We don't write much about cyber-security.

There are a couple of reasons for that.

First, everything is moving very quickly and it's tough to hit a moving target. For the past several years, the US Government—especially DoD—has been struggling to adopt a cyber-security framework that provides assurance that contractors (and their supply chains) are reasonably secure from cyber-intrusions. There have been several iterations of that framework and we have been waiting until the framework seemed to reach a close-to-final state.

Second, there are lots and lots of articles that are already being published by law firms, consulting firms, and want-to-be CMMC audit firms. We don't feel we have much to add to that pile of publications, so we have refrained.

Third, it's not like we haven't been ringing this bell for *literally years*. In 2019, we wrote **this article** about "cyber-security and subcontractors." But our interest in this general topic goes back to **2013**, when we wrote about supply chain risk, and noted that a final DFARS rule had just been published "that requires 'defense contractors to incorporate established information security standards on their unclassified networks and to report cyber-intrusion incidents that result in the loss of unclassified controlled technical information from these networks.'" We concluded that 2013 article with a simple sentence: "You have been warned." We were there seven years ago and we warned our readers that things were changing in this area, and that it was time to get very serious about securing the supply chain.

Thus, savvy contractors (or at least the ones that read this blog) have had *seven years* to prepare for this. When did your company start preparing?

Where do things stand today, seven years later?

There is the new CyberSecurity Maturity Model (CMMC), which establishes levels of maturity for contractors (and their suppliers) with respect to cyber-security practices. Oversight is provided by the CMMC Accreditation Body (**CMMC-AB**), The CMMC-AB determines who can be a Registered Practitioner and who can be a Provisional Assessor. In November, 2020, individuals started receiving official “badges” for those positions—and if you are a contractor in need of Certification, you can go to the “marketplace” and find somebody to evaluate you.

There is also something called a CMMC Third Party Assessment Organization (C3PAO) that hasn’t quite jelled yet. But we are quite sure that many consulting firms are ready and eager to get their C3PAO designation so that can help you in this area.

We should mention that the CMMC-AB has itself had an “evolution” over the past year, with Board Members being replaced and new operating philosophies being implemented. But insofar as we can tell, things are settling down there.

Effective 30 November 2020, a new interim **DFARS rule** dealing with assessments of contractor cyble-security maturity—and establishing required maturity levels in RFPs and contracts—came into effect. To help understand how to implement that new rule, John Tenaglia (the new Director of DoD’s Defense Pricing and Contracting group) issued a helpful **guidance memo**
.

Without rehashing the entire memo, here are some bits we found interesting. Rather than relying on our excerpts, we suggest you go read the memo. But knowing our readers, most will not do so. For them:

-

On or after November 30, 2020, the contracting officer shall, prior to awarding a contract, task order, or delivery order to, or exercising an option period or period of performance with, an offeror or contractor that is required to implement NIST SP 800-171 in accordance with the clause at DFARS 252.204-7012, verify that the summary level score of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old, unless a lesser time is specified in the solicitation) is posted in Supplier Performance Risk System (SPRS) for each covered contractor information system that is relevant to an offer, contract, task order, or delivery order.

-

On or after November 30, 2020, when a requiring activity identifies a requirement for a contract, task order, or delivery order to include a specific CMMC level, the contracting officer shall not award to an offeror that does not have a CMMC certificate at the level required by the solicitation, or exercise an option or extend any period of performance on a contract, task order, or delivery order unless the contractor has a CMMC certificate at the level required by the contract Contracting officers shall use Supplier Performance Risk System (SPRS) to verify an offeror or contractor's CMMC level.

-

On or after November 30, 2020, use the new provision at DFARS 252.204-7019 in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of COTS items.

-

On or after November 30, 2020, use the new clause at DFARS 252.204-7020 in all solicitations and contracts, task orders, or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for those that are solely for the acquisition of COTS items. This clause is required to be flowed down to subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items (excluding COTS items)

-

November 30, 2020, through September 30, 2025, use the new clause at DFARS 252.204-7021in solicitations and contracts or task orders or delivery orders, including those using FAR part 12procedures for the acquisition of commercial items, except for solicitations and contracts or orders solely for the acquisition of COTS items, if the requirement document or statement of work, as determined by the requiring activity and approved by OUSD(A&S), requires a contractor to have a specific CMMC level.

-

On or after October 01, 2025, CMMC requirements will apply to all solicitations and contracts or task orders or delivery orders, except for solicitations and contracts or orders solely for the acquisition of commercially available off-the-shelf (COTS) items. On or after October 1, 2025, use the clause at DFARS 252.204-7021 in all solicitations and contracts or task orders or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts or orders solely for the acquisition of COTS items. This clause is required to be flowed down to all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items, excluding COTS items.

-

The CMMC level to be required for subcontractors is the level that is appropriate for the information that is being flowed down to the subcontractor.

To conclude this article, DoD is now making your cyber-security practices—and those of your supply chain—a matter of responsibility for new competitions. If you don’t have what it takes, then don’t bother to submit a proposal. Further, if you do win a new contract award, be prepared to make cyber-security a matter of on-going contract compliance.

We told you this was coming seven years ago. Don’t say you weren’t warned.