

## **The TIC Council Comments to the Qualification Process for Cybersecurity Maturity Model Certification “CMMC” CMMC 3<sup>rd</sup> Party Assessment Organization “C3PAO”**

The TIC Council would like to comment on the CMMC program’s C3PAO application for certification requirements as published. TIC Council is a global association representing over 90 international independent third-party testing, inspection, certification, and verification organizations. Testing, Inspection and Certification (TIC) companies cater to a diverse range of industry sectors and a variety of standards and legislation. The industry represents an estimated one million employees across the world. The purpose of the TIC Council’s comments is to provide awareness to items impacting full operational functionality of the CMMC program, specifically when operating the CMMC program at expected capacity, and within the published C3PAO application requirements.

### **Resource burden**

The TIC Council has noted a majority of the currently approved C3PAOs are **not** accredited. The CMMC application requirements would also require the currently unaccredited C3PAOs to become ISO 17020 accredited in the period specified. We strongly support the need for accreditation to ISO 17020 to help ensure that all providers are qualified to support the needs of the program.

Global TIC organizations are currently prepared to become 3CPAOs with ISO 17020 compliant management systems to immediately support and engage in the program. Increasing the ability to introduce these accredited global TIC organizations into the program will alleviate the burden to operate the CMMC program at expected capacity, while unaccredited 3CPAOs go through the rigors of ISO 17020 accreditation. Under the current 3CPAO approval process there will be few (if any) applicants that meet the requisite accreditation qualifications. The need for accreditation services coupled with the lack of current qualified resources will impact the ability of this program to provide the assurance that is needed in evaluation/ approval of DoD contractors in accordance with CMMC program requirements.

### **Untapped international resources**

Further burdening the current CMMC program the inability to engage the available resources within the global TIC industry. The new US administration can incorporate the global TIC industry in this CMMC government program by expanding the C3PAO application requirements to include foreign owned accredited TIC organizations that are also located in the United States.

The current application requirements for the C3PAO limits the goals of the program to *“support of the global supply chain”* thorough the requirement for participation of only US citizen owned companies/ corporations. The C3PAO application process’ strict requirements inherently exclude the most qualified and experienced service providers. Many of the largest TIC Sector organizations do

not meet this requirement, resulting in a lack of qualified services providers to implement the program.

TIC Council member organizations currently certify for DIB supply chain vendors to ISO standards, such as ISO 9001, AS9100, ISO 27001 in highly sensitive areas by using US Citizen auditors and back-office staff, as necessary.

### **Need for institutional knowledge and experience**

Newly approved, but **unaccredited** C3PAO entities, are inexperienced and will face hurdles in achieving ISO 17020 (or similar accreditation). This lack of experiential knowledge will create a “certification bandwidth” issue, requiring many to seek out the necessary training for their staff to meet the requirements of ISO accreditation.

Many of the TIC Council organizations are ISO accredited, and are currently providing these services. These TIC Council organizations are qualified and ready to implement this program. In addition, the accredited TIC industry brings a wealth of experience and knowledge, along with a global network of experts to deal with the risks related to data protection, impartiality, and conflict of interest.

### **In summary**

The ISO 27001 Certification Scheme has been available to the market since 2013; and today there are roughly 36,000 certified organizations around the world. With a global network of auditors, the TIC Council organizations manage the certification process for ISO 27001, under accredited schemes based on ISO 17021. This has proven to be an effective framework for Information Security Management Systems.

It is the TIC Council’s position to expand the inclusiveness of the application process to accommodate for the above without prejudice to a TIC organization’s corporate structure, nationality of ownership or association with foreign affiliates, and stay the course with required ISO accreditations. The program can immediately be opened to fully accredited ISO 17020 or ISO 17021 TIC organizations to achieve early adoption of the processes defined by these international standards and by doing so, further strengthen the CMMC program outlook for fast adoption and implementation.

**Contact person:** Karin Athanas, Executive Director, TIC Council Americas, [kathanas@tic-council.org](mailto:kathanas@tic-council.org)

**TIC Council** is a global association representing over 90 international independent third-party testing, inspection, certification, and verification organizations. Testing, Inspection and Certification (TIC) companies cater to a diverse range of industry sectors and a variety of standards and legislation. The industry represents an estimated one million employees across the world with annual sales of approximately USD 200 billion. For further information please see the [Report on the TIC sector](#).