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

Revised NIST Guidelines May Put Contractors In Straitjacket

By **Daniel Wilson**

Law360 (May 12, 2023, 10:30 PM EDT) -- The National Institute of Standards and Technology's proposed clarification of its guidelines on how contractors should handle sensitive unclassified federal information also makes that guidance more prescriptive, potentially making it harder for contractors to comply.

NIST on Wednesday issued a draft proposed third revision of its Special Publication 800-171, first introduced in 2015, which provides guidance to federal contractors on how they should protect the confidentiality of federal controlled unclassified information, or CUI, that they store or process. SP 800-171 underpins both current and pending U.S. Department of Defense cybersecurity rules, and is also likely to be the basis for other agencies' future cybersecurity rules.

The draft proposal would significantly change the guidelines included in SP 800-171, staying with 110 security controls in total, but removing or consolidating some older requirements while adding certain new requirements and providing additional explanations and details for many existing controls. Although more clarity regarding compliance with federal rules and requirements is typically welcomed by contractors, those additional details may paradoxically make it harder for contractors to comply.

"I like the fact that Revision 3 does a much better job explaining the details of many individual requirements," said Bob Metzger, co-chair of Rogers Joseph O'Donnell PC's cybersecurity and privacy practice group. "However, it is all too possible that the greater detail will make satisfaction with 800-171 much more difficult for many, and extremely difficult for smaller and medium-sized enterprises who already are struggling to meet Revision 2."

In the current version of SP 800-171, Revision 2, each of the 110 requirements — such as ensuring access to systems holding CUI is limited to authorized users — is typically explained in a broad single sentence, giving companies flexibility in how they meet those requirements.

The proposed third revision, while more informative and easier to understand, particularly for the broader contracting community beyond cybersecurity specialists, effectively also drives contractors toward a more rigid compliance approach that doesn't necessarily take into account their differing circumstances, Metzger said.

More specificity also cuts against the initial stated purpose of SP 800-171, introduced as a contractor-specific, more flexible offshoot of NIST's SP 800-53, a set of security and privacy controls for information systems, said Evan Wolff, co-chair of Crowell & Moring LLP's privacy and cybersecurity group.

"I do have concerns around some of the specificity. ... While they've layered in and added in more controls, [and] some of them are areas that I think industry, and specifically companies, need to grow into, I've got concerns over taking risk-based components out of this," he said. "And given the tens of thousands, or hundreds of thousands, of companies that have to comply with this, they're adding on a lot more complexity that may be difficult [to comply with]."

Even proposed changes aimed at providing more flexibility, such as allowing federal organizations to tweak certain requirements to meet their own needs through the use of "organization-defined parameters," also come with their own potential downside for contractors.

Companies that do work for multiple agencies, for example, could be torn in different directions by competing implementations of the same requirement, said Michael Gruden, counsel at Crowell & Moring and a former DOD information technology acquisition branch chief.

"I think what we're going to see as a result is that contractors will need to determine the highest common denominator from a security perspective, and then architect their network to meet those standards," he said. "And I think that that is a marked change from Revision 2, where there was a lot of flexibility [for contractors], where the government wasn't telling you, essentially, what was expected to meet a certain control. Now, you can have four or five different agencies telling you differently how they want it to be met."

NIST said it expects to issue at least one more draft ahead of a final version of Revision 3 due in early 2024, which will be followed by changes to related guidance such as SP 800-171A — covering the assessment of CUI security requirements — and it will likely take some time before the new requirements are incorporated into related regulations and contracts.

In the meantime, in addition to providing formal feedback on the draft to help shape its final form, contractors should examine where they already comply with the dozens of proposed changes that NIST has highlighted as "significant" and where they need to start closing compliance gaps, according to Alex Major, co-chair of McCarter & English LLP's government contracts and global trade practice.

While there will inevitably be at least some tweaks between the draft and final versions, the broad substance of the draft version "will probably be how it's going to look when it becomes final," Major said.

"Contractors need to realize that there are new obligations in these controls that they're not used to," he said. "And contractors should expect to see updates to their contracts, and/or modifications that may include [SP 800-171] updates."

For many contractors, particularly smaller businesses, another prudent action would be to call on expert outside providers to help them manage aspects of their compliance with SP 800-171 and other federal cybersecurity requirements, particularly with the DOD's looming Cybersecurity Maturity Model Certification program, a sweeping cybersecurity program underpinned by SP 800-171 that is already set to mandate third-party assessments for many defense contractors, Wolff of Crowell & Moring said.

"I think this will continue to push them through that threshold of not being able to manage networks themselves, because of the added security, [effectively] forcing their hand at turning to others, which isn't necessarily a bad thing. It does add cost, but there are some real benefits," he said.