OPINION PAPER:

ADDRESSING HOW THE US DEPT. OF DEFENSE CONTRACT WITH THE CMMC ACCREDITATION BODY RISKS THE UNITED STATES' NATIONAL DEFENSE

---

02 February 2021
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 industrial base (DIB) companies and others will be audited against the CMMC model and receive a CMMC Maturity Level rating. These 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 Body (CMMC-AB), and tasked it to oversee this scheme. The DoD originally utilized a largely symbolic "Memorandum of Understanding" (MOU) to stand up the CMMC-AB, but in late 2020 signed a no-bid contract with the CMMC-AB formally assigning the body its sole authority as the nation's sole CMMC accreditation authority. The "statement of work" (SOW) portion of that contract was made public in February of 2021, after Freedom of Information Act requests were filed by journalists. (For reasons which are not clear the DoD has refused to release the entire contract.)

The SOW reveals troubling defects which put the nation's cybersecurity at risk, and present a clear and present danger to the national security of the United States. Primarily, this is due to the requirement for foreign oversight and appeals authority which the DoD has unwittingly injected into the nascent CMMC scheme. More frustrating still, this comes after the DoD's CMMC Program Management Office and the Office of the Undersecretary of Defense for Acquisitions & Sustainment was notified repeatedly that the arrangement would pose a risk to national security.

ISO STANDARDS & CERTIFICATION

The standards published by the International Organization for Standardization (ISO) are widely accepted by the world's nations and used to facilitate trade and technical matters. Without standards, one nation might have a different means of measuring inches or hours or electrical currents.

The DoD has opted to rely on some key ISO standards for the CMMC program.

> **ISO 17020** – a standard for inspection bodies, the DoD has declared that all CMMC Third Party Assessment Organizations ("C3PAOs") must be accredited to this standard.
>
> **ISO 17024** – a standard for training bodies, the DoD has mandated that "CAICO," an eventual training body that does not yet exist, will be accredited to this standard.
>
> **ISO 17011** – a standard for accreditation bodies, the DoD has mandated that the CMMC-AB itself will comply with this standard. To verify compliance, the DoD has mandated that CMMC-AB will undergo peer evaluations by the IAAC.

ACCREDITATION HIERARCHY

Within common accreditation schemes, there is a standard hierarchy. A company obtains "certification" to a standard or specification by undergoing inspections or audits performed by an authorized "certification body," or "CB."

The CB gets its authority by undergoing similar audits of its own activities, to ensure it is operating fairly and objectively. Those audits are conducted by an "accreditation body," or "AB". The AB then accredits the CB, authorizing them to issue certificates with national or international recognition.

The air at the top of the AB pyramid begins to thin, with fewer available bodies to provide oversight at that level. In response, the International Accreditation Forum (IAF) was formed, to provide a means of overseeing ABs with the same level of rigor as was being used to certify companies or accredit CBs.

DEPT. OF DEFENSE "SOW" FOR CMMC-AB

In late 2020, the DoD's OUSD A&S office announced it had signed a no-bid, sole-source contract with the CMMC-AB authorizing it to act as the nation's sole accreditation authority for CMMC. The DoD has refused to release this contract, prompting journalists to file FOIA requests. To date, only the SOW portion of that contract has been made public; the surrounding contractual text and signature pages are presumably still being withheld by the OUSD A&S.

The SOW makes several demands on the CMMC-AB, the main issue of concern related to this report is the demand that CMMC-AB become accredited to ISO 17011 and subject itself to oversight by the Inter-American Accreditation Cooperation (IAAC) and – by extension – the International Accreditation Forum (IAF).

The specific text of the SOW, found in clause III.4, reads as follows:

> a. The CMMC-AB, upon achieving ISO/IEC 17011 compliance, shall maintain compliance with the ISO/IEC 17011 standard to include meeting all requirements for self-assessments, peer reviews, and other assessments.
>
> b. The CMMC-AB shall become a full member of InterAmerican Accreditation Cooperation (IAAC) after achieving ISO/IEC 17011 compliance and shall remain in good standing.

