OPINION PAPER:

THE PATH FORWARD FOR THE CMMC ACCREDITATION BODY AND THE CYBERSECURITY MATURITY MODEL CERTIFICATION SCHEME

---

17 September 2020
r0

Christopher Paris
Founder, Oxebridge Quality Resources International LLC
Tampa FL USA
chris@oxebridge.com

Intended for public release and circulation.

PREAMBLE

Few will argue that the security of the United States against cyberthreats is a critical issue, and never more critical than now. The US Dept. of Defense recognizes this, and has mandated that one means of shoring up the nation's defenses in this area will be the Cybersecurity Maturity Model Certification (CMMC) program. Under this scheme, defense contractors and others will be audited against the CMMC standard (called the "model") and receive a CMMC Maturity Level rating. These ML ratings will then be used to determine a contractor's likely suitability to receive government contract awards, with the assumption being that a CMMC rating will indicate the company has reasonable, standardized controls in place to prevent breaches, data loss and unauthorized data access. The higher the Maturity Level, the more controls that the company is likely to have.

To this end, the DoD established the CMMC Accreditation Board (CMMC-AB), and tasked it to oversee this scheme. Unfortunately, DoD then made two primary errors. First, it declined to fund the CMMC-AB, forcing it to find creative ways to fund itself. Next, DoD ignored the nation's 40-year history of accredited certification schemes, and thus has fallen into the trap of repeating the errors of the past.

The CMMC-AB now finds itself mired in controversy, and facing public calls for reformation before the CMMC certification program even fully launches. Some have called for the entire CMMC program to be scrapped, and replaced with an enhanced version of NIS 800-171. This paper will not go into those controversies, but instead will provide a path forward for both the CMMC scheme and the CMMC-AB, based on decades of American accreditation experience and long-established and accepted accreditation standards.

ACCREDITATION vs CERTIFICATION

Much of the confusion in this area comes from a general misunderstanding of the terms "certification" and "accreditation." Both the DoD and the CMMC-AB have revealed their lack of understanding of the concepts by conflating them or treating them as synonyms. They are not.

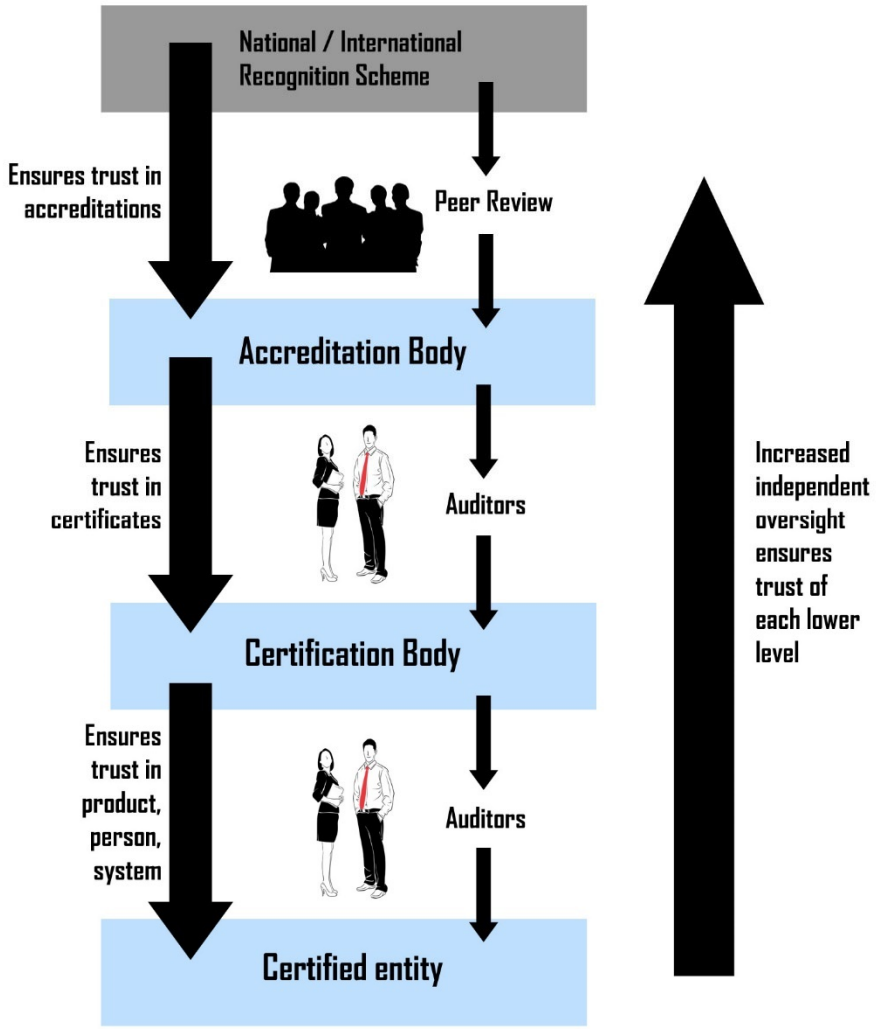
Essentially, there is a simple hierarchy: "accreditation" is a higher form of authentication and sits over "certification." They are not the same thing, and cannot be performed by the same body.

