LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Gov't Contracting Policies To Watch In 2023: A Midyear Report

By **Daniel Wilson**

Law360 (July 19, 2023, 10:16 PM EDT) -- Government contractors have a variety of pending policy changes to watch for in the back half of 2023, including final versions of a sweeping greenhouse gas emissions disclosure mandate and a long-delayed Pentagon cybersecurity rule.

Here, Law360 previews five important upcoming policy changes that will likely significantly affect federal contractors.

Contractors Required To Reveal Greenhouse Gas Emissions

The Federal Acquisition Regulatory Council is scheduled to finalize a contentious, sweeping rule by the end of the year requiring contractors to disclose — many for the first time — their greenhouse gas emissions.

Part of a broader effort by the Biden administration to curb carbon emissions, the Federal Supplier Climate Risks and Resilience Rule, proposed in November, would require "major" federal contractors to publicly disclose their greenhouse gas emissions and climate-related financial risks, and set emissions reduction targets.

"The government is aggressively moving ahead and embedding these types of sustainability measures [into the contracting process], whether it's disclosure requirements, or [in deciding] the types of products that they're going to buy, which will fall squarely on contractors," said Crowell & Moring LLP associate Issac Schabes.

Major contractors, defined as those that receive more than $50 million in contracts each year, would also have to disclose certain indirect emissions, such as from the electricity they use and from the extraction and production of purchased materials.

Most provisions of the rule would also apply to "significant" contractors with annual contract awards between $7.5 million and $50 million, and companies that don't comply will be considered "nonresponsible," effectively unable to be chosen for federal contracts.

Common themes in comments on the proposed rule have included concerns about outsized burdens for larger contractors from having to collect indirect emissions data, and about smaller businesses being included in the "significant" contractor definition.

"I think the whole idea of tracking indirect emissions is problematic," said K&L Gates LLP partner Sheila Armstrong. "It puts a whole layer of compliance where you really need to rely on your subcontractors to provide information, and I don't think the government appreciates the cost and practicality of doing that."

Business groups have implicitly threatened lawsuits if the rule is not significantly revised or withdrawn. According to the administration's most recent regulatory agenda, a final rule is due in December.

DOD to Release Reworked Cybersecurity Requirements

A rule implementing "Version 2.0" of the U.S. Department of Defense's Cybersecurity Maturity Model Certification — a wide-ranging cybersecurity framework intended to apply to all defense contractors — is expected to finally appear later this year, after several delays.

Citing a steady rise in cyberattacks against the defense industrial base, the DOD said it was necessary to implement an overarching cybersecurity framework for all defense contractors, subcontractors and suppliers, beyond its existing cybersecurity rules. It released the first version of the CMMC in 2019.

But after a chorus of complaints, the DOD reworked the CMMC, releasing a draft proposal for Version 2.0, a simplified framework more in line with the National Institute of Standards and Technology's existing standards, in November 2021.

Under Version 2.0, "Level 1" contractors would have to follow basic cybersecurity requirements, while "Level 2" contractors with more advanced cybersecurity needs would have to comply with NIST's Special Publication 800-171, a standard for protecting controlled unclassified information — sensitive but unclassified federal information.

"Level 3" contractors, who handle particularly sensitive information or important contracts, would need to comply with more stringent requirements, including parts of NIST's more advanced SP 800-172 cybersecurity standard.

The rule has been beset by delays, and there are still a number of questions despite related information trickling out over time, such as the specific controls from SP 800-172 that will apply to Level 3 contractors, and how the department will accommodate small businesses' needs.

It is also uncertain how the final framework will integrate changes recently proposed by NIST in a draft third revision of SP 800-171 which is complicating contractors' efforts to try to get an earlier start on CMMC compliance, said Michael Gruden, counsel at Crowell & Moring LLP.

"There's obviously that delta between Rev. 2 and Rev. 3," he said. "And so part of the [uncertainty] is, can people right now, with confidence, engage with a [third-party assessor] and know that their CMMC certification will stand, or will there be some type of modified or updated certification needed once Rev. 3 is incorporated into CMMC?"

The administration has indicated that a notice of proposed rulemaking for CMMC 2.0 will be released by September.

Prevailing Wage Changes for Construction Contractors

Proposed in March 2022 and originally scheduled to be finalized in February, a final rule implementing sweeping revisions to prevailing wage requirements for federally funded construction projects under the Davis-Bacon Act is also expected before the end of 2023.

