critics and collaborate with its many stake holder associations, non-profits, standards bodies and other communities of practice. Only the "Big Six" seem to have unfettered access.

8.1 Summary of IT-AAC recommendations for improving Global Defense Supply Chair Cyber Resilience:

Stepping back from the narrow focus of improving CMMC shortcomings, the IT-AAC team suggests that GAO and DOD consider making some near term changes that would significantly improve implementation success while reducing the significant burden imposed on SMBs who are already struggling with the economic impact of COVID.

1) DOD should reissue or modify the no-cost contract with the CMMC-AB to:

i) Restrict the AB authority to just 3PAO management, training and certification.

ii) Eliminate the AB's marketplace that has become a pay-to-play construct allowing untrusted resources in to sensitive security areas.

iii) Restrict the AB's ability to use its monopoly power to harm and interfere with other parties working in the CMMC ecosystem.

iv) Enforce the AB code of ethics that would prohibit unfair competition by Board members.

2) Migrate the CMMC PMO out of OUSD A&S and into an office that is equipped to manage cybersecurity throughout the DIB. We recommend DOD CIO, NIST or DHS CISA who could build CMMC into a whole of government approach.

3) Update interim DFARS rules to reduce compliance mandates on SMBs and put greater onus on Prime Contractors to support subcontractors via shared secure CUI/FCI enclaves that government can partially reimburse. Primes have great opportunity for achieving economies of scale and this should be encouraged.

4) Leverage the significant capabilities of the IT-AAC and CMMC-COE partners. Select and fund specific automated technological solutions that address the identification and remediation of cybersecurity risk within the DIB. Some options could include such technologies as continuous monitoring solutions or third-party assurance platforms. The emphasis should be on secure and cost-effective cloud instances where DIB companies can keep sensitive data.

5) IT-AAC, and other industry groups, have initiated significant efforts to support cyber preparation and remediation for small and medium sized businesses preparation and sustainment activities with its CMMC-COE initiative, but lacks official support from DOD due to its exclusive arrangement with the CMMC-AB. Small, Medium Businesses need mentoring, coaching, preparation assistance, training and other activities that will not only enable them to achieve the correct CMMC level for their contract but to maintain it in the years between assessments. This is a gap that the AB cannot fill and is outside of the AB charter to be "laser focused on certification and accreditation".

Given the increased risk to the DIB supply chain, and the potential negative impact on SMBs who are already struggling with the cost and effort of doing business with DOD, we strongly recommend the DOD and Congress recognize the significant gaps in the current approach and take full advantage to the robust Cybersecurity ecosystem of trusted standards bodies, innovators and NATO partners who have rallied under the IT-AAC's public/private partnership and the CMMC-COE.org. We thank our esteemed members of Congress and GAO for their efforts to address these important issues and stand ready to help fill these gaps.

IT Acquisition Advisory Council (IT-AAC.org)
CMMC Center of Excellence (CMMC-COE.org)
A Public/Private Partnership managed by;
the Interoperability Clearinghouse (ICHnet.org)
904 Clifton Drive
Alexandria, Virginia 22308, USA