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

Time Is On My Side: DoD Hears Industry Concerns – Additional Time Provided to Implement Security Controls Under New Cyber Rule

Article By:

Susan B. Cassidy

John W. Sorrenti

On December 30th, the Department of Defense (DoD) issued a Second Interim Rule amending its "Network Penetration Reporting and Contracting for Cloud Services" Interim Rule and giving contractors until December 31, 2017 to implement the NIST SP 800-171 security controls required by DFARS 252.204-7012. As noted in a previous post, DoD has already issued a class deviation giving covered contractors up to nine (9) months (from the date of contract award or modification incorporating the new clause(s)) to satisfy the requirement for "multifactor authentication for local and network access" found in Section 3.5.3 of NIST SP 800-171. This current revision appears responsive to significant concerns raised by Industry about compliance with the remaining safeguarding requirements imposed overnight on contractors on August 26, 2015.

The Second Interim Rule imposes the following changes:

- contractors have until December 31, 2017 to implement NIST SP 800-171 security requirements on covered contractor information systems;
- contractors must, within 30 days of contract award, notify the DoD Chief Information Officer (CIO) of any NIST SP 800-171 security requirements that are not implemented at the time of contract award;
- DFARS 252.204-7012 is amended to delete the requirement for DoD CIO acceptance of alternative, but equally effective, security measures prior to award;
- the subcontractor flow down requirements are amended to limit the requirement to flow down the clause only to (i) subcontracts for operationally critical support, or (ii) where subcontract performance will involve a covered contractor information system (previously the Interim Rule required the clause to be flowed to "all subcontracts"); and
- other than identifying the parties, changes in the substance of DFARS 252.204-7012 are now

expressly prohibited when flowing down the clause to subcontractors.

In the Federal Register notice, DoD states that it is granting 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 timelines." Although this delay in implementation is a welcome respite, it is important that contractors analyze their existing security controls to determine which gaps exist so that appropriate notice can be provided to DoD at the time of contract award. Absent a notice to the DoD CIO of those 800-171 security controls that the contractor has not yet implemented, DoD will reasonably presume that the contractor is in compliance with all of the 800-171 requirements.

Failure to identify those gaps, however, could put contractors at risk of a contract breach or potentially a false implied certification if DoD later determines that the contractor's security controls were not in compliance. Given the requirements to report cyber incidents and the level of disclosure required, contractors do not want to be in a position where a breach results from the absence of a security control that had not been disclosed to DoD.

National Law Review, Volume V, Number 364