Both terms relate to the concept of "authenticated verification" of a thing. They aim to provide confidence that said thing – whether a product, a company, a person or a practice – meets certain standards because it has been assessed by a recognized, authorized and independent body. That is where the similarities end.

"Certification" relates to the assessment of the thing and issuance of a certificate attesting to its compliance with a certain standard. A university degree or diploma is the most widely known "certificate" within daily life, although people are surrounded by certified products and services without knowing it. Electrical cords are "UL Listed," as they are certified to certain electrical standards; foods are certified as "organic" or "Kosher" to comply with related standards. The examples go on and on.

"Accreditation" sits above certification, and aims to distinguish true, objective certifications from those issued by fly-by-night "certificate mills." In the higher education scheme, a person may get a university diploma from an accredited university, such as Yale or Harvard, or they can buy a degree from the website of some unaccredited company operating on an uncharted island. Likewise, people can buy properly-certified electrical or medical devices, or they can buy counterfeit product from Chinese black market operators.

In food schemes such as Kosher or organic, an over-arching Accreditation Body acts to ensure the inspection bodies only issue certificates to foods that meet the applicable standards. This is to prevent foods from reaching the market that do not comply, but where the producer may have bribed or otherwise influence the inspection body.



The reality is that throughout the world, companies self-attest or "certificate mills" issue wholly invalid certifications that do not truly ensure the quality of the thing being certified. ***Accreditation provides the distinction.*** Accreditation means the Certification Body (CB) has undergone an audit of its own, by the Accreditation Body (AB) which attests the CB complies with the relevant standards governing their activities. In the ISO certification scheme, the international standard ISO 17021 defines the requirements for operating a certification body, and ISO 17011 defines the requirements for accreditation bodies. Both standards emphasize the need for decisions on certification or accreditation to be made in accordance with key principles, including objectivity, confidentiality, and – most of all – impartiality.

This two-level tier constitutes an "accredited certification" scheme intended to ensure confidence in the resulting certificates issued, and thus confidence in the certified thing itself.

Certification without accreditation cannot be trusted with any degree of confidence.

At the same time, because accredited certification relies on purging conflicts of interest, a single body cannot simultaneously provide both certification and accreditation. Such a relationship injects insurmountable conflicts and eradicates trust in the resulting certifications.

AMERICAN LESSONS LEARNED

The United States began to privatize standardization activities during a period that roughly began in the 1970s and continued through the 1980s. Prior to that, standards development and resulting certification typically fell within the public sector, with standards being written by agencies such as the DoD and certification being performed by government auditors.

In 1993, the United States fully committed to having standards developed by outside bodies such as the International Organization for Standardization (ISO). The White House Office of Management and Budget (OMB) issued Circular A-119, ending government standards and establishing "*policies on Federal use and development of voluntary consensus standards and on conformity assessment activities*." The US had all but surrendered to this inevitable end years prior, but the OMB Circular formalized it.

The US then began a slow process of formally recognizing private "ISO certifications" as viable tender requirements for those companies bidding on US government contracts. The most famous such certification was for "ISO 9001," the international standard on quality management systems. To this day, companies without ISO 9001 certification often cannot bid on government contracts.

