JENNER & BLOCK

FAR Council Issues Long-Awaited Proposed Rule to Implement Controlled Unclassified Information Program

Client Alerts

January 21, 2025
By: Moshe B. Broder

On January 15, 2025, the Department of Defense (DOD), General Services Administration (GSA), and the National Aeronautics and Space Administration (NASA) (collectively, "the FAR Council") issued a long-anticipated proposed rule to amend the Federal Acquisition Regulation (FAR) to implement the National Archives and Records Administration's (NARA) Controlled Unclassified Information (CUI) Program. The CUI program establishes a unified approach to manage information that requires safeguarding or dissemination control by virtue of some law, regulation, or governmentwide policy. For government contractors tasked with protecting such unclassified information on federal or non-federal information systems, the proposed rule creates new compliance obligations and expectations. And given that recent enforcement actions have increasingly prioritized information protection and cybersecurity (as we covered here and here), contractors should pay close attention to these evolving requirements.

As background, stemming from a 2010 executive order establishing the executive branch's CUI program, and a 2017 notice of proposed rulemaking, this proposed rule offers a vision for implementing the NARA CUI program for virtually all federal contractors. The proposed rule provides details on how contractors will implement this program, including safeguarding, marking, and reporting the unauthorized disclosure or use of CUI.

By now, government contractors are widely aware that DOD has implemented the requirements of the CUI program through the clause at DFARS 252.204-7012 (the -7012 clause). Although the -7012 clause imposes obligations on companies that enter into contracts with DOD, there had been no parallel provision for "civilian" contractors doing business with non-DoD entities. Instead, the primary information security clause for such contractors, FAR 52.204-21 (the -21 clause), required the protection of a broad and loosely defined category of information known as Federal Contract Information. These compliance obligations were relatively modest compared to DOD's -7012 clause; rather than the 110 controls required by DOD under the -7012 clause, the -21 clause required only 15 security controls. Moreover, the FAR -21 clause lacked an explicit reporting timeline for incidents affecting such information.

But companies that do business with DOD are not the only ones that receive or generate CUI while performing contracts for the government, and the current proposed rule was intended to fill the gap to ensure consistent and widespread protection of CUI. In a proposed rule that purports to be "modeled after" the -7012 clause, the FAR Council has imposed parallel and in some cases more onerous restrictions on government contractors.

Most importantly, the proposed rule creates a parallel obligation already existing under the -7012 clause: contractors receiving or generating CUI on their own internal information systems must protect that information by implementing the 110 security controls set forth in NISP SP 800-171 rev 2. (The FAR Council acknowledged that, in May 2024, NIST published the third revision to NIST SP 800-171, but the proposed rule nonetheless requires contractors to implement the prior version, v2. Future rulemaking is expected to require compliance with the current version.)

Also significant is the proposed rule's eight-hour reporting requirement. Not only is this reporting time objectively brisk and also substantially shorter than the 72-hour timeline required by the -7012 clause, it is also apparently subject to variation where a "different time period is required for a specific category of CUI or a Federally controlled facility."

Moreover, under the proposed provision FAR 52.204-WW, an offeror must notify the Contracting Officer "if the Offeror discovers any CUI that is not marked, not properly marked, not identified on the SF XXX, or is involved in a suspected or confirmed CUI incident." Under the -7012 clause, by comparison, the obligation to report is limited to "cyber incidents," and there is no obligation to notify the government where CUI is not properly marked or identified. Notably, a literal application of the proposed rule has the potential to create a deluge of notifications, an outcome seemingly in tension with the proposed rule's estimate that there may be only "580 incident reports submitted each year."

The notification requirement is likely to trigger significant feedback from industry. The proposed rule includes a number of specific questions for public comment, including how contractors will handle disparate incident reporting timelines—an implicit recognition of these differences.

The proposed rule also introduces a new Standard Form, "SF XXX, Controlled Unclassified Information," that helpfully requires the government to identify the categories of CUI that will be provided under a contract. In practice, contracting activities often omit such guidance, leaving contractors unsure of the scope of compliance obligations. However, the relatively lengthy Standard Form (currently 16 pages) creates many opportunities for identifying various information relevant to CUI compliance, and it remains to be seen whether this will simplify and standardize compliance industry-wide (a central goal of the CUI program) or further complicate matters and create confusion.

Next, under the new clause FAR 52.204-XX, Controlled Unclassified Information, where a CUI Incident has occurred, and the contractor "is determined to be at fault for a CUI Incident (e.g., not

safeguarding CUI in accordance with contract requirements), the Contractor may be financially liable for Government costs incurred in the course of the response and mitigation efforts in addition to any other damages at law or remedies available to the Government for noncompliance." This cost-shifting term may be another significant area for contractor comment.

Finally, the proposed rule requires contractors to submit to the government the operative system security plan required by NIST SP 800-171 rev 2. The proposed rule states that such "validation" requests are intended to be "rare," and though the government can otherwise request a copy of such documentation via other means, contractors reporting a cyber incident should expect to be at increased risk of this type of scrutiny.

Comments on the proposed rule are due no later than March 17, 2025. Jenner & Block will continue to monitor developments in this area.

Related Attorneys

Moshe B. Broder
Partner
mbroder@jenner.com
+1 202 637 6334

Related Capabilities

Government Contractor Litigation and Compliance

615729. Information regarding the data we collect and the rights you have over your data can be found in our Privacy Notice. For further inquiries, please contact dataprotection@jenner.com.

Stay Informed →