ACEC
American Council of Engineering Companies

March 17, 2025

General Services Administration
Regulatory Secretariat Division
1800 F Street NW, 2nd Floor
Washington, DC 20405

RE: Controlled Unclassified Information (FAR Case 2017-016)

Dear FAR Council:

Please accept these comments on behalf of the American Council of Engineering Companies (ACEC) – the business association of the nation's engineering industry. Founded in 1906, ACEC is a national federation of 51 state and regional organizations representing nearly 5,500 engineering firms and nearly 600,000 engineers, surveyors, architects, and other specialists nationwide. ACEC member firms drive the design of America's infrastructure and built environment.

ACEC appreciates the desire to protect information our government has and shares with private sector partners. We recognize the nearly fifteen-year administrative history of this proposed rule going back to Executive Order 13556, "Controlled Unclassified Information" and the National Archives and Records Administration (NARA) final rule in 2016 that established policies for agencies on designating, marking, safeguarding, disseminating, and disposing of CUI, which was codified at 32 CFR Part 2002.

Government agencies struggle following their own procedures on CUI. Many examples exist in recent years of documents or presentations marked CUI or "For Official Use Only" (FOUO) posted to public government websites. Much work remains to educate government and industry personnel about existing procedures beyond the procedures contemplated in this proposed rule.

This proposed rule is especially significant as it introduces new obligations for contractors with civilian agencies that are like, but not the same as, existing requirements under DFARS clause 252.204-7012. The proposed rule introduces significant new requirements for contractors and subcontractors, posing challenges across the federal contracting ecosystem. While the proposed rule aligns with established security standards like NIST SP 800-171 and simplifies compliance compared to the Department of Defense Cybersecurity Maturity Model Certification (CMMC) Program, the proposed rule's reliance on self-attestation and lack of tailored support for small businesses could limit its effectiveness while increasing contractor liability. The comprehensive information to be included on the new Form SF XXX (Controlled Unclassified Information [CUI] Requirements) will be invaluable in supporting contractors in making bid decisions and in implementing correct controls during contract execution. However, contractors will be reliant on

Government agencies providing accurate and complete information on the Form SF XXX. Unmarked or mismarked CUI is not considered a CUI incident unless the mismarking or lack of marking has resulted in the mishandling or improper dissemination of the information. Government agencies will understandably be unfamiliar with this new form during its initial use, which will result in increased contractor risk over an indefinite timeframe. Below are some unresolved questions from our member companies:

- Are terms in the SF XXX negotiable, i.e., use of CUI with third parties for the purpose of private sector business transactions?
- Is the SF XXX leveraged in the RFP process, or after the contract has been awarded?
- Does change in the SF XXX at any point in the contract require a contract modification or bilateral renegotiation?
- If CUI is identified and reported in the contract, but the SF XXX is not amended to cover the additional CUI, is there any responsibility to protect that data?

Definition and Application

The proposed rule states, "to the maximum extent practicable, the offeror or contractor shall identify and mark its proprietary business and attributional information. These costs are also not quantified since an offeror or contractor usually marks its proprietary information as a best business practice to protect its own interests and information." This assumption is true of basic offerings and deliverables but does not consider other government deliverable products that may not traditionally be marked as propriety information, such as rendering or engineering drafts/drawings/models. ***Consider applications for architectural and engineering physical and digital models.***

Application to Critical Infrastructure

The proposed rule does not address the proliferation of CUI information outside of direct contracts, for instance, commercial contracts between two private entities for engineering or design of facilities, structures, equipment, etc. that may include CUI data, but are not directly related to the government contract. FERC CEII data is one example, which has often is not marked, and is discovered post-contract execution. This issue is extremely common and further exacerbates the mishandling of CUI information outside of government control. ***Consider specifying not just subcontractors, but any proliferation of CUI information that may or may not be directly linked to government contracts, but still requires CUI data in order to complete the assigned work or service.***