IAF & IAAC

The International Accreditation Forum was originally formed in the late 1990s with major influence by the United States, through the US' sole national accreditation body at the time, the Registrar Accreditation Board (RAB, now known as ANAB.) Through the 2000's RAB/ANAB maintained effective control over the IAF. In the 2010s, however, ANAB yielded control of the IAF to China. The current president of the IAF is Xiao Jianhua, who is also the chief executive of the Chinese National Accreditation Service (CNAS), the sole Chinese accreditation body authorized by the Chinese national government. Prior to his ascendancy as President, Mr. Xiao had been a long-time fixture within the IAF, heading various committees and performing multiple duties.

The IAF's role, as said previously, is to ensure the world's accreditation bodies comply with the applicable ISO standards, and operate objectively and fairly. The IAF enforces this through a master Multilateral Agreement (MLA) and other contractual documents agreed to by its various signatory members.

The IAF then uses a set of "Regional Accreditation Groups" (RAGs) to carry out practical enforcement of the MLA. For the North, Central, and South America, this is the Inter-American Accreditation Cooperation (IAAC). Other regions of the globe utilize different IAF RAGs. Chinese CNAS officials can be found on the staff of some of these RAGs as well as within the IAF executive structure itself.

The IAF MLA requires the regional groups, such as IAAC, to require members to undergo peer evaluations. These are codified in official IAF "Mandatory Documents" (MDs) as well as other policies and procedures, all available for public review at www.iaf.nu. The IAAC then has developed its own regional policies, procedures and MDs for use by it, which are available for public review at www.iaac.org.mx. The IAAC policies must comply with the overall rules mandated by the IAF.

In all cases, the IAAC rules reinforce the uphold the IAF MLA; the IAAC has an MLA of its own, as well.

While the IAF is operated under Chinese management, with a Canadian consultant (Elva Nilsen) acting as day-to-day administrator, the IAAC operates out of Mexico. The current IAAC President is from Uruguay; only a tiny handful of IAAC staff are from the United States.

For purposes of international trade and less critical social functions, the role of international bodies in the IAF management is not a particular concern; in fact, many would argue that using such platforms to build bridges with hostile nations like China or Venezuela may lead to longer-term peace. In the area of cybersecurity, however, this relationship represents an insurmountable risk to national security.

By demanding that the CMMC-AB become a "full member" in IAAC, the DoD has thus required that the CMMC-AB be in full compliance with procedures and multilateral agreements written and enforced by foreign actors.

For the IAAC, "Full Membership" applicants must first fill out IAAC form FM27 "*Application Form for Full Membership*." That form (available here) will require the CMMC-AB to submit legal and other information that will be considered and reviewed by foreign nationals in Mexico. That form requires signing a "Declaration" binding the CMMC-AB to various requirements, including:

- *to abide by all IAAC MOUs and Arrangements to which IAAC is signatory*
- *to abide by IAAC Policies and Procedures for a Multilateral Recognition (if applicable)*
- *to be represented, attend and support IAAC meetings, working groups and peer evaluation activities whenever appropriate or feasible*
- *to contribute to the efficient resolution of any complaints received by IAAC in circumstances where our organization is involved*

The actual list is much longer, but these are the most troubling. In short, it puts the management of CMMC-AB under the procedural thumb of Mexico and foreign nations. Any violations mean the CMMC-AB would lose its membership in IAAC, and losing that membership means it loses its authority under the DOD contract.

Meaning: ***Mexico or other Central or South American nations can control whether or not the US has a cybersecurity accreditation body.*** If political relations deteriorate between the US and Mexico, or perhaps another Central or South American nation with influence at IAAC such as Brazil, the US could find itself "punished" by losing its sole CMMC accreditation body overnight. Likewise China, through the IAF, can eject the CMMC-AB from its scheme upon a whim.

