Draft Proposal to Director, CMMC regarding the Consideration of Certain Foreign-Owned Assurance Companies as CMMC Third-Party Assessor Organizations

Proposal

Definition of qualified contractor for third-party assessment of cybersecurity.

A qualified contractor for third-party cybersecurity assessment of a defense contractor in the United States includes a company that meets the following requirements:

> (a). The contractor is a United States subsidiary of a company headquartered in a country that has a defense industrial cooperation agreement with the United States; and
>
> (b). The Government of the country with whom the United States has the defense cooperation agreement has signified in writing to the Secretary of Defense that the company is established and well-recognized in that country and that the Government supports its application as a third-party cybersecurity assessment organization to the U.S. Department of Defense.

Explanation and Justification:

The U.S. Government and its trusted international defense partners are rightly concerned about the security of sensitive unclassified information generated by or shared with companies within the U.S. Defense Industrial Base, whether domestic or foreign. The U.S. and its trusted defense partners have recognized the critical contributions that they make to each other's national security and have established avenues to foster more active sharing of knowledge, technology, products, and services between them through mutual defense industrial cooperation agreements.

The Department's proposed CMMC program is a laudable step in protecting sensitive unclassified information within the U.S. Defense Industrial Base (DIB). The security of such information is in the interests of both the United States, its trusted international defense partners, and the U.S. and foreign companies that make up the DIB. Likewise, the United States' trusted defense partners can and wish to contribute to the success the CMMC program. One avenue is through the participation of qualified independent assurance companies as accredited CMMC Third-Party Assessor Organizations.

The U.S. Department of Defense has long relied on independent, third-party certification and verification to assure them that their suppliers uphold and deliver on the highest standards of quality and safety. Since 1999, the AS 9100 Quality Management System for the Aviation, Space, and Defense Industry has been the flagship standard.[1] Major aerospace and defense suppliers worldwide require

[1] Prior to development of AS 9100, the U.S. military applied two specifications to supplier quality and inspection programs: MIL-Q-9858A Quality Program Requirements, and MIL-I-45208A Inspection System Requirements. For years these specifications represented the basic tenets of the aerospace and defense industry. The U.S. Government withdrew those two quality standards when it adopted ISO 9001. Large aerospace companies then began requiring their suppliers to develop quality programs based on ISO 9001. As aerospace suppliers soon found that ISO 9001 did not address the specific requirements of their customers, including the U.S. DOD, NASA, FAA, and commercial aerospace companies including Boeing, Lockheed Martin, Northrop Grumman, GE Aircraft Engines and Pratt & Whitney, they developed AS 9100, based on ISO 9001, to provide a specific quality management standard for the aerospace industry.

independent certification of compliance with AS 9100 as a condition of doing business with them. This certification work is done by accredited certification bodies, including such globally recognized names as DNV, BV, BSI, Intertek, LRQA, SGS, and TÜV, among others. Thus, the U.S. subsidiaries of foreign-owned assurance companies are already extensively involved in providing independent quality assurance and inspection verification services to U.S. defense contractors. These inspection services have kept the U.S. defense contractors protected and they are comfortable with using these services. Now is not the time to strike this arrangement either directly or as a matter of policy.

The smooth, rapid rollout of the Defense Department's CMMC program would benefit greatly by the involvement of a defense contractor's ISO 9001 / AS 9100 certifier. The NIST cybersecurity standards upon which the CMMC program is built are largely analogous to those in the ISO 27001 Information Security standard. To comply with either the NIST or ISO standards, a company must effectively integrate the underlying cybersecurity principles and methods into its overarching management systems. For defense contractors that already certify their management systems to the ISO/AS standards, it would be most efficient to conduct CMMC certification in parallel with their ISO/AS management systems certification, with both activities performed by the same organization. Performing the work concurrently increases audit efficiency and validity, thereby reducing both direct and indirect costs, including the defense contractor's own staff resources necessary to facilitate the relevant audits.