Launched in 1987, the ISO 9001 standard and surrounding third-party audit program quickly grew into a full-fledged accredited certification scheme. Led by the Registrar Accreditation Board (RAB), a US-based not-for-profit with ties to ANSI, an international accreditation model was created. RAB joined its equivalent bodies in allied nations such as the United Kingdom's UKAS and Germany's DAkkS to create a recognized network of accreditation bodies. This led to the formation of the International Accreditation Forum (IAF), which oversees such accreditations, and to the development of international standards such as ISO 17011[1] and ISO 17021. These standards, recognized by the United States, apply to certification bodies and accreditation bodies respectively. They define the requirements for such bodies when operating in an accredited certification scheme.

Unfortunately, as we will see, the DoD did not consult these standards nor reflect on the rich history of US accreditation, nor pay heed to the painful lessons learned by it and others in the industry over the past 40 years. The CMMC-AB has thus been making many of the mistakes originally made by RAB, and remaining wholly uninformed on the established international accreditation standards that should have guided its formation and operation.

One such lesson remains a critical warning for CMMC-AB. The original RAB accreditation body was formed to provide both accreditation of ISO 9001 certification bodies (called "CBs" or "registrars") as well as to certify CB auditors. It did so throughout the 1990s, but was hounded by accusations of conflicts of interest. Whereas RAB would conduct audits of its accredited CBs – to determine whether they should remain accredited – the fact

[1] *The formal and proper reference for this standard is ISO 17011-1, but the name "ISO 17011" is used herein for brevity and clarity.*

that RAB also offered certification of its CBs' auditors raised uncomfortable questions. The common allegation was that RAB could, feasibly, issue nonconformities against its CBs and threaten to withdraw their accreditation if the CB did not put its auditors through official RAB training. This led to accusations that RAB was weaponizing audit findings of certification bodies in order to increase its own revenue.

Whether or not the accusations were true, the RAB brand was damaged. So much so, in fact, that RAB was forcibly split into two. The accreditation body activities were rebranded under the name ANSI National Accreditation Board (ANAB), and the auditor certification business was sold outright to an Australian firm. At the same time, the resulting international standards were then updated to prohibit such relationships. These standards were originally issued as ISO "Guides" – enforceable by contract agreements, but later evolved into the ISO 17011 and ISO 17021 standards we have now. The rules against such conflicts of interest remain.

Ironically, DoD consulted with ANAB during the development of the CMMC accreditation program, but ignored the very reason ANAB bears its name, rather than "RAB."

The original Memorandum of Understanding (MoU) issued by the DoD and mandating the formation of the CMMC-AB directly invoked the ISO accreditation standards, but bungled their understanding. The MoU called for CMMC-AB to pursue "ISO 17011 certification" which is impossible, since accreditation bodies are "accredited" to ISO 17011, not certified to it. This error reveals the authors of the MoU conflated the meanings of certification vs. accreditation, and thus signed it without proper vetting.

At the same time, the MoU invoked another standard – ISO 17020 – which would not be applicable to the AB at all. It is not clear if this was simply a mistyping of "ISO 17021," but even then would not make sense.

Finally, the DoD MoU dictated that while the CMMC-AB would pursue ISO 17011 compliance, it would also be tasked with certifying persons and training organizations. This requirement directly conflicts with ISO 17011, which prohibits bodies from doing also certifying persons. As a result, there was no way the CMMC-AB could ever comply with the DoD's requirements since they canceled themselves out. Nevertheless, the MoU was signed by both parties.

As this paper is written, the DoD announced it was replacing the MoU with a no-bid contract to be issued to the CMMC-AB. A draft copy of that Statement of Work (SOW) included the same language as the MoU, ensuring that the contract would remain as corrupted – and legally unenforceable – as the MoU. A source reported that the final version of the SOW would remove references to the ISO standards altogether, an inelegant solution that will only invite more conflicts of interest and questions of impropriety, not less. If true, then the resulting CMMC-AB will not be held to any standards at all, and can engage in whatever conflicts it wants. This will erode trust in its decisions, its mark, and its authenticity.

Already, however, CMMC-AB is dogged with the same accusations that plagued RAB in its early days, as CMMC-AB tries to tackle accreditation of its certification bodies (called "C3PAOs" in this case), and to fund itself through the certification of auditors and other personnel. The very same allegations that were made against RAB in the 1990s are now being thrown up as warning signs for the CMMC-AB. We will not be able to fully trust decisions made by the CMMC-AB if they can generate revenue by offering paid services that will "cure" potential audit findings they may write up against their various C3PAOs.