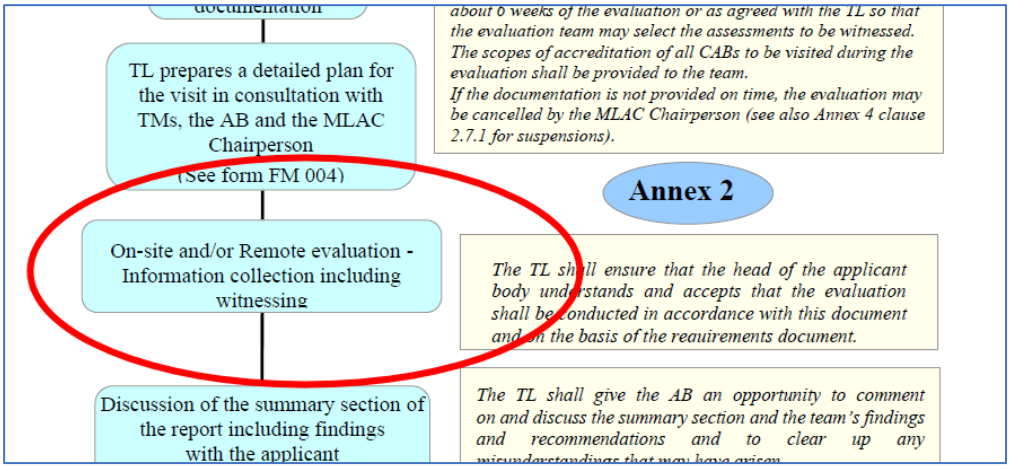
PEER EVALUATIONS

The concept of peer evaluations is the keystone to the IAF accreditation scheme. The intent is that peer ABs will audit each other to ensure the overall health of the system, and to ensure each AB is acting independently and objectively. The system is ineffective, corrupt, and results in nothing but silent scandal. It was always nonsensical to assume that competing ABs would fairly audit each other. It could have gone very bad, with ABs

suing each other, but instead, the opposite happened: AB peer evaluations are largely rubber stamp exercises, out of the ***fear*** of litigation. One AB will never recommend de-listing another AB, lest they get sued. So ABs never lose their accreditation authority, since they never fail peer evaluations.

But despite the fact that the scheme is corrupt, the ***process*** of conducting the evaluations is outright dangerous because it gives key players insight into the workings of their competitors.

The IAAC has a procedure for its peer evaluations, published as MD002 (here). That procedure requires ABs to both provide peer evaluators to audit other ABs, but also undergo peer evaluations itself. The procedure then includes a multi-page flowchart defining the peer evaluation process. The key step involved is that actual audit of the AB itself by IAAC peers -- in this case, the CMMC-AB would have to submit to a physical (or remote) audit by foreign nationals. This main activity conducting during this audit (like any audit) is "*information collection and witnessing*":



This would include allowing IAAC peer audit team members to review the CMMC-AB's audit reports of its C3PAOs, including any deficiencies the AB may have written against those C3PAOs. This can -- and is likely to -- ***include a review of the C3PAO audit reports for the end user defense industrial base company as well.***

That procedure references "Annex 2," which then goes on to explain in great detail what that peer audit will look like. For the CMMC-AB, since they will be accrediting C3PAOs to ISO 17020, the Annex 2 text gives this explicit instruction on what will be examined during a peer evaluation:

Inspection ISO/IEC 17020	Includes witnessing of the assessment by the AB of the CAB performing inspection. Depending on the risk number of accredited inspection bodies, the variety of the scopes, and IAAC MLAG decisions. it may be necessary to perform more witnessing.

