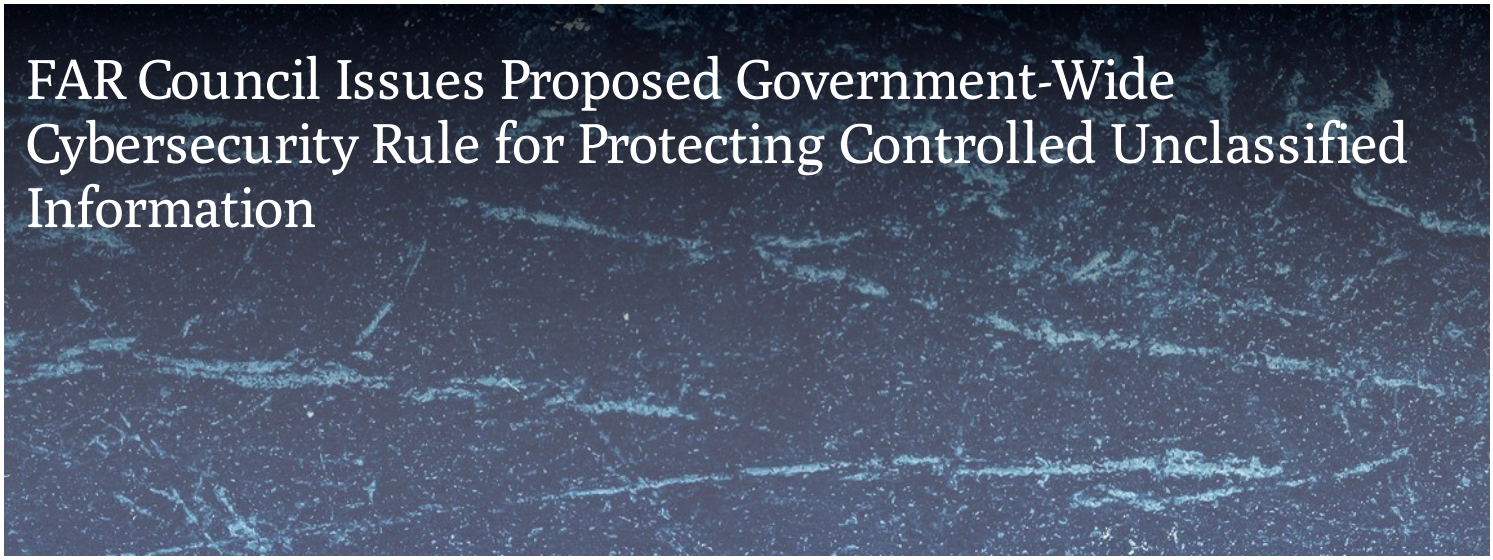
WINSTON & STRAWN LLP

BLOG

FAR Council Issues Proposed Government-Wide Cybersecurity Rule for Protecting Controlled Unclassified Information



FEBRUARY 4, 2025

On January 15, 2025, the Federal Acquisition Regulation (FAR) Council issued a proposed cybersecurity rule to implement the National Archives and Records Administration's (NARA) Controlled Unclassified Information (CUI) Program across all federal agencies. This Proposed Rule (Proposed Rule) will impose requirements on all federal contractors that are substantially similar to those that DOD contractors and subcontractors have wrestled with for many years. Existing DOD contractors that have been complying with Defense Federal Acquisition Regulations Supplement (DFARS) CUI clauses, such as DFARS 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting" (7012 Clause) and DFARS 252.204-7021 "Cybersecurity Maturity Model Certification Requirements," will have an easier time complying with the requirements of the FAR CUI Rule. However, they will still need to adjust some procedures in order to comply with the requirements in the Proposed Rule. Comments to the proposed rule must be submitted by March 17, 2025, in order to be considered in the formation of the final rule.

The Proposed Rule is for a government-wide cybersecurity rule that will establish uniform requirements for how the government and federal contractors will manage CUI. The Proposed Rule introduces a variety of new clauses, definitions, requirements and standard forms, and also revises existing FAR clauses and numbering, including:

- Adding a new standard form, SF XXX Controlled Unclassified Information Requirements, which will be used to help federal agencies and contractors consistently identify CUI and handling requirements. This form will be included in all solicitations and contracts that will require the handling of CUI.
- Requiring Prime contractors receiving form SF XXX to prepare a SF XXX for distribution to any subcontractors that will handle CUI to ensure proper handling and safeguards for CUI.
- Specifying contractor training in form SF XXX that must be completed before any employee can handle CUI.
- The Proposed Rule creates three new FAR clauses:
  - **FAR clause 52.204-WW, Notice of Controlled Unclassified Information Requirements**, will inform offerors of requirements on restricted use of Government-provided information. It will also instruct offerors on how to identify sensitive offeror information and will specify how to notify the Government regarding unmarked or mismarked CUI.

- **FAR clause 52.204-XX, Controlled Unclassified Information**, is modeled after the 7012 Clause and will require contractors to comply with applicable CUI requirements for handling the CUI specified in SF XXX.
- **FAR clause 52.204-YY, Identifying and Reporting Information That Is Potentially Controlled Unclassified Information**, is used where the government has indicated on the SF XXX that no CUI is involved in the performance of the contract. This clause requires the Contractor to notify the government if there appears to be unmarked or mismarked CUI involved in the performance of the contract, or a suspected CUI incident.