This, in turn, will result in a lack of confidence and trust in any resulting CMMC Maturity Level issued.

THE CMMI MODEL

The DoD and CMMC-AB had decided early on to mimic the scheme provided by Carnegie Mellon University and the Software Enterprise Institute (SEI) for its Capability Maturity Model Integration, or CMMI. The CMMI scheme was designed initially to issue "maturity level" ratings to companies related to their software development capabilities and, later, was expanded to include more comprehensive scopes, such as IT services, product design and more.

At a 30,000 foot level, the CMMI scheme appears to resemble the ISO certification scheme: companies implement requirements defined in a standard, then undergo third party audits to confirm their compliance. At the end, they receive a certificate from the third party attesting to their compliance.

The similarities between the ISO scheme and CMMI end there, however. The CMMI Institute was very careful to avoid branding the issuance of CMMI Maturity Levels as a "certification" program, and the Institute itself does not refer to itself as an "accreditation body." The auditors in the CMMI scheme are called "appraisers," the audits "appraisals" and the CMMI standard itself is called a "model," not a standard.

This was not done for some random purpose of distinguishment, nor for branding. By doing so, the CMMI Institute ensured that industry stakeholders understood the program was not going to be subject to ISO 17011 norms on international accreditation. By not adopting a role of "accreditation body" or itself, the CMMI Institute liberated itself from those rules, for good or for bad.

Fortunately, the Institute has largely avoided many of the problems that the ISO accreditation rules were established to control, and the CMMI program – while not devoid of problems or conflicts of interest – remains well respected. This was due to rigor within the CMMI Institute, SEI and Carnegie Mellon University.

As soon as the DoD and CMMC-AB tried to merge the structural skeleton of CMMI into an ISO-based "accredited certification" scheme for CMMC, it doomed the project. The CMMI model cannot easily be converted to a formal accreditation scheme without the placement of tremendous hurdles. Given the CMMC-AB had CMMI experts in its midst, this error is baffling. But it exists, and must be addressed.

Specifically, the CMMC-AB attempted to mimic the role of the CMMI Institute, which cannot be done under a formal, internationally-recognized accreditation scheme. Under CMMI, the Institute is its own god, wholly omnipotent, and bearing final authority in all things. It allows itself to approve auditing bodies, auditors, user organizations, trainers and standards developers. None of that complies with ISO 17011, which assumes that such omnipotence would inject conflicts of interest. The CMMI Institute succeeds only based on the strength of its program and reputation, as well as the influence of Carnegie Mellon, but – to be fair – it risks collapsing into scandal if those controls are not adequately maintained. Every day the CMMI Institute wakes up it faces disaster.

The CMMC-AB aped the CMMI Institute to take on a similar omnipotent "god" role, fueled largely by its unique and powerful DoD mandate. Whereas the CMMI Institute could justify its solitary status on the basis of its reputation, the CMMC-AB would do so because the DoD said so.

Immediately, and without proper restraint, the CMMC-AB announced it would "certify," "register," "approve" or "license" the same bodies under its scheme: standards developers, auditors, trainers, consultants, clients, client representatives. Without due diligence, it rolled out these programs even before it had completed its official business and tax filings, and even without official Bylaws governing the work of its Board of Directors.

The plans and outlines for certifications were developed before the CMMC-AB even had an office, and much continues as the AB still lacks basic staff. Even the logo for the CMMC-AB has not been trademarked as of this publication, despite appearing on official documents. The rush to populate the CMMC-AB website with content outstripped its responsibility to ensure programs were properly developed.

The DoD personnel likewise had no understanding of the CMMI model, as shown by its MoU for the CMMC-AB with its "impossible contract" contradictions, and references to ISO 17011.

What the DoD and CMMC-AB must do, then, is abandon the goal of mimicking the CMMI, and create an entirely new "hybrid" accreditation model that ensures the CMMC-AB operates free of conflicts of interest and in accordance with ISO 17011, while offering a CMMI-style "maturity model" appraisal system.

Alternatively, the DoD could resort to reliance purely on its mandate and bully power over the Defense Industrial Base, and drop all attempts to make the CMMC scheme comply with norms related to accreditation. It could declare the CMMC-AB the god of the scheme, and abandon all claims to ISO 17011 compliance. To do so would invite disaster, scandal and – likely – criminal corruption. It would most certainly result in the weakening of US cybersecurity efforts, not the strengthening of US defenses. This paper assumes the DoD would not pursue such a scorched earth policy.