This means the IAAC will have to witness the actual audits of the CMMC-AB of their C3PAOs. The procedure then goes on to reinforce that witnessing will include on-site accompaniment of the AB, or side-by-side participation if the audit is performed remotely:

> If an AB only uses on site assessment techniques for an accreditation scheme, then the peer evaluation must include witnessing of on-site assessment. If an AB uses remote assessment and on-site assessment for the same accreditation scheme, the Lead Evaluator, with the approval of the MLAG Chair, will determine the type of witnessing to be performed, on-site, remote, or a combination of both. This determination will be made based on a risk assessment that will include considerations such as the results of previous peer evaluations, complaints received by IAAC, the complexity of the accreditation scheme, etc. The remote and/or on-site evaluation techniques implemented must ensure that all the relevant requirements of ISO/IEC 17011 and IAAC are evaluated for compliance during the witnessing of the evaluated accreditation scheme(s). On-site witnessing will normally be required for extensions to the scope of recognition that include onsite assessment and always be required for initial evaluations, when onsite assessment techniques are utilized by the AB for that accreditation scheme(s).

The procedure then goes on to reiterate that ***any and all*** of the CMMC-AB's assessments of C3PAOs can be witnessed, including initial assessments and re-assessments:

> It is important to have the opportunity to witness assessments covering all accreditation requirements, particularly in the initial evaluation. It may be necessary to perform more witnessing in initial evaluations than in re-evaluations.

So, the IAAC must ***physically oversee an actual assessment of a C3PAO as it is performed by the CMMC-AB.*** In fact, it will have to review ***multiple*** assessments.

If there remains any lingering doubt, we can review the official IAAC Form 003 "*Checklist for Peer Evaluations.*" That form indicates the questions that must be verified by the IAAC peer evaluators, and provides spaces to capture audit evidence. In the example below, for instance, the IAAC would have to verify records that prove the CMMC-Ab issued a "decision" on a complaint or appeal, and that it was "*made by individuals not involved in the activities in question.*" The only way to verify this is for the IAAC to directly review actual complaints and the CMMC-AB's documented replies.

Inter-American Accreditation Cooperation

Requirement (Clauses refer to ISO/IEC 17011:2017, except where otherwise specified.)	AB's Documents	Notes from IAAC Evaluation Team for consideration by the AB
c) ensuring that any appropriate action is taken in a timely manner.		
7.13.6 The accreditation body receiving the appeal shall be responsible for gathering and verifying all necessary information to validate the appeal.		
7.13.7 The accreditation body shall acknowledge receipt of the appeal and provide the appellant with progress reports and the outcome.		
7.13.8 The decision to be communicated to the appellant shall be made by, or reviewed and approved by, individual(s) not involved in the activities in question.		
7.13.9 The accreditation body shall give formal notice of the end of the appeals handling process to the appellant.		

What does this mean in practice? A C3PAO will have to undergo an accreditation audit by the CMMC-AB. At any audit, the IAAC is allowed to tag along as a witness, for peer evaluation. **No one can object to this**: not the CMMC-AB, not the C3PAO, nor any DIB company who might have their information exposed. IAF rules allow for blacklisting any company that objects to this arrangement, prohibiting them from obtaining ISO certification.

So during the CMMC-AB's audit of the C3PAO, the CMMC-AB auditors will be questioning the C3PAO on its decisions related to issuing or denying a CMMC certification to a DIB company. This will include an in-depth review of the audit deficiencies issued by the C3PAO to its DIB end clients. **All while foreign nationals from the IAAC peer team are directly observing, in real-time.** Rules demand that these "witness auditors" have full

access to the information being given to the CMMC-AB, so there any obfuscation or hiding is disallowed by procedure.

The only protection is a weak and wholly unverifiable requirement that at the end of an audit, the IAAC peer review team will "*destroy all documents they have received*." There is no means to verify this whatsoever, and no real legal recourse if it is discovered that the IAAC has failed to do so. Since a peer team can simultaneously comprise auditors from Jamaica, Brazil, Canada, and Chile, the legal systems and courts of multiple countries would come into play, creating an impossibly complex litigation problem.

> **1.3.2** Unless otherwise agreed the Team Leader (TL) and Team Members (TM) shall destroy all documents they have received, when the final decision has been made by the MLA Group.

