DPAP issues guidance regarding NIST SP 800-171 security controls implementation

September 28, 2017

The Defense Pricing/Defense Procurement and Acquisition Policy Directorate (DPAP) at the Department of Defense (DoD) issued guidance last week regarding the fast-approaching December 31, 2017, implementation deadline for the security controls in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. For contractors and subcontractors still wrestling with the DFARS clause, this guidance, combined with information the DoD provided during a June 2017 Industry Day, should provide helpful information to find practical means of addressing the requirements in advance of the looming deadline.

Under DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, contractors with information systems that contain or transmit covered defense information are required to provide "adequate security" on contractor information systems for covered defense information. Under the clause, adequate security consists of the 110 security controls in NIST SP 800-171, which must be implemented no later than December 31, 2017.

Most importantly, DPAP's guidance emphasizes system security plans (SSPs) and plans of action (POAs) as tools for contractors to demonstrate implementation or planned implementation of the security controls. Based on Section 3.12.4 in NIST SP 800-171 Rev. 1 (December 2016), contractors develop and document plans that describe their IT systems' boundaries and implementation of security controls. Section 3.12.2 requires that contractors develop and implement POAs to correct deficiencies or eliminate vulnerabilities in their systems. Contractors should have SSPs in place by December 31, 2017, and any associated POAs to describe contractors' next steps to satisfy unimplemented security requirements, correct outstanding deficiencies, and reduce vulnerabilities in their systems.

These plans may become particularly relevant for contractors representing compliance in their offers under DFARS 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls. They may also be required components of contractors' technical proposals and/or may be incorporated by reference into contracts' Section H special contract requirements. Significantly, the DPAP guidance notes that contractors' SSPs and POAs may factor into requiring activities' evaluation of the overall risk posed by contractors' IT systems. The DPAP is collaborating with the DoD's chief information officer (CIO) to develop guidance describing cybersecurity safeguarding requirements for procurements and the level of risk requiring activities are willing to accept.

Importantly, the DPAP guidance recommends that, if a contractor or subcontractor was awarded a contract prior to the issuance of NIST SP 800-171, Rev. 1, then the contract should be modified to authorize the use of NIST SP 800-171, Rev. 1, clarifying the contractor's or subcontractor's ability to utilize SSPs and POAs. While DoD acquisition personnel are being instructed to facilitate such contract modifications, this action is likely to be more complicated for subcontractors, particularly if the prime does not believe its contract should be updated. Moreover, contractors and subcontractors should first assess whether they have provided timely notification to the DoD's CIO regarding any requirements of NIST SP 800-171 that were not implemented following contract awards as required by the clause.

The DPAP guidance also describes how contractors are likely to approach implementing NIST SP 800-171. The

security controls focus on policies, processes and configuration of information technology. Some controls require security-related software, such as anti-virus protection, or additional hardware, such as a firewall. The complexity of contractors' IT systems largely determines whether additional software or tools are required. The DPAP guidance recommends that contractors measure their current policies and processes against the standards set forth in NIST SP 800-171. Based on that review, certain security controls can be accomplished by in-house IT personnel while others may require external assistance. For clarification regarding a security control's requirements, the DPAP guidance recommends using NIST SP 800-171's Appendix D to determine the corresponding security control in NIST SP 800-53. NIST SP 800-53 includes a "Supplemental Guidance" section with clarifying guidance and examples of how to implement security controls, though not all aspects of NIST SP 800-53's security controls are included in NIST SP 800-171 and, correspondingly, not all of the guidance may be applicable.

As contractor personnel work with members of their information technology team to bring IT systems into compliance with NIST SP 800-171 by the end of this year, the DPAP guidance should provide helpful information regarding the initial assessment of current IT systems and the importance of SSPs and POAs. Even contractors who suspect they may not be able to fully implement NIST SP 800-171's security controls by December 31, 2017 should use their SSPs and POAs, together with the DPAP guidance, to demonstrate to DoD acquisition personnel how and when full implementation will be accomplished.

Your Key Contacts

Phillip R. Seckman
Partner, Denver
D +1 303 634 4338
phil.seckman@dentons.com