- New definitions also are added, moved, and revised by the Proposed Rule to clarify requirements, including:
  - FAR 2.101 adds new definitions for "contractor-attributional information," "controlled unclassified information (CUI)," "CUI incident," "CUI Registry," "Federal information system," and "Information system," and removes the definition for "Federally-controlled information system."
  - FAR 4.403-1 adds definitions for "CUI Basic," "CUI categories," "CUI Specified," "handling," "lawful Government purpose," "limited dissemination control," and "on behalf of an agency."
  - FAR 4.401 adds a revised definition for "information" that was moved from FAR 4.1901 as well as definitions for "covered contractor information system" and "covered Federal information."
  - The term "Federal contract information" was changed to "covered Federal information" to align with the term "covered contractor information system."
  - FAR 52.204-21 revises the definition of "covered Federal information" to align with FAR 4.401.
- The Proposed Rule includes a requirement for contractors to report suspected or confirmed CUI incidents within 8 hours. Offerors and contractors must also notify the government within 8 hours in the event any unmarked or mismarked CUI is discovered.
- The Proposed Rule requires contractors operating Federal information systems that handle CUI to comply with agency-identified security controls from NIST SP 800-53 and any other requirements identified in the SF XXX. Cloud service providers must meet Federal Risk and Authorization Management Program (FedRAMP) Moderate Baseline requirements established by the government.

As noted above, the proposed new FAR 52.204-XX was modeled after and therefore has some similarities to the 7012 Clause. For example, both rules mandate compliance with NIST SP 800-171 for protecting CUI on non-federal information systems and include cybersecurity incident reporting requirements. That said, there are distinctions between the Proposed Rule and the 7012 Clause that are worth noting. For example:

ASPECT	FAR CUI RULE	DFARS 252.204-7012
Applicability	Applies across all federal agencies and contractors.	Limited to DoD contracts or subcontracts.
Identification of CUI	Introduces a Standard Form (SF XXX) to define CUI.	CUI is typically identified in the contract.
NIST 800-171 Version	Presently specifies implementation of the requirements of NIST SP 800-171 Revision 2, and defers any implementation of NIST SP 800-171 Revision	Specifies the security requirements of NIST SP 800-171 in effect at the time the solicitation is issued or as authorized by the Contracting Officer, but a DOD Class Deviation specifies compliance with NIST SP 800-171 Revision 2, instead of the

	3 (or a current version) to future rulemaking.	version of NIST SP 800-171 in effect at the time the solicitation is issued.
Cybersecurity Certification	No explicit certification requirements (yet).	Requires a tiered CMMC certification (Level 1-3).
Incident Reporting Details	Requires contractors to report any suspected or confirmed CUI incident to the agency website or point of contact identified in the SF XXX within 8 hours of discovery.	Requires contractors to "rapidly report" cyber incidents, which is defined as within 72 hours of discovery of any cyber incident.

CONCLUSION AND IMPLICATIONS FOR CONTRACTORS

The Proposed Rule aims to create uniform CUI practices across all federal agencies, which may reduce confusion for contractors working with multiple agencies. Existing DOD contractors will no doubt be more readily able to adjust to the requirements of the new FAR CUI rule, but those contractors that do not do work with the DOD will plainly have a steep learning and compliance curve to master. While the Proposed Rule does not presently include an analog to CMMC certification requirements, it is likely that a final FAR CUI Rule will adopt such a requirement. Contractors previously focused on DOD compliance will, once the Proposed Rule is made final, need evaluate their systems and practices for FAR-specific adjustments, particularly the identification of CUI using the new SF XXX, and the requirements of 52.204-WW, 52.204-XX, and 52.204-YY. Contractors that wish to provide comments on the Proposed Rule must do so by March 17, 2025.

For more information, please contact the authors or your Winston & Strawn relationship partner.

5 Min Read

Authors

William T. Kirkwood

Lawrence S. Sher

Lawrence "Larry" Block

Elizabeth Leavy

Michael Hill

Warren Geary

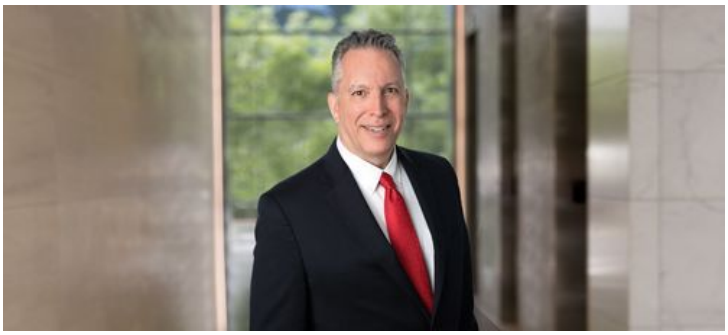
Related Topics

Federal Acquisition Regulation (FAR) | Cyber Security | Federal Contractors

Related Capabilities

Government Investigations, Enforcement & Compliance | Government Contracts & Grants

Related Professionals



William T. Kirkwood

Lawrence S. Sher

Lawrence “Larry” Block

Elizabeth Leavy

Michael Hill

Warren Geary

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.