COMPLAINTS AND APPEALS

Another key element of IAF accreditation oversight is to provide an escalation pathway for complaints and appeals. This attempts to address the conflicts of interest which arise when an organization is asked to process a complaint against itself. The IAF scheme allows for complaints to be escalated through the C3PAO, to the CMMC-AB, and then – if the responses are not adequate – to the IAAC and eventually the IAF itself.

As a result, China now exerts control as the final arbiter of any such appeal.

The IAAC procedure PR005 (available here) provides the rules for handling complaints and appeals. This includes complaints issued against the CMMC-AB by any third party, whether a DIB company, a C3PAO or an industry stakeholder such as Oxebridge. That procedure then requires the active participation of the IAAC executives – again, foreign nationals – in managing and resolving the dispute.

> **5. COMPLAINTS AGAINST AN IAAC MEMBER ACCREDITATION BODY**
>
> 5.1 If a complaint is submitted against the activities of an IAAC member, by a third party, IAAC shall ensure that the complaint be handled first by the IAAC member against whom the complaint was lodged, in order for the complaint to the addressed by the AB's complaints procedure.
>
> 5.2 To comply with the above, when a complaint is received, the complainant shall be asked to provide evidence that the complaint was handled and resolved by the specific AB, and the corresponding process will be followed according to section 4. If no information is received about how the complaint was handled by the AB, the complaint shall not be considered valid.
>
> 5.3 When the IAAC Chair, in consultation with the Executive Committee, consider it necessary, they may ask the IAAC Secretary, to provide a lead evaluator, before a peer evaluation, the details about a complaint received against an IAAC member, in order to verify additional information if it were necessary.

This may then trigger a special peer evaluation, with all the national security risks present as for normal peer evaluations, as discussed previously.

Furthermore, the IAAC holds the authority to revoke the CMMC-AB's accreditation status based on complaints from third parties:

> **2.7 Suspension and withdrawal of MLA Group**
>
> **2.7.1** It may be that the IAAC MLA Group cannot accept the corrective action taken by an AB with regard to significant changes notified by the AB, or to nonconformities which have been found, or to substantiated complaints from interested parties. It may also be that the AB does not provide the documentation required to perform the evaluation, delays reevaluations or follow up visits, or does not appropriately respond to the nonconformities of a peer evaluation in the time frame established in this document. The IAAC MLA Group may then take appropriate action. This action can be suspension for a maximum period of 12 months or withdrawal from the IAAC MLA.

In this case, the IAAC alone would have the authority to "substantiate" a complaint, perhaps from another foreign actor.

My firm, Oxebridge, has seen this first hand. In 2019, in retaliation for its whistleblowing activities, an American certification body threatened a client for hiring Oxebridge, in violation of accreditation rules demanding impartiality and objectivity. Oxebridge filed a complaint with the CB, which closed the complaint without action. Oxebridge then escalated the complaint to the applicable accreditation body, ANAB, who similarly dropped the issue without thorough investigation. As a final step, Oxebridge was forced to escalate the complaint to IAAC. The escalation paperwork was authored in Spanish and submitted to the IAAC Secretariat in Mexico. It was then processed by representatives of Jamaica, Uruguay and Brazil. Some communications were copied to the IAF, including Xiao Jianhua of China. In this case, the matter did not pertain to national security, so was relatively innocent.

In the CMMC scheme, a likely scenario will be similar, but with far more serious consequences for national security. A DIB company is likely to object to a C3PAO assessor's ruling during a routine CMMC assessment. To object, the DIB company will have to file a complaint with the C3PAO. If the result is not satisfactory to the DIB company, it will have to escalate the issue first to the CMMC-AB, and then to the IAAC. This will further expose cybersecurity data to foreign actors, and grant final authority over the CMMC-AB to Mexico or China.

Even if a complaint is mutually resolved at the C3PAO or CMMC-AB level, the records of that complaint will be visible to the IAAC or IAF during the peer evaluation process. Foreign actors can "mine" such data for useful information on the nation's cybersecurity weaknesses.

DOD REJECTED PRIOR WARNINGS

The OUSD A&S office openly rejected warnings submitted to it related to this potential scandal.