THE PATH FORWARD FOR CMMC-AB

Currently, the CMMC-AB offers multiple certification and accreditation paths, targeted at different organizations or individuals. As of this writing, there are nine separate accreditation/certification schemes offered or under plan by the CMMC-AB, although just one of those is itself broken into three levels, bringing the total number of possible certifications to be managed by CMMC-AB to eleven.

It is worth briefly mentioning that for an unfunded organization which will rely on donations and service fees for its revenue, operating nine simultaneous certification programs appears impossible. The likelihood is that this will stretch the CMMC-AB's resources far beyond its limits, and cripple the organization. This already appears to be the case, as the CMMC-AB struggles to process the very first crop of "Provisional Auditors," and has struggled to develop funding methods for its daily operations, never mind the rollout of nine separate programs.

In order to roll out this massive plan, the CMMC-AB has listed at least nine different "committees," with an additional seven "working groups." Yet reviewing the CMMC-AB webpage shows that the persons assigned to these committees and working groups are the same nine or ten people, largely Board members. Most are assigned to multiple roles.

In other established schemes, this massive number of certification programs would be performed by three or four different entities, each taking on a different task and working in accordance with their particular ISO 17xxx accreditation rules. The CMMC-AB – unfunded, unstaffed, and still relying on volunteer labor – promises it can do ***all*** of these.

As of this writing, the CMMC-AB defines the following certification programs under its control:

Scheme	Type	Description
Accreditation of "Certified Third Party Assessor Organizations" (C3PAOs)	Organizational	These organizations will audit and certify the end user organizations to the appropriate CMMC maturity level
Certification of "Certified Professionals" (CPs)	Individual	These individuals essentially hold the role of audit team member, working under a Certified Assessor (below)
Certification of "Certified Assessors" (CAs)	Individual	These individuals act as "lead auditors" and can conduct CMMC appraisals. There are three different levels, allowing the CA to perform audits at the various CMMC ML levels.
Registration of "Registered Provider Organizations" (RPOs)	Organizational	These organizations will be authorized to provide to consulting while bearing official CMMC-AB recognition; RPOs will be comprised of RPs (below)
Registration of "Registered Practitioners" (RPs)	Individual	These individuals will be authorized to provide consulting while bearing official CMMC-AB recognition.
Licensing of "Licensed Instructors" (LIs)	Individual	These individuals will be authorized to provide CMMC training; presumably, LIs will work for LTPs (below)
Licensing of "Licensed Training Providers" (LTPs)	Organizational	These organizations will be authorized to provide CMMC training and issue recognized training certificates.
Licensing of "Licensed Publishing Partners" (LPPs)	Organizational	These organizations will be authorized to sell CMMC related training courses "direct to the consumer." The intersection between LTPs and LPPs is unclear.
Licensing of "Licensed Software Providers" (LSPs)	Organizational	This has not yet been formally defined by the CMMC-AB, but one assumes these organizations will be authorized to sell CMMC related software, possibly for implementation or system control.

As we can see, confusion arises from the CMMC-AB's seemingly random use of terms such as "accreditation," "certification," "registration" and "licensing." In practice, they are identical: the CMMC-AB will issue some form of formal approval for the individuals or organizations within the given silo. Legally, the CMMC-AB may be considering some distinction between them, but as of right now, this is wholly unclear. Representatives of both DoD and the CMMC-AB have used the various terms interchangeably, often confusing them.

The introduction of so many programs also introduces a complex network of problems brought on by applicable international standards, all of which are formally recognized by the United States. The certification of individuals and training bodies would fall under ISO 17024, an entirely different standard; this would be applicable to the CP, RP, LI, and LTP schemes at a minimum. The certification of software providers or publishing partners (LPP, LSP) would likely fall under ISO 17020 – yet another standard. The accreditation of C3PAOs would fall under ISO 17011, but each C3PAO would then be required to comply with ISO 17021.

A complex and confusing brew, to be sure.

ENFORCING IMPARTIALITY

To simplify this, one need only understand a core concept in play with nearly all of the ISO 17xxx standards: the key principle of "impartiality." This runs through as a genetic blueprint in all such standards, and demands that decisions of certification or accreditation always be made objectively, impartially, and free of conflicts of interest.

