wiley

ALERT

Not So Fast, NIST: DOD Issues Class Deviation to Retake Control Over What Cybersecurity Requirements Apply to its Contracts

May 6, 2024

WHAT: On May 2, 2024, the U.S. Department of Defense (DOD) issued a Defense Federal Acquisition Regulation Supplement (DFARS) class deviation related to the cybersecurity standards required for covered contractor information systems. Class Deviation 2024-O0013 clarifies that DOD will continue to require contractors to comply with National Institute of Standards and Technology (NIST) SP 800-171 ***Revision 2***, even though NIST intends to release Revision 3 later this month.

WHEN: Effective immediately, contracting officers must use Class Deviation 2024-O0013 instead of the evolving DFARS 252.204-7012 clause.

WHAT DOES IT MEAN FOR INDUSTRY: Before this Class Deviation, DOD's standard contract clause, DFARS 252.204-7012, stated that contractors must implement the version of NIST SP 800-171 "in effect at the time the solicitation is issued." That meant once NIST issued a new version of SP 800-171—as it plans to do later this month—that new version would apply automatically to all new DOD contracts. For some time, we have doubted whether this sort of dynamic incorporation is lawful, and DOD had signaled with its proposed Cybersecurity Maturity Model Certification (CMMC) 2.0 rulemaking that it intended to stick with Revision 2. But this Class Deviation was still needed to bring an end to the uncertainty and avoid potential disputes over which set of requirements will apply to contractors.

Class Deviation 2024-O0013

Authors

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Cybersecurity
Government Contracts
Privacy, Cyber & Data Governance

The Class Deviation prescribes an alternate clause that will require contractors that are subject to DFARS 252.204-7012 to comply with NIST SP 800-171 Revision 2. DOD explains in its announcement that the Class Deviation is intended to provide industry time for a more deliberate transition and will also provide DOD time to "best align any of the necessary supporting mechanisms."

What does DOD's action mean for contractors?

More Certainty. This action gives contractors certainty that SP 800-171 Revision 2's security requirements will continue to apply until DOD says differently. DOD did not include an expiration date for use of the Class Deviation's alternate clause. By specifying that Revision 2 will apply, DOD also avoids potential legal challenges to the DFARS -7012 clause's questionable use of dynamic incorporation.

More Consistency. DOD's action is consistent with its proposed rules for the CMMC program (covered here), which, unlike the current DFARS -7012 clause, would tie the CMMC program specifically to Revision 2.

More to Come? DOD said in its announcement that this action is intended, in part, to provide DOD time to align supporting mechanisms. We read this as a reference to the forthcoming CMMC program, and thus that DOD may not transition to 800-171's Revision 3 until it has addressed other processes: for example, until it has prepared its assessors to begin assessing contractors against any updated requirements in SP 800-171 Revision 3.

Although DOD stated that it based this decision on timing concerns, we also know DOD did not fully agree with all the changes that NIST proposed in the drafts of Revision 3. Among other things, DOD suggested that NIST remove "organization-defined parameters" (ODPs), which NIST viewed as a significant part of forthcoming Revision 3. As reflected in the excerpt below from comments to NIST submitted by DOD's Office of the Chief Information Officer (CIO), DOD criticized these ODPs as inappropriate and unworkable:

> The statement "Organization-defined parameters (ODPs) are included for some requirements. These ODPs provide flexibility through the use of assignment and selection operations to allow federal agencies and nonfederal organizations to specify values for the designated parameters in the requirements" is problematic. It is noted that the FPD now allows the option for nonfederal organizations to specify the values, but this is still a problem, as it creates confusion as to who is responsible for establishing the requirement. Clearly, the 'organization' should be the non-federal organization (the owner/operator of an information system NOT operated on behalf of the government, but for internal business purposes) and it would be inappropriate for a USG agency to specify what parameters are assigned. Aside from having no knowledge of the nonfederal organization's system, it is especially problematic in that different Agencies (or different elements within an Agency) would almost certainly specify different parameters for the same requirement, creating unnecessary churn and a chaotic security environment if the nonfederal org has to continually accommodate differing or conflicting requirements simultaneously. It also creates unacceptable contract administration issues for the USG, expected to issue some 100K contracts a year requiring compliance with NIST SP 800-171, as it is simply not possible for the USG Requiring

> Activities/Contracting Officers to complete the many ODPs in rev3 for each contract. Note also that only a few of the many ODPs are simple enough (e.g., frequency of review or update) for the Agency to specify a value – the rest require knowledge of the system operation to complete, which the Agency does not have, and so should be left to the nonfederal organization. Nevertheless, inevitably Agencies will attempt to specify such parameters.

(See the DOD CIO's recent comments on the revision here). It's possible that DOD could seek to resolve these substantive issues before requiring contractors to comply with Revision 3. Throughout the process for developing Revision 3, however, NIST has been reluctant to remove ODPs, and that could mean DOD has to issue its own regulations defining those ODPs before it can require contractors to comply with Revision 3.

Key Takeaways

Contractors should be vigilant and ensure contracting officers use the Class Deviation clause in any new solicitations and contracts. If contracting officers include the standard clause instead of the new alternate, contractors should remind them of this Class Deviation and request that the contracting officer incorporate it.

Wiley is deeply engaged in the emerging CMMC and NIST SP 800-171 requirements and has advised government contractors across a wide range of cybersecurity compliance and incident response challenges.