On September 17, 2020, Oxebridge released a white paper entitled "*The Path Forward for the CMMC Accreditation Body and the Cybersecurity Maturity Model Certification Scheme*." That paper pointed out the problems inherent with IAF oversight and its Chinese executive management. Copies were sent to the OUSD A&S office, including to Mr. Fahey and Ms. Arrington personally, as well as to Ellen Lord. That paper may be read here.

Despite this, on September 18th, the CMMC Project Management Office, led by Stacy Bostjanick, arranged a meeting with key CMMC-AB Board Members and ANAB. According to official meeting notes, the attendance included Ms. Arrington, Ms. Bostjanick as well as Mary Saunders of ANSI (which owns ANAB) and ANAB's representative Reinaldo Figueiredo. Curiously, however, Mr. Figueiredo was introduced as an "ISO/CASCO

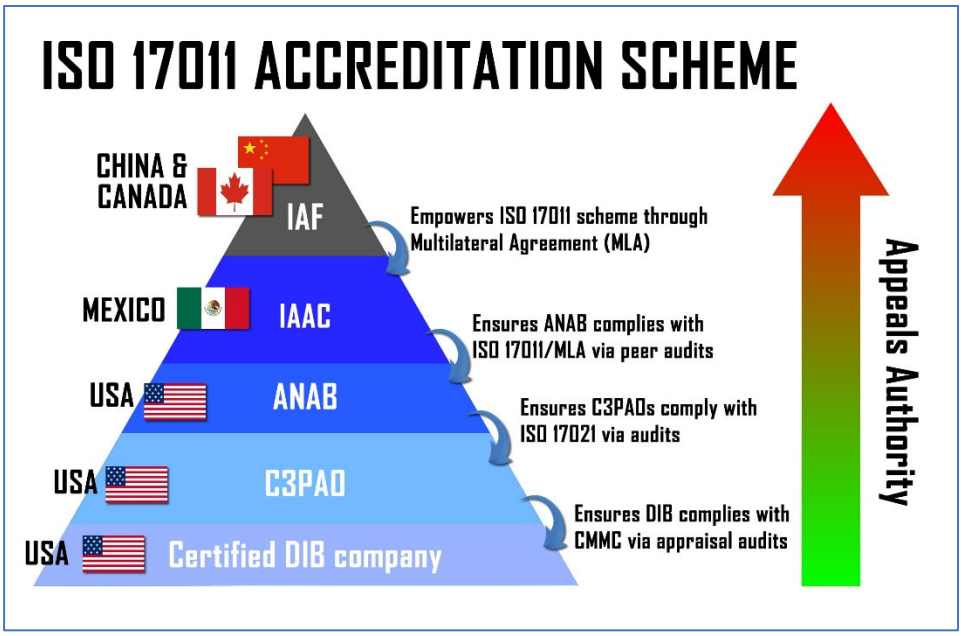
Chair," and his role in ANAB was not disclosed to the CMMC-AB participants in attendance. Figueiredo is a foreign national from Brazil, and previously held roles in that country within the certification industry; he is also a representative of IAAC, and a former Chair of that organization. These latter points were also not reportedly disclosed to the attendees.

The stated purpose of the meeting was to solicit ANSI's expertise related to "*applicable ISO/IEC standards for the implementation of CMMC.*" The actual intent was to apply pressure on the CMMC-AB to sign the SOW, with the undertone being that if they did not, Ms. Arrington would dismantle the CMMC-AB and hand over CMMC control to ANAB.

Additional records revealed that Arrington's office had "*conducted initial outreach to ISO and ANSI*" two days earlier, on Sept. 16th. The notes reported that ISO advised Arrington's office to contact ANSI, who then put her in contact with Mr. Figueiredo. He is again referenced only as the "ISO/CASCO Chair."

Given that the Oxebridge white paper essentially was released simultaneously with – or one day before – the ANAB meeting, it can be excused. However, the DoD failed to respond to messages at that point. To address this, I personally sent Mr. Fahey a copy of the white paper on September 29th, which he acknowledged receipt of.

