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

Flexibility In Info Security Policy May Add Compliance Burden

By **Daniel Wilson**

Law360 (May 15, 2024, 9:04 PM EDT) -- New federal guidance for contractors handling sensitive, but unclassified information could introduce confusion and compliance burdens if agencies implement security controls without consulting contractors.

In guidance that is expected to underpin cybersecurity rules, the U.S. Department of Commerce's National Institute of Standards and Technology, a science lab aimed at promoting economic innovation and developing standards to be used across the federal government, introduced "organization-defined parameters" that give agencies the flexibility to dictate requirements such as whether contractors must install cryptographic protections or allow remote access to systems containing so-called controlled unclassified information.

For contractors, ODPs may be both a "gift and curse," potentially allowing companies to convince agencies to let them establish their own security requirements, but also potentially introducing ambiguity and confusion as different agencies introduce their own specific, and possibly disparate, requirements, according to Alex Major, co-chair of the government contracts group at McCarter & English LLP.

"If the government or the agency decides to … take the [latter] path, then that can become very grueling for contractors," said Major, whose practice often involves cybersecurity and data privacy risk issues.

Because only agencies can implement ODPs, contractors looking to take advantage of the flexibility they offer or at least limit potential difficulties stemming from agencies imposing their own requirements will need to collaborate closely with agencies and lean on the adage that "cybersecurity is a team sport," said Crowell & Moring LLP counsel Michael Gruden.

"I can see scenarios where some of those defined terms may be too stringent, and there may be a misunderstanding of what's required," said Gruden, a cybersecurity specialist and former U.S. Department of Defense contracting officer. "And there may be a need for industry to look very carefully at those ODPs, and then to request clarifications, or to gently push back and to open up dialogue."

ODPs drew concerns from contractors, industry groups and cybersecurity assessors when NIST introduced its first draft of the guidance in May 2023 about potentially inconsistent expectations, and inconsistent implementation of similar provisions, creating confusion and leading to increased compliance costs. The agency responded to that feedback by significantly dropping the number of ODPs from more than 100 to 34 in a revised draft, before ultimately settling on 49 ODPs.

That final number shows the agency likely tried to walk a "fine line" between the interests of contractors and of agencies, and avoid being prescriptive to the point of potentially hindering compliance with security controls, said Elle Ross, a Greenberg Traurig LLP associate who frequently counsels clients on cybersecurity issues.

"I wouldn't be surprised if, in going back to their agency stakeholders, in addition to industry, NIST heard that there might have been almost too much pull back [on the number of ODPs], and that for some of these ODPs it made sense to re-insert them to give that flexibility," she said.

The effects of NIST's guidance won't be directly felt by contractors until agencies finalize pending cybersecurity rules, or revise existing rules. The DOD earlier this month indefinitely kept existing compliance requirements in place in anticipation of the new guidance, saying it wanted "to provide industry time for a more deliberate transition" and give itself "time to best align any of the necessary supporting mechanisms."

But contractors should still try to adjust their processes for securing controlled unclassified information to account for NIST's latest guidance as soon as possible, as the DOD's freeze can be rescinded at any time, and civilian agency cybersecurity rules might not be far away either, attorneys said.

"It's a different document in a lot of important ways … it would make a lot of sense for companies to at least start to think about it, start to do that analysis of, 'OK, what is different about this publication?,' identifying gaps, and in particular identifying any new requirements," Ross said.

--Editing by Emily Kokoll.
