LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

New Proposal For Controlled Information Not Entirely Realistic

By **Daniel Wilson**

Law360 (January 16, 2025, 10:34 PM EST) -- A proposed rule intended to clear up confusion and better protect controlled unclassified information via a governmentwide standard has created new uncertainties and could lead to unattainable demands such as unrealistic incident reporting deadlines.

After a long process kicked off by a 2010 executive order, the Federal Acquisition Regulatory Council formally published a proposal on Wednesday to implement a governmentwide definition and set of protections for controlled unclassified information — sensitive but unclassified federal information the government doesn't want made public.

Each federal agency can currently set its own standards for determining what it considers to be CUI and how it expects that information to be protected, but having a uniform definition and requirements will help eliminate inconsistencies and inefficiencies and improve the protection of that information, the FAR Council said.

However, the proposed rule, if finalized, would create new burdens for contractors in areas such as identifying and reporting potential CUI that cut against the goals of efficiency, consistency and protection, said Alex Major, co-chair of the government contracts group at McCarter & English LLP who focuses heavily on cybersecurity-related liability in his practice.

"I think they made the complicated issue of CUI maybe a little bit more complicated by removing any sense of certainty that previously existed," he said.

All contractors and contract bidders, even those that don't expect to handle CUI and haven't previously had to worry about protecting that information, will have new CUI-related requirements under the proposal, according to Crowell & Moring LLP partner Michael Gruden, a specialist in cybersecurity and data security issues.

"No matter who you are, whether you handle CUI or not, you'll have to know what it is," Gruden said. "Every company [working with the government] will need to know the categories of CUI, and ... what distinctly makes CUI itself CUI."

The proposal, for example, puts the onus on contractors in certain circumstances to inform agencies about any CUI they believe has been mismarked or left improperly unmarked by the agency and safeguard that information while a contracting officer makes a decision on whether it actually is CUI.

"If you miss something ... are you going to be on the hook for that?" asked Sheppard Mullin Richter & Hampton LLP partner Townsend Bourne, leader of the firm's governmental practice cybersecurity and data protection team. "Because that does seem incredibly unfair."

Reporting any mismarked CUI must also be done within a tight deadline of eight hours from discovery, a deadline that will also apply to contractors when there is a CUI-related incident, out of step with several existing federal requirements to report cybersecurity incidents within 72 hours — most federal cybersecurity rules are effectively aimed at protecting CUI — and likely difficult for many companies to comply with.

"Practically speaking, I don't really know how you even meet that [deadline] as a company, and I think especially for companies that already have multiple incident reporting regimes that they're thinking about, that eight-hour reporting requirement is going to be a burden to incorporate into their incident response plans," said Elle Ross, a senior associate at Greenberg Traurig LLP who frequently counsels clients on cybersecurity issues.

That deadline could also lead companies, acting out of an abundance of caution, to report potential incidents that, after further investigation, turn out not to have exposed any CUI, wasting time and resources for both the company and the government, attorneys said.

The rule also seeks to prevent a contractor or bidder from using any government-provided information, including CUI, "for its own purposes," unless that information is already public or provided by a third party, but doesn't explain what "its own purposes" means, according to Major.

"If you're responding to a CUI [request for proposals], then aren't you using it for your own purposes?" he asked.

And although the FAR Council said the rule is modeled after an existing Defense Federal Acquisition Regulation Supplement regulation, defense contractors can't simply use their existing CUI protection plans, as the new proposed rule differs in several significant ways, Gruden said.

For example, not only are there different incident reporting requirements, but contractors may also be required to describe their system security plans to the government and allow the government to review those plans in circumstances such as when a CUI incident is reported.

"Traditionally, contractors have not elected to provide [those plans], and consider those technical descriptions to be highly sensitive, highly proprietary," Gruden said. "But now with this requirement to essentially agree to produce your [system security plans] upon request from the government, that is significantly elevating legal compliance risk, especially when we think about the current era of [U.S. Department of Justice] cyber enforcement."

The proposed CUI rule will also require contractors to comply with Revision 2 of the National Institute of Standards and Technology's Special Publication 800-171, a set of security controls for protecting CUI stored or processed outside the government.

But Revision 2 is an older version of those standards, with NIST finalizing a new Revision 3 of SP 800-171 in May, paring down the number of controls and giving agencies more flexibility to tweak certain CUI security requirements to meet their specific needs, and the FAR Council said it "anticipates" the CUI rule will be updated at some unspecified point to include Revision 3, leaving contractors unsure about what

standard to shoot for ahead of a final rule.

"What they're basically saying [is], 'at some point in the nebulous future, we'll amend this,'" Ross said. "And I think that could be more difficult than people think, and I think it goes back to, potentially, a miscomprehension on the government's part about how similar the Rev. 2 and the Rev. 3 publications are."

The new governmentwide "Standard Form XXX" required by the proposal is a potentially positive change, creating a uniform way for agencies to inform contractors and bidders about CUI, which could help make contracting officers more mindful about identifying CUI, but those forms will only be as good as the information they contain, Bourne said.

"Right now, there's a CUI registry that has a list of categories," she said. "It's not super helpful if it's just, 'Here are the 10 categories that you might have under this contract.' That doesn't really get us anywhere."

There is also the potential that the standard form ultimately won't be standard at all in practice, Gruden said.

"I think even when reviewing the standard form, there are many opportunities for government agencies to tailor and to provide very unique and specific requirements — when it comes to safeguarding, when it comes to training, when it comes to physical access and facilities," he said.

--Editing by Jay Jackson Jr. and Drashti Mehta.