On September 30th, an article was then released on the Oxebridge website entitled *DOD's Arrington Threatens to Disband CMMC-AB, Hand Accreditation Authority to Body Subject to "Peer Audits" by China*. That can be seen here. The article included this graphic representing the roles of Mexico and China in the proposed DoD scheme being considered at that time:



The article went "viral" and prompted replies by many industry actors. I personally forwarded a copy to Mr. Fahey on September 30th. Mr. Fahey replied, using his personal email address. He rejected the points made by the article, and went on to tout himself as the architect of the accreditation arrangement, taking personal responsibility for it while defending Ms. Arrington. The email was also dated September 30th, and read as follows (emphasis added):

Chris not sure where you are coming up with your information Ms. Arrington is 100% behind the AB. I have asked her to develop options which she continues to work. Chris we are trying really hard to do the right thing and protect our DIB and IP. We will all learn as we figure it out. ***Much of what Katie is doing is based on my ideas with my quality background going from 9858 to iso9000 and software and systems engineering maturity experience! I led her down the maturity model and industry led certification process.*** *Katie has done a remarkable job and does listen to industry, she is passionate and only wants to serve for the greater good. This is very hard please help us succeed. It really is important and time is not our friend.*

V/R

Kevin

Meanwhile, on LinkedIn, Ms. Arrington and Ms. Bostjanick had both begun to attack me personally, presumably in response to the article and White Paper. Mr. Bostjanick openly questioned my patriotism, and Ms. Arrington claimed I had no "validity" in the CMMC industry.

This, along with the Fahey response, indicated that the DoD CMMC managers had elected to attack the messenger, rather than understand the points being made to them related to inviting foreign actors into the CMMC oversight scheme.

CMMC-AB MISMANAGEMENT

At about the same time, around 20 September, Oxebridge began working behind the scenes with the CMMC-AB to provide a roadmap on how it might obtain ISO 17011 compliance without IAF oversight. A discussion was had about offering to pay Oxebridge, but we instead agreed to perform the work pro bono. At the request of Board Members, Oxebridge provided various PowerPoint slides showing an accreditation roadmap, with the hope that the CMMC-AB would provide this to the DoD as an alternative path forward. The materials aligned with the White Paper, allowing for independent oversight of the CMMC-AB without the use of foreign nationals or IAF/IAAC actors.

It is not clear what happened with the materials. Other board members later reported they never saw the materials, and that they had not been formally presented at any meetings. At the same time, Karlton Johnson and Yong Gon Chon took over as "acting" Board Chair and Treasurer respectively and adopted a posture that was subservient to Ms. Arrington and Mr. Fahey, leading some other Board members to resign. The new leadership rejected outside advice, and adopted a hostile response to criticism. Mr. Chon likewise began making personal attacks on LinkedIn, while Mr. Johnson and fellow Board member Jeff Dalton elected to "block" Oxebridge posts from their view entirely.

These actions show that the CMMC-AB had been notified of the risks of inviting the IAF and IAAC into their oversight, but took concrete and deliberate actions to ignore these risks, without concern for national security.

CONCLUSION

The decision by the DoD OUSD A&S office, along with those within the CMMC-AB leadership, to require CMMC scheme oversight by bodies owned and operated by foreign nationals ***poses a direct and imminent risk to the United States' national security.*** By requiring the CMMC-AB to subject itself to oversight by the IAAC, it forces the CMMC-AB, its C3PAOs, and those DIB companies pursuing CMMC certification to reveal potentially sensitive information and details about the nation's cybersecurity maturity and, more frighteningly, specific weaknesses in our cybersecurity defense.

The only course of action is that the DoD contract with the CMMC-AB must be immediately canceled, and replaced with a new contract that utilizes a plan whereby independent oversight of the CMMC-AB can be done by either the DoD itself, or by US-based ombudsman organization, as suggested in the original Oxebridge White Paper from September 2020.

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.

www.oxebridge.com