Published on *The National Law Review* https://natlawreview.com

Department of Defense Provides Government Contractors Grace Period for Compliance with Key Cybersecurity Requirements

Article By:

Alexander W. Major

In response to industry concerns and comments, on December 30, 2015, the ***Department of Defense*** issued a new interim rule amending the ***Defense Federal Acquisition Regulation Supplement (DFARS)*** cybersecurity rules promulgated in August. Specifically focusing on provision 252.204–7008, *Compliance with Safeguarding Covered Defense Information Controls*, and DFARS 252.204–7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, under this second interim rule contractors have until December 31, 2017 to implement the security control requirements specified by National Institute of Standards and Technology Special Publication 800-171 (SP 800-171). As the prior interim rule had no grace period for implementing the new cybersecurity controls, this a fortunate change for DoD contractors. This welcome extension, however, is not without conditions. Contractors, in line with the notification outlined in DoD's class deviation addressing "multifactor authentication for local and network access," now have 30 days to inform the DoD Chief Information Officer (CIO) if any of the SP 800–171 security requirements are not implemented at the time of contract award. Absent that notice, DoD will presume contractors are meeting all of the NIST-established controls. As the new interim rule describes, this 30-day period will allow DoD the opportunity to monitor progress across its government contractors to identify and address any problems with the implementation of the NIST security controls.

The other changes in the interim rule limit the manner in which certain regulations are to be flowed down to subcontractors and limit the scope of DoD review:

- DFARS 252.204–7009 was amended to require inclusion of the clause into subcontracts "for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting." Further, the clause must be included "without alteration," except as needed to identify the contracting parties subject to the clause. These changes now limit the clause to specific types of subcontracts and direct that the exact phrasing of the clause must be flowed down versus "the substance of the clause," as was required previously.

- DFARS 252.204-7012 is similarly limited now only to subcontractors whose efforts will involve covered defense information or operationally critical support and also must be included in applicable contracts without modification.

- The allowance for “alternative but equally effective security measures” in lieu of the NIST security controls allowed under 252.204-7012 no longer needs the DoD CIO’s approval but, now, can be approved by an “authorized representative” of the DoD CIO.

While DoD contractors should appreciate the much needed breathing room the amended interim rule permits, they should avoid procrastination and use this time to align their practices – to the best of their ability – with NIST SP 800-171. What’s more, and in line with many of the NIST’s standards, defense contractors also need to ensure they stay flexible. As the interim rule reflects, this is by no means a “one and done” rule – contractors should expect, and be ready to adopt and adapt to, changes and additional DoD guidance as the NIST security controls find their way into common practice. Change is a constant in the world of cybersecurity.

Copyright © 2025, Sheppard Mullin Richter & Hampton LLP.

National Law Review, Volume VI, Number 4

Source URL:https://natlawreview.com/article/department-defense-provides-government-contractors-grace-period-compliance-key