As a result, the standards are separate because it is understood that a single organization attempting to do too many things will inevitably face conflicts of interest which create "risks to impartiality" which cannot be overcome. As discussed previously, an accreditation body such as CMMC-AB could not simultaneously certify C3PAOs and assessors since it risks a conflict of interest in its decisions regarding both.

Even the power to write and publish the CMMC model itself can be a conflict, as the CMMC-AB could "edit" the standard in order to enhance its position in the market. As I write this, the DoD and CMMC-AB are discussing the dilution of CMMC ML3 requirements to yield to market pressure, and increase likely update. This raises questions as to whether the CMMC-AB is considering this in order to boost its revenue at the risk of reducing US cybersecurity resilience.

The solution, therefore, is for CMMC-AB to comply with the accepted standards, and ***divest its certification activities, limiting its role to solely the accreditation of C3PAOs.***

The suggestion is not as draconian as it appears, and fortunately we have decades of US experience to guide us.

Rather than attempt to single-handedly take on every possible role under the CMMC scheme, the CMMC-AB must instead authorize others to perform each of the remaining silo activities, and then ensure the quality and trust in those activities by requiring those providers to each maintain their own applicable ISO 17xxx accreditation.

Reviewing each silo activity separately, this would require the following:

Recommendation		Silo Activity
Appraisals	Retain	**Accreditation of the "Certified Third Party Appraisal Organizations" (C3PAOs)** CMMC-AB would retain this authority, and treat it as its primary responsibility. CMMC-AB would restructure its operations to comply with ISO 17011.
	Divest	**Certification of "Certified Assessors" (CAs)** CMMC-AB would divest this activity. It would issue an RFP to solicit auditor certification bodies to take on the role. Such bodies would have to be accredited to ISO 17024 by an independent accreditation body.
Training	Divest	**Licensing of "Licensed Training Providers" (LTPs)** CMMC-AB would divest this activity. It would issue an RFP to solicit independent training bodies to take on the role. Such bodies would have to be accredited to ISO 17024 by an independent accreditation body.
	Drop	**Licensing of "Licensed Instructors" (LIs)** CMMC-AB would drop this designation entirely. The CMMC-AB should not regulate nor approve any consulting bodies, as this introduces an insurmountable conflict of interest. Instructors would be managed by the ISO 17024-accredited LTPs.
	Divest	**Certification of "Certified Professionals" (CPs)** CMMC-AB would divest this activity. It would require the ISO 17024-accredited LTPs (above) to issue CP certificates to their students.
Consulting	Drop	**Registration of "Registered Provider Organizations" (RPOs)** CMMC-AB would drop this designation entirely. The CMMC-AB should not regulate nor approve any consulting organizations, as this introduces an insurmountable conflict of interest.
	Drop	**Registration of "Registered Practitioners" (RPs)** CMMC-AB would drop this designation entirely. The CMMC-AB should not regulate nor approve any individual consultants, as this introduces an insurmountable conflict of interest.
Products	Drop	**Licensing of "Licensed Publishing Partners" (LPPs)** CMMC-AB would drop this designation entirely. The CMMC-AB should not regulate nor approve any training products nor any sellers of such training products, as this introduces an insurmountable conflict of interest.
	Drop?	**Licensing of "Licensed Software Providers" (LSPs)** UNKNOWN – at this time, it is not clear what the purpose of the LSP certification program would be, and no recommendation can be made. If the intent is to license CMMC related software products, then the recommendation for LPP above would apply.

The plan above would reduce the CMMC-AB's activities from nine separate certification programs to only one – the accreditation of C3PAOs – allowing it to conform to ISO 17011 while maintaining a role that is long-established and well recognized within the US and internationally.

It would then only have the responsibility to approve auditor certification bodies and training providers, but only doing so if those organizations have a pre-existing ISO 17024 accreditation issued by an independent body.

These bodies would then be responsible for the training and internal certification of their various staff (auditors, trainers, etc.) under the ISO 17024 rules governing them.

In this manner, the CMMC-AB would still retain ultimate authority over the scheme, but rely on accredited and proven suppliers to manage other activities.

