ACEC
American Council of Engineering Companies

February 26, 2024

Ms. Diane Knight
Office of the DoD Chief Information Officer
Department of Defense
4800 Mark Center Drive, Suite 11G14
Alexandria, VA 22350

RE: ACEC Comments on the Cybersecurity Maturity Model Certification (CMMC) Program (Docket ID: DoD-2023-OS-0063)

Dear Ms. Knight:

The following comments are submitted on behalf of the American Council of Engineering Companies (ACEC). Founded in 1906, ACEC is a national federation of 51 state and regional organizations representing more than 5,600 engineering firms and 600,000+ engineers, surveyors, architects, and other specialists nationwide. As the business association of the nation's engineering industry, ACEC member firms drive the design of America's infrastructure and built environment.

ACEC member firms are engaged in a wide range of engineering works that support the quality of life, including transportation, energy, and water infrastructure onboard American military installations, as well as in support of civil works projects of the Army Corps of Engineers, such as levees, dams, and our nation's waterways.

The Council welcomes this opportunity to provide input and seek clarifications on the proposed rule entitled "Cybersecurity Maturity Model Certification (CMMC) Program," as published in the Federal Register on December 26, 2023, as **Docket ID: DoD-2023-OS-0063**. Within this rule, the DoD CIO proposes "to establish requirements for a comprehensive and scalable assessment mechanism to ensure defense contractors and subcontractors have, as part of the Cybersecurity Maturity Model Certification (CMMC) Program, implemented required security measures to expand the application of existing security requirements for Federal Contract Information (FCI) and add new Controlled Unclassified Information (CUI) security requirements for certain priority programs.

Controlled Unclassified Information (CUI)

ACEC member firms continue to express frustration with the defense services' contracting community's inconsistent application of CUI and requests that the Department and the services uniformly define what constitutes CUI as clearly as possible. In addition, more specific guidance is needed for the DoD contracting community on how to categorize the proper CMMC Level. It is the view of ACEC that establishing a clear definition and standards for CUI will help

maximize participation by the industrial base, while saving time and money for the government, industry, and the American taxpayer. A considered review may lead DoD to conclude that a good portion of AEC (Architecture, Engineering and Construction) documentation does not constitute CUI, in which event applying CMMC standards to all AEC documentation would result in excessive work and diversion of energy. Therefore, to the extent practicable, we request that DOD articulate what types of facilities and infrastructure will require Levels 1, 2, and/or 3 CMMC certification, so that industry may appropriately allocate resources to prepare for this requirement.

Adjustments to Contracting

DoD is provided broad discretion in Phase 1 to add the CMMC Levels 1 and 2 Self-Assessment requirements to the contract option period awards. Adding the CMMC Levels 1 and 2 Self-Assessments as part of the option period award will require DoD to adjust the contract ceiling price so that the incumbent contractor can comply. The uncertainty of whether and how these requirements will be applied puts contractors in a difficult position, as they may not have proposed on the original opportunity had these requirements been stated at the solicitation phase. Furthermore, if the contractor does not have a completed CMMC Levels 1 or 2 Self-Assessment, contracting officers are afforded an unfair opportunity to recompete the contract. **We recommend that the final rule include specific language about contract funding adjustments related to Level 2 Self-Assessments.**

Furthermore, DoD is given broad discretion in Phase 1 to add in CMMC Level 2 Certification Assessment. Such uncertainty as to whether the DoD will include the requirement in a solicitation creates challenges within the contractor industry in whether to compete for an opportunity or whether the contractor should invest in the opportunity depending on the CMMC Program requirements. Industry stakeholders can better plan with certainty when the rule takes effect. The Council believes the government should consider removing this discretion. **We recommend the final rule consider only an "either on or off approach" rather than the discretionary choices by the DoD.**

Cost to Implement

The cost impact analysis provided within the draft rule does not account for associated cost increases and schedule delays that will have a direct impact on the warfighter and the taxpayer. Accounting for these costs would reveal the full cost to the government which in turn would allow for more flexibility in the defense of funding for initiatives to keep the warfighter and the economy whole. The costs for implementing compliance and certifying against the standards are likely to exceed those in the proposed rule.

The investment required for Information Technology infrastructure and systems compliance far outweighs the expense of certification. Firms of all sizes are faced with the unique challenges of implementing CMMC. For smaller firms, the costs will be an overwhelming expenditure, which will need to be done right the first time. Larger firms continue to experience multi-million-dollar costs for implementation, which dwarfs the certification and self-assessment cost.

The DoD's position is "to the extent that defense contractors or subcontractors have already been awarded DoD contracts or subcontracts that include these clauses, and process, store, or transmit FCI or CUI in support of the performance of those contracts, costs for implementing those

cybersecurity requirements should have already been incurred." We believe this hard line will impact the ability of contractors to maintain compliance with SB/SDB quotas as will DoD be challenged in meeting their quotas. The DoD's strategy needs to find a balance that protects information without ignoring the unintended consequences and impacts to our warfighters. Although this may be perceived to be an issue for the industry to resolve, the concern is that this will quickly become an issue impacting the DoD and the readiness of our warfighters by introducing significant and direct impacts on capability, cost, and schedule and thus reducing the DIB pool, particularly the SB community.

Impact on International Partners

Multinational A/E firms routinely depend on local firms to support contractual requirements in foreign countries. The rule as written will significantly impact the ability of these multinational companies to fully support the DoD's overseas mission. The final rule should clarify how multinational corporations with facilities abroad supporting DoD clients and or non-US organizations (e.g., construction contractors abroad) are expected to comply with CMMC given US-centric aspects of many of the underlying requirements such as CUI, CAGE codes, and more. **Foreign partners must be provided clear guidance when supporting US firms that is transparent, understandable and does not interfere with operations.**

Contractor information systems are an aggregate of information systems as opposed to a singular system. As such they are dynamic and complex environments supporting various clients and governments globally. A significant probability exists that in maintaining a certified environment, challenges will occur that require remediation. The A/E industry works alongside many external partners, it is a responsibility and burden that must be spread throughout the supply chain. The American engineering industry strives to work closely with each of our federal clients as these requirements take effect.

We appreciate the Department's work to implement CMMC and their interest in working with their private industry stakeholders on this critical effort. For additional questions, please contact Dan Hilton at dhilton@acec.org.