GT GreenbergTraurig

Alert | Government Contracts

March 2025

Proposed FAR CUI Rulemaking Nears Comment Deadline

Go-To Guide:

- The comment period on the proposed FAR Controlled Unclassified Information (CUI) Rule closes Monday, March 17, 2025.
- To date, filed comments demonstrate core concerns, including the difficulty of complying with the eight-hour incident reporting requirement for potential CUI incidents or mismarked CUI.
- The FAR Council may issue the final rule later this year after adjudicating submitted comments and a 90-day Office of Information and Regulatory Affairs review period.
- Once the rule is finalized, government contractors performing work for any government agency who receive CUI must implement the security controls in NIST SP 800-171.

Despite the potentially sweeping impact of the proposed FAR CUI Rule (Proposed Rule), less than 30 comments have been filed to date during the comment period, which ends March 17, 2025. The FAR Council will adjudicate each of these comments, and any additional ones submitted by the deadline, before issuing the final rule, which may be expedited given the relatively low number of submissions.

The long-awaited Proposed Rule, published on Jan. 15, 2025, would implement the final piece of the National Archives and Records Administration (NARA)'s Federal Controlled Unclassified Information (CUI) Program, which dates back to 2010.

As we previously covered in a January 2025 GT Alert, the Proposed Rule would standardize cybersecurity requirements for all federal contractors and subcontractors and implement NARA's policies under 32 CFR part 2002. The Proposed Rule would also introduce new procedures, including reporting and compliance obligations, and define roles and responsibilities for both the government and contractors who handle CUI.

Commenters Express Common Concerns and Themes

Commenters expressed many of the same concerns, and the submitted comments correspond to common themes.

- The Eight-Hour Incident Reporting Timeframe Is Unreasonable. A key requirement under the Proposed Rule is to report a suspected or confirmed CUI incident within eight hours of discovery. This obligation also flows down to subcontractors and requires them to notify the prime or next higher tier subcontractor within the same eight-hour timeframe. Many commenters appear concerned about the potential burden and cost impact of this requirement, especially for small businesses. Commenters seek to align the reporting timeframe with other existing federal frameworks, such as the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), which calls for a 72-hour timeframe to report qualifying incidents to the Cybersecurity and Infrastructure Security Agency. Similarly, DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting) also requires defense contractors to "rapidly report" cyber incidents to the Department of Defense within 72 hours of discovery. Notably, the Proposed Rule does not attribute this eight-hour reporting requirement to defense contractors due to their existing obligations under DFARS 252.204-7012. Accordingly, maintaining the current expedited timeframe structure has potential to further complicate federal contractor and subcontractor obligations under the Proposed Rule, depending on which agency they are working with.
- The Definition and Scope of "CUI incident" Require Clarification. Under the Proposed Rule, FAR 2.101 would be amended to add "CUI incident," which shall be defined as "suspected or confirmed improper access, use, disclosure, modification, or destruction of CUI, in any form or medium." In response, several commenters have noted that this term is poorly defined and overly broad. Core to these commenters' concern is the related obligation for contractors to expeditiously report a suspected or confirmed CUI incident—a vaguely and broadly defined term would be potentially burdensome and drastically increase the number of reported events to the government. Given the breadth of the definition, the FAR Council's estimate of 580 incident reports annually might be a significant underestimation.
- Small Business Contractors Would Incur High Compliance Costs. The FAR Council estimates that non-defense contractors and subcontractors would incur labor, hardware, and software costs in order to comply with the Proposed Rule. For small businesses, the total initial year cost estimate is $175,700, with recurring annual costs expected to be $103,800. The Proposed Rule recognizes this impact and has engaged in a Regulatory Impact Analysis (RIA) that considers specific business concerns. In response, one commenter has detailed the potential outsized impact of the Proposed Rule on small businesses, which do not have dedicated compliance teams or the built-in expertise to continuously monitor their systems with in-house resources, structure incident reporting chains, or implement training programs. This commenter suggests that the FAR Council's estimate for training costs is underestimated. Such comments align with the FAR Council's express invitation for feedback from small entities on any RIA assumptions or other expected burdens that may help inform the final rule. However, to date, small business concerns and other interested parties have largely been absent from

the public comment efforts. Such entities should consider submitting comments to provide additional detail around the anticipated costs and considerations the RIA may have missed.

Other Concerns Raised

Some commenters have requested further guidance on how to handle legacy records and information that might have been previously designated as For Official Use Only (FOUO), a designation that is no longer utilized, and how those records would be marked under the CUI framework. Other comments request more guidance on how CUI would be identified, especially for small business concerns. While these are important considerations, they are likely outside of the current rulemaking's scope, which arises under Title 48 of the CFR (the acquisition regulation). The Proposed Rule implements NARA's CUI Program, which is separately described under 32 CFR part 2002, and which codified a standardized approach to designating, handling, and safeguarding CUI.

Additionally, some comments seek an extension of the public comment period. Given that the comment period remained in effect during the new administration's regulatory freeze pending review, it appears unlikely that a continuance will be granted, and the 60-day comment period may close as scheduled.

Interested contractors should submit their comments on the Proposed Rule by March 17, 2025. Given the relatively few comments received, the adjudication process may be quicker than originally anticipated. The FAR Council may issue the final rule in 2025, with standardized cybersecurity standards for all federal contractors and subcontractors going into effect and the clauses included in contracts by year end or early 2026.

Authors

This GT Alert was prepared by:

- Eleanor M. Ross | +1 202.530.8565 | Eleanor.Ross@gtlaw.com
- Cassidy Kim | +1 415.590.5133 | Cassidy.Kim@gtlaw.com
- Olivia Bellini | +1 703.903.7514 | Olivia.Bellini@gtlaw.com