At that same time, this would reduce the CMMC-AB's estimated operating budget down to a tiny fraction of what it would be if the group carries out its plan to oversee nine separate certification silos.

ORGANIZATIONAL CHANGES

In addition to the scope changes suggested above, CMMC-AB would have to commit to organizational and structural changes. These would be easily recognized by existing accreditation bodies and industry actors, but may appear radical given the current CMMC-AB structure.

By adopting ISO 17011 and divesting the activities indicated above, the CMMC-AB Board and executive leadership would have to simultaneously commit to ensuring its impartiality, and remove all potential risks for conflicts of interest. Currently, the CMMC-AB commits only to disallowing Board members from working for "*a company planning to perform CMMC assessments*."2 The only other conflict of interest guidance comes from generic statements provided in the organization's Code of Ethics[3] and Conflict of Interest Summary page[4]. These generic statements provide only high-level guidance which might sway Board members away from conflicts of interest, but so far have gone largely unenforced. For example, despite statements in the Conflicts of Interest Policy Summary that prohibit Board members from engaging in conflicts related to "Financial Interests" or related to "Other Organizations," incidents of both current and former Board members being engaged in selling related CMMC consulting products remain evident, pointing to the CMMC-AB's unwillingness to enforce the policy.

Instead, the CMMC-AB must rewrite and publish a revised Conflict of Interest Policy, in compliance with ISO 17011, which prohibits Board members and staff from engaging in any activity whatsoever that would cast doubt on accreditation decisions made by CMMC-AB. This means a fully enforceable prohibition of any consulting, training, product sales or other related services being offered by a such persons.

To comply with ISO 17011, CMMC-AB would have to develop and publish a formal complaints handling procedure, something it has still not done as of this publication. This procedure must be included as a public-facing document on the CMMC-AB website, and allow for the processing and investigation of complaints by CMMC-AB staff who are unrelated to the issue being reported. This would also require CMMC-AB to have ready access to independent and objective third parties who could act as arbitrators when a complaint resolution is disputed by the complainant.

Next, the CMMC-AB would have to ensure the Board represented a distribution of applicable experts not only from the cybersecurity field, but from government, private industry, and accreditation industry experts. This should likewise include representatives of the public. The predominance of private consultants must be prohibited by a change in the CMMC-AB's Bylaws, and made irrevocable.

[2] Source: https://www.cmmcab.org/board-of-directors as of 17 Sept. 2020.
[3] https://www.cmmcab.org/ethics
[4] https://www.cmmcab.org/coi

Next, the CMMC-AB would have to tie staff salary – including that of any executives or Board members – to industry standard rates, and decouple them from any "performance" figures. This would remove incentives for CMMC-AB members to engage in public relations work that may undermine the body's independent voice and objective authority, as well as eliminate the possibility that CMMC-AB personnel would engage in misleading public statements intended to promote CMMC and thus improve their own personal income.

Finally, the CMMC-AB would have to appoint a single independent Ombudsman to provide a semi-annual report on the status of the CMMC-AB, specifically related to impartiality and general good governing. This person should be selected from outside the cybersecurity field, but with experience in such oversight matters. The role would be fixed for a period of 5 years, with the person not being subject to termination by the Board except in cases of gross mismanagement or fraud. The Ombudsman's reports would be issued to the public, without censorship by the CMMC-AB itself. Any recommendations of the Ombudsman would be acted upon by the Board.

THE IAF QUESTION & ULTIMATE OVERSIGHT

Under the ISO accreditation scheme, certification bodies (registrars) are accredited to ISO 17021 by their accreditation bodies. Those accreditation bodies (such as ANAB) are then held to compliance with ISO 17011 through peer review audits governed by the International Accreditation Forum (IAF). Such bodies must sign a Multilateral Agreement (MLA) which not only allows the bodies to recognize each other's accreditations, but also obligates them to comply with ISO 17011.

The IAF then has a set of six Regional Accreditation Groups (RAGs) that oversee the peer reviews and other activities in key geographical regions. The RAG for the United States is, for example, the Inter American Accreditation Cooperation, or IAAC.

While the IAF oversight scheme has been plagued with its own conflicts of interest and corruption, it represents the only means by which accreditation bodies can be held accountable outside of the courts. For the DoD and CMMC-AB, however, participation in the IAF is impossible, because of the influence of foreign actors. This is because the IAF and RAGs are intended to serve the entire world – in a manner similar to the United Nations – and not the United States specifically.

