THE
NATIONAL LAW REVIEW

Cyber Update: DoD Contractor Cybersecurity Certification and 33 New Enhanced Controls to Combat the Advanced Persistent Threat

Wednesday, June 26, 2019

The Government remains intensely focused on how best to protect its Controlled Unclassified Information (CUI) once it is released to contractors. In a shift from its initial approach of "we will take the contractor's word for it," the Department of Defense (DoD) announced in June 2019 it is in the process of developing a new cybersecurity certification program for its contractors, which will involve using third party auditors to validate contractor compliance with required security controls. In addition, on June 19, 2019, the National Institute of Standards and Technology (NIST) released two new highly-anticipated draft special publications – NIST SP 800-171, Rev 2 and NIST SP 800-171B – with a tight turnaround time for comments by **July 19, 2019**.

SheppardMullin

Article By
Townsend L. Bourne
Sheppard, Mullin, Richter & Hampton LLP
Government Contracts, Investigations & International Trade Law Blog
Government Contracts, Maritime & Military Law
Communications, Media & Internet
All Federal

DoD Cybersecurity Maturity Model Certification

In 2017, DoD informed industry that its cybersecurity rule (DFARS 252.204-7012) "does not require 'certification' of any kind . . . Nor will DoD give any credence to 3rd party assessments or certifications . . ." (*see* our prior blog article, *Achieving Cyber-Fitness in 2017: Part 3—Proving Compliance and the Role of Third-Party Auditors*, for a more detailed discussion of the roles of third-party auditors in proving compliance). However, two years later DoD has decided it needs more assurances regarding contractor cybersecurity controls and supply chain protections.

DoD recently announced its new approach, the Cybersecurity Maturity Model Certification (CMMC), which it hopes to finalize by January 2020 and share for industry feedback by next summer.[1] The new system will involve "levels" of cybersecurity capability (tentatively, Level 1 through Level 5) to which contractors may be certified, allowing DoD to streamline the acquisition process by setting forth the specific level of cybersecurity it desires in each solicitation. It is anticipated the levels will incorporate existing security controls from NIST SP 800-171, as well as additional requirements developed with industry and research institutions. Third party auditors also will be engaged to verify security capabilities.

This model sounds a lot like FedRAMP, the current certification program for government cloud computing providers, which has proven very successful in encouraging collaboration between government and contractors in the name of security. DoD hopes to do the same here – industry meetings are being set up throughout the country in July and August to give the private sector an opportunity to weigh in on the new model and how best to mitigate/eliminate supply chain risk. The new program also aims to assist lower-tier subcontractors and small businesses, which should be able to secure a lower cost Level 1 certification, and includes creation of cybersecurity education and training materials.

NIST Draft Publications

Currently, per DoD's cybersecurity clause (DFARS 252.204-7012), DoD contractors must demonstrate, at a minimum, implementation of the 110 security controls in NIST SP 800-171. NIST released Revision 1 of the publication in December 2016. A draft Revision 2, as well as a draft NIST SP 800-171B, a new companion publication that includes enhanced controls for critical programs and assets, were released on June 19, 2019.

Comments on both draft publications are due by July 19, 2019.

The draft Revision 2 does not contain notable changes when compared to its predecessor. It consists of minor editorial updates and a relocation of the "Discussion" sections relating to the security controls from Appendix F to Chapter 3. No changes have been made to the 110 security requirements. In the draft Revision, NIST promises a "comprehensive update to this publication (including updates to the basic and derived requirements)…in Revision 3 following the issuance of NIST Special Publication 800-53, Revision 5, which will include modified control families, privacy integration, and make other conforming edits."

Draft NIST SP 800-171B includes an additional 33 enhanced security controls to be used when necessary to protect CUI from an Advanced Persistent Threat (APT) in a critical program or high value asset. An APT is an "adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors" and "pursues its objectives repeatedly over an extended period; adapts to defenders' efforts to resist it; and is determined to maintain the level of interaction needed to execute its objectives." When required by an agency, these enhanced security controls are to be implemented in addition to the 110 controls in NIST SP 800-171.

The enhanced requirements center around three components: (1) penetration resistant architecture, (2) damage limiting operations, and (3) designing for cyber resiliency and survivability. The enhanced controls are organized within the existing security control families in NIST SP 800-171, though some families do not have associated enhanced controls. Examples of the draft enhanced controls include:

- requiring two authorized individuals to execute certain operations;
- providing additional training focused specifically on advanced threats;
- maintaining a cyber threat hunting capability;
- engaging in more rigorous personnel vetting;
- closely monitoring supply chain risk; and
- establishing a cyber incident response team that can be deployed within 24 hours.

These NIST publications are expected to be finalized later this year, as is a new FAR clause addressing CUI protection in contractor systems under civilian agency contracts.

[1] This announcement was made at a Professional Services Council conference on June 13, 2019, by Special Assistant to the Assistant Secretary of Defense Acquisition for Cyber, Katie Arrington.