

ALERT

DOD Revises Interim Rule for Safeguarding Covered Defense Information: Adopts Two-Year Phase-In Period to Meet NIST Standards

December 30, 2015

In a major development quietly sandwiched between the winter holidays, the U.S. Department of Defense (DOD) this morning issued a three-page interim rule revising the August 2015 interim rule on Safeguarding Covered Defense Information. See 80 Fed. Reg. 81472 (Dec. 30, 2015). We previously covered the initial interim rule in August. The revision adopts a two-year phase-in period for contractors to implement the adequate security requirements outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, requiring contractors to implement those standards ***“as soon as practical, but not later than December 31, 2017.”*** Contractors will no longer be required to obtain written approval from the DOD Chief Information Officer (CIO) prior to contract award authorizing “alternate but equal” capabilities, but will instead be required to notify the DOD CIO, via email, within 30 days after contract award “of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award,” with an undertaking to implement the necessary standards later. Likewise, if contractors are unable to implement the required standards outlined in NIST SP 800-171, they may implement “[a]lternate but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DOD CIO.”

The revision affords contractors significant and much-needed flexibility to implement the NIST SP 800-171 standards in a timely fashion, with DOD appropriately acknowledging that it was not reasonable to expect industry to immediately comply with the new

Authors

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Practice Areas

Government Contracts

NIST 800-171 standards imposed earlier this year. The revision comes on the heels of a wave of industry criticism regarding the draconian implementation requirements under the initial interim rule. DOD stated that the interim rule was being issued without the opportunity for public comment “to provide immediate relief from the requirement to have NIST 800-171 security requirements implemented at the time of contract award,” as contractors would otherwise be “at risk of not being able to comply with the terms of contracts that require the handling of covered defense information” upon contract award under the initial interim rule. DOD believes that the revision will “limit[] the burden imposed on industry in the first interim rule” by “grant[ing] additional time for contractors to assess their information systems and to set forth an economically efficient strategy to implement the new security requirements at a pace that fits within normal information technology lifecycle timeliness.”