As of this writing, the IAF President is a Chinese national, an executive of the Chinese National Accreditation Service (CNAS), the official accreditation body of China. Likewise, the Director for Quality for APAC – the IAF RAG which oversees activities in all of Asia and Australia – is a CNAS official. CNAS is an official Chinese governmental department. Both these men are sworn first and foremost to serve the Chinese government, with their duties related to international accreditation being tertiary at best.

If the CMMC-AB were to participate in this scheme – in order to ensure compliance to ISO 17011 by undergoing peer review audits managed by the IAF – it would expose its operations to the very same enemy actors the nation's cybersecurity work is intended to defend against. Complaints filed against the CMMC-AB could be appealed to the IAF, and then potentially ruled on by Chinese executives.

As a result, the CMMC-AB must steer far clear of the IAF and participation in its peer-review process. This, however, introduces multiple avenues for subsequent violations of the CMMC-AB against ISO 17011, and for it to quickly devolve into full non-compliance. In short, CMMC-AB would be self-declaring compliance to ISO 17011 without any independent oversight or formal blessing, making it an "accreditation mill."

To circumvent this, the CMMC-AB would have to issue an RFP for a single auditing body to perform annual ISO 17011 compliance audits of the CMMC-AB itself. This body would report to the Ombudsman referenced above, although the compliance audit reports themselves would be confidential to the CMMC-AB. If, in the decision of this independent auditing body, it was found the CMMC-AB no longer complies with ISO 17011, this would be communicated to the Ombudsman and reflected in his/her semiannual report to the public.

The selection of the ISO 17011 auditing body would have to ensure the body was independent of the cybersecurity industry and certification scheme, to ensure maximum independence and objectivity. Such auditors would be granted full access to all CMMC-AB records, accreditation audit reports, etc., while be subject to strict confidentiality agreements.

CONCLUSION

The current path pursued by the DoD and CMMC-AB cannot ensure the integrity of the US Defense Industrial Base because it is based on a flawed understanding of accreditation, and ignores decades of lessons learned by the US in this space. The current approach will only likely introduce conflicts of interest and questions about the validity of resulting CMMC certifications, while not improving the nation's cybersecurity posture.

Only through the adoption of a structure that reinforces impartiality in the issuance of CMMC certifications can the program succeed. With these suggestions, there will be a dramatically improved likelihood that CMMC ratings will be an indicator of an individual organization's ability to safeguard critical US data.

ABOUT THE AUTHOR

Christopher Paris has been involved in ISO certifications, standards and accreditation since 1988. In 1999, he founded Oxebridge Quality Resources, an ISO consulting firm which moved on to specialize in AS9100, the aerospace quality certification program. He was chief AS9100 quality system architect for SpaceX, working with them from 2005 to 2014. He has implemented certified quality systems for major firms including GKN Aerospace, Northrup Grumman, ASCOM Transport Systems and over 300 small manufacturers within the industrial supply chain.

Mr. Paris worked on standards development for ISO Technical Committee 176, responsible for the ISO 9000 family of standards, and has consulted for numerous ISO certification and accreditation bodies. He previously headed the Management Maturity Model (M3) Development Council, which aimed to port CMMI style approaches to the manufacturing standards. That effort led Mr. Paris to help develop the Oxebridge Q001 accredited certification program, combining the approaches of ISO 9001 and CMMI into a rated quality system certification scheme.

Mr. Paris' company operates the world's only independent ISO Whistleblower Program, collecting and processing complaints related to the ISO certification scheme from all of the world. That program has resulted in the de-certification of multiple "bad acting" certification bodies, the investigation of over a dozen international accreditation bodies, and one criminal investigation. Mr. Paris has provided independent whistleblowing reporting to the DoDIG, FDA, FAA, NASA and the House Committee on Science, Space & Technology.

Mr. Paris' work in exposing accreditation fraud and the work of unaccredited "certificate mills" has led to a widespread understanding of the problems, and changes to international approaches to managing such mills. In 2019, Oxebridge was awarded a $1.6 million judgment against a self-accredited mill in a US Federal lawsuit.

He has published multiple books on ISO 9001 and AS9100, including the satire standard "Eyesore 9001."

Born in New York City, Mr. Paris now lives in Lima Peru.