Small Business Impact

Smaller contractors may struggle with the costs and technical expertise required to implement NIST SP 800-171 controls. This could also cause smaller businesses to exit the market because the complicated (and inconsistent) contract requirements are increasing at an unsustainable rate surpassing their ability to invest in security practices to compete. The risk associated with the potential release of proprietary information and the associated penalties could be too much for some small businesses. ***Consider a phase in period for small businesses.***

Self-Attestation

The lack of a certification process may leave gaps in enforcement and accountability. The FAR Council noted that they did not believe it necessary to adopt a "100 percent inspection requirement." The proposed rule also reminds contracting officers that they should not interpret a contractor's CUI incident report to mean that any entity or person failed to provide adequate safeguards. Indeed, cybersecurity incidents can happen to entities with significant controls and an entity should not be punished for coming forward. The government, however, still retains significant authority to inspect a company's compliance at any time, and has many means for enforcement. Just as the government has threatened or done with other cybersecurity requirements, it could attempt to leverage its wide-ranging enforcement tools, including contractual remedies, the False Claims Act, and suspension or debarment. The proposed rule does not specify how the government would pursue such a claim. Would the contracting officer do so on behalf of the government under the Contract Disputes Act?

Incident Response and Reporting

The new eight-hour time trigger is an extremely compressed timeframe and will be difficult to integrate into policies, including incident response plans. This is a notable deviation from the DFARS 252.204-7012 incident reporting process, which requires subcontractors to report directly to the government. The revised process contemplates that subcontractors will notify the prime contractor or next higher-tier subcontractor of incidents within the same 8-hour window. The proposed rule is not clear as to whether this is in addition to or instead of reporting to the agency website or single point of contact. ***We request that the FAR Council revise the proposed FAR 4.403-4 eight-hour timeframe for reporting Controlled Unclassified Information (CUI) Incidents to 72 hours, in alignment with the DFARS 252.204-7012 cyber incident reporting requirement. While we recognize the importance of timely reporting, as well as the difference in definition between a "cyber incident" under DFARS 252.204-7012 and the proposed definition of a "CUI Information Incident" under FAR 2.101, eight hours is an extremely compressed timeframe for the required information to be assembled. We also request that subcontractors report cyber incidents directly to the government. Consider the use of existing processes for government wide reporting such as the Supplier Performance Risk System (SPRS) or DIBnet.***

Coordination Not Necessarily Harmonization

The proposed rule could benefit from addressing lessons learned from the DoD's CMMC framework, such as ensuring clear guidance, equitable resource allocation, and streamlined compliance processes. However, the two efforts do not seem to be sharing comments, which may result in contractors being confused when facing this proposed rule, the final CMMC acquisition rule, and the increasing litany of new requirements.

The proposed rule has a potential inconsistency with 32 CFR 170, which allows for FedRAMP Moderate Baseline or "Equivalent." The ability to pursue a Third-Party Assessing Organization (3PAO) provided some flexibility for cloud services that met the baseline requirements, but were held up by unreasonably long approval timelines. ***We recommend adjusting language to include an "equivalent" option by citing existing FedRAMP requirements – whatever they are as they are updated and evolve over time.***

Existing Regulatory Freeze and Ten for One Rule

We support efforts to strengthen cybersecurity practices and understand that companies who support our government are critical partners in protecting information from malicious entities. Consistent with Executive Order 14192 titled "Unleashing Prosperity Through Deregulation," how does this rule get through the regulatory freeze and the requirement to eliminate ten rules for every new regulation? As acquisition streamlining initiatives are underway, it is important for the executive branch, Congress, and the FAR Council to prevent creating a two-tiered acquisition system 1) for FAR based contracts that have established rules and 2) other acquisition mechanisms where the risk of cyber incidents and critical information loss remain, but lack additional terms and safeguards for both government and industry.

Thank you for your consideration of our comments.

Respectfully,

Bradley J. Saull
Vice President, Federal & International Programs
American Council of Engineering Companies (ACEC)