Prevailing wages for construction contracts are currently set based on either the wage paid to 51% or more of a particular type of worker, or a "weighted average" rate if there is no such majority wage. Under the proposal, described by the U.S. Department of Labor as the "most comprehensive" adjustment to prevailing wage requirements in decades, that standard would be replaced by a "30% rule."

Prevailing wages would be set by the wages paid to at least 30% of workers of a particular classification, if the majority of workers aren't paid the same wage. In effect, the rule would revert the prevailing wage standard to a method used for decades, before being changed by the Reagan administration in 1983.

The proposed version of the rule drew thousands of comments. Critics argued that the proposed changes would give unions an outsized role in setting prevailing wages and wouldn't accurately reflect local conditions; supporters said it would enable prevailing wage determinations to better reflect actual market wages and help prevent companies with unfair wage practices getting access to lucrative federal contracts.

A final rule was originally due in February before being pushed back, with the most recent estimate set for June. That means a final rule could come any day, although there is speculation that the Labor Department is waiting for a new boss after Labor Secretary Marty Walsh stepped down in March, said Holland & Knight LLP partner Eric Crusius.

"Or, it could just be that it's complicated, and it's taking a while," Crusius said. "[The administration] views it as economically significant, which is not a lie."

Software Contractors To Make Security Attestations

Amid ongoing cybersecurity and supply chain security concerns, the White House has pushed contractors to attest to the security of the software they sell to the government, and those attestations could be required to start at some point during the second half of the year.

Mandated by a September memorandum intended to help protect agencies from cyberattacks, contractors will have to attest that any new or updated software they sell to agencies is in compliance with NIST guidelines related to secure software development and securing software supply chains.

"I think this reflects the government's evolving realization that they want more understanding about the commercial products they're using, in addition to the bespoke products ... about what they're buying and what is in what they're buying," said Covington & Burling LLP partner Susan Cassidy.

For "critical software," an agency will also be able to ask for a software bill of materials, a sort of "ingredient list" of software components and dependencies, according to the National Telecommunications and Information Administration.

Agencies were originally due to start collecting attestations for "critical" software by June, and by September for other software, but the administration postponed those deadlines in June amid delays in the Cybersecurity and Infrastructure Security Agency issuing a draft of the required attestation form.

The new deadline for collecting critical software attestations, according to the Office of Management and Budget, will be three months after the form is finalized for critical software, and six months for other software.

Despite related memoranda from the OMB, there are still important questions regarding how the attestation requirements will be applied, and who they will apply to, Bob Huffman, senior of counsel at Covington & Burling, told Law360.

"What is a software producer? I don't believe that term is defined in either of the OMB memos," Huffman said. "And then, of course, [is] the question of what is 'software'? Both memos use a very broad, but somewhat ambiguous description of software. And then what is a software 'end product' in the context of the definition of software?"

Also left unclear is how software attestations will be collected by agencies and what they will do with the information they collect. Clarity on those important issues might have to wait for a related FAR Council rule, also due later this year, Cassidy said.

FAR Council To Set Governmentwide CUI Requirements

Another FAR Council rule, intended to create a set of standardized requirements for controlled unclassified information across the government and likely to underpin new or revised cybersecurity requirements at civilian agencies, is also imminent.

For the government, the rule should be a significant boost to its ongoing efforts to bolster cybersecurity at federal agencies. And for defense contractors already used to dealing with the DOD's stringent cybersecurity requirements, the FAR Council's rule is unlikely to create many, if any, new compliance burdens.

But non-defense contractors are likely to see a mix of benefits and drawbacks in a governmentwide CUI rule, according to Crowell & Moring's Gruden. For example, there is likely to be less flexibility in CUI requirements compared to what many civilian agencies currently allow, but contractors will also have a single, consistent — and hopefully clear — standard that will apply across multiple agencies, he said.

"Companies can actually know what the target is, and then plan to hit that target," he said. "Right now, you have this wildcard paradigm where, with every solicitation of various agencies, you don't really know what you're going to get [and] what's going to be required of you."

The proposed rule is expected by the end of the month.

--Editing by Kelly Duncan and Jay Jackson Jr.

All Content © 2003-2023, Portfolio Media, Inc.