THE COALITION FOR COMMON SENSE IN GOVERNMENT PROCUREMENT

July 23, 2026

Federal Acquisition Regulatory Council
Washington, D.C.
Via Federal eRulemaking Portal: https://www.regulations.gov

Subject: Comments on FAR Part 40 (FAR Case 2026-001), 91 FR 37550

The Coalition for Common Sense in Government Procurement (Coalition) appreciates the opportunity to comment on the Federal Acquisition Regulatory Council's proposed rule with respect to Federal Acquisition Regulation (FAR) Part 40 (Information Security and Supply Chain Security) and related clauses in Part 52.

By way of background, the Coalition is a non-profit association of firms selling commercial products and services to the Federal Government. In Fiscal Year 2025, its members collectively delivered over $170 billion in goods and services to the Federal Government. These members include small, medium, and large business concerns. The Coalition is proud to have collaborated with Government officials for more than 45 years promoting the mutual goal of common-sense acquisition.

FAR clause 52.240-6 (Notice of Controlled Unclassified Information Requirements)

With respect to paragraph (b)(1), the requirements related to Government information that the contractor cannot use for "its own purposes" unless the information is in the public domain or made available by a non-Government source are overbroad and unnecessary. The intent of the clause is to provide notice of Controlled Unclassified Information (CUI). A contractor's ability to use Government-provided information should be governed by the data rights provisions in the contract and the phrase for "its own purposes" could be interpreted so broadly that it encompasses lawful activities.

With respect to paragraph (b)(2), the Coalition recommends that the FAR Council remove references to the broader, sometimes inconsistent, CUI provisions in 32 CFR Part 2002. Offerors should only be bound by the solicitation specific CUI handling procedures an agency chooses to provide.

With respect to paragraph (c), the requirement to report unmarked or mismarked CUI within 72 hours should be removed. Agencies should be solely responsible for properly marking CUI in a solicitation. This burden should not be shifted to offerors. Contracting officers should be trained to limit CUI use in the solicitation phase. Prospective offerors are not even under contract at this stage, and it is questionable how this clause will be effective and when the obligations for non-awardees under the clause cease.

With respect to paragraph (d), the purpose of 52.240-6 is to protect CUI within the solicitation and alert contractors to the fact that CUI may be used in performance of the contract. The reporting of non-compliance with respect to CUI is addressed in FAR clause 52.240-7. Thus, there is no reason to address reporting of non-compliance or provide a plan of action and milestones in 52.240-6. Further, 52.240-6's requirement to report "any" non-compliance with 52.204-7 goes beyond the requirements of 52.204-7 and will lead to over-disclosure and unnecessary reporting. In addition, the requirement to disclose plans of actions and milestones could expose vulnerabilities that could be exploited by malicious actors. For that reason, contractors typically don't share that information in written form even with auditors and instead share that information through a secure viewing platform. The Department of War (DoW) has established the SPRS database that requires contractors to report their compliance with NIST 800-171, Rev 2. The FAR Council should leverage the SPRS database or adopt an equivalent database for non-DoW agencies so that offerors don't have to submit such information in a potentially unsecure manner. Creation of a database or utilization of the DoW database would help ensure that only offerors with compliant systems are provided access to CUI.

FAR clause 52.240-7 (Controlled Unclassified Information)

With respect to paragraph (b) and the definition of "CUI incidents," the Coalition supports the definition, and we appreciate the clarification that "[i]mproper handling of CUI (e.g., unmarked or mismarked CUI) is not a CUI incident unless the improper handling has resulted in an unauthorized disclosure, improper modification, or improper destruction of CUI."

With respect to paragraph (b) and the definition of "Unauthorized disclosure," we recommend that the rule be adjusted to focus on disclosure, access, or observation of CUI by an unauthorized person. This would make the rule more consistent with DFARS 252.204-7012 (e.g, "Compromise" means disclosure of information to unauthorized persons…). If an authorized person accesses or observes CUI in a method that is counter to an internal policy this should not be viewed as an unauthorized disclosure.

With respect to paragraph (c)(1)(ii), the requirement to report any inconsistency between the clause and the SF Form XXX is ambiguous. Contractors are already required to report CUI that is not identified in the SF Form XXX or is not marked or properly marked under paragraph (c)(1)(i). The Government should not be shifting this administrative burden to contractors.

With respect to paragraph (c)(3), as discussed above, the requirements related to information that the contractor may not use for "its own purposes" depending on whether the information is in the public domain or provided by a non-Government source are unnecessary and ambiguous. Complying with the CUI requirements is burdensome enough for industry, and additional requirements are outside the confines of this clause.

With respect to paragraph (d)(1), we again recommend the removal of references to 32 CFR Part 2002. The requirements for handling CUI under a specific contract should be set forth by the agency in the contract and SF Form XXX, and not be based on broader, potentially inconsistent, general standards.

DoW uses NIST SP 800-171, Rev. 2 for its CUI safeguarding clause (DFARS 252.204-7012) and Cybersecurity Maturity Model Certification (CMMC). The FAR Council is proposing to use NIST SP 800-171, Rev. 3 for civilian agencies. It would be helpful for industry for the Federal Government to use the same cybersecurity standard, and to coordinate the migration to higher standards so that contractors do not have to manage compliance with multiple standards.

FAR 40.303-2

With respect to "Covered Federal information," we recommend that FAR 40.303-2 provide an exception for commercial off-the-shelf items (COTS), consistent with FAR 40.304-7(b) which exempts solicitations and contracts for COTS from the requirements related to CUI.

FAR clause 52.240-5 (Covered Federal Information)

We are concerned that using the term "Covered Federal information" instead of "Federal Contract information" will confuse industry as the term "Federal Contract Information" has already been defined by DoW with respect to CMMC. In accordance with this Administration's executive orders on returning common sense to Federal acquisition, consistent definitions, reporting timelines, and standards should be utilized throughout the Federal Government to the maximum extent possible.

With respect to paragraph (b)(2) "Other handling requirements," it is unclear when this would apply, i.e., covered Federal information should not be handled outside of a covered contractor information system.

FAR clause 52.240-2 (Security Prohibitions and Exclusions—Representations and Certifications)

We encourage the Government to create a search mechanism within the System for Award Management (SAM) for "covered procurement actions," similar to the search mechanism in SAM for Federal Acquisition Supply Chain Security Act orders.

FAR Part 52

We concur with the FAR Council's plan to establish a new subpart in part 52 and renumber all new provisions and clauses under 52.4 to provide a distinction between the old clauses and provisions under 52.2.

The Coalition hopes you find these comments useful and thanks you for your time and consideration. If you have any questions, I may be reached at (202) 315-1053 or rwaldron@thecgp.org.

Regards,

Roger Waldron
President