Pepper Hamilton LLP
Attorneys at Law

STRATEGIC CYBER PARTNERS

Government Contracts Cyber Café Series
The COTS Carve-Out, Cyber in 2020 and CMMC Update
January 14, 2020

SPEAKERS

- Hilary S. Cairnie, partner and chair, Government Contracts Practice Group, Pepper Hamilton LLP
- Heather Engel, Managing Partner, Strategic Cyber Partners, LLC

Disclaimer: We do not address in these sessions the civilian agency counterpart regulations appearing at FAR Subpart 4.19.

Disclaimer: Our principal purpose in these sessions is to heighten your awareness of the many moving parts associated with DOD's regulatory framework for cyber compliance, but we are not providing legal or technical advice that is specific to your organization.

OVERVIEW OF WEBINAR

Since January 2017, we have discussed many aspects of DOD's cybersecurity requirements imposed on prime contractors and required to be imposed on subcontractors. Reference: DFARS Subpart 204.73, DFARS 252.204-7012 (the Cyber Clause).

Three years have come and gone, during which contractors and DOD contracting and programming groups have been digesting the many requirements of the Cyber Clause, including the 110 cyber controls embodied in NIST 800-171. The learning curve has been steep, and progress at times has been slow.

Contractors have experienced increased costs for developing and implementing cybersecurity compliance frameworks (policies, procedures, personnel, consultants, testing, auditing, reporting, updating, etc.).

In this session, we are going back to basics on the one hand by focusing on an intended carve-out, *i.e.*, exception, for "commercially available off-the-shelf" (COTS) procurements. And, on the other hand, we are looking ahead to the next wave of cyber requirements comprising DOD's Cybersecurity Maturity Model Certification (CMMC) program.

Reference Resources

- FAR 31.205 – Cost Principles
- DFARS 204-7300, DFARS 252.204-7012 – Safeguarding Covered Defense Information and Cyber Incident Reporting
- DFARS 239.7600, DFARS 252.239-7010 – Cloud Computing
- DOD FAQs: https://dodprocurementtoolbox.com/cms/sites/default/files/resources/2018-04/Revision%20to%20Cyber%20DFARS%20FAQs%20-%20April%202%202018.pdf
- DOD OIG Report, Audit of Protection of DOD Controlled Unclassified Information on Contractor-Owned Networks and Systems (July 23, 2019): https://media.defense.gov/2019/Jul/25/2002162331/-1/-1/1/DODIG-2019-105.PDF
- CMMC DRAFT: https://www.acq.osd.mil/cmmc/draft.html
- DFARS 204.73, SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING: https://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm

COTS COVERAGE UNDER DFARS 204.7304(C)

Context: Go back in time to our first Cyber Café in early 2017. One of the first observations shared with attendees was the importance of reviewing the regulations, the solicitations and ultimately the contract, task order, purchase order, etc. to identify the knowns and the unknowns about the extent of Cyber Clause coverage in your contracts. Now we come full circle to discuss a coverage carve-out associated with COTS procurements.

DFARS 204.7304(c) states as follows: “Use the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, in all solicitations and contracts, including solicitations and contracts using FAR Part 12 procedures for the acquisition of commercial items, except for solicitations and contracts solely for the acquisition of COTS items.”

What is the difference between COTS items and commercial items? Refer to FAR 2.101’s definitions for the answer:

- “Commercial item” – the definition is extensive and multifaceted:

- Any item, other than realty, that is of a type customarily used by the general public for other than government purposes, and that
  - Has been sold, leased or licensed to the general public; or
  - Has been offered for sale, lease or license to the general public.
- Any item evolved from the above through advances in technology or performance and that is not yet available in the commercial marketplace, but will be in time to satisfy the delivery requirements under the solicitation.
- Any item that satisfies either of the foregoing but for
  - Modifications of a type customarily available in the commercial marketplace; or
  - Minor modifications of a type not available in the commercial marketplace made to meet government requirements. "Minor modifications" means those that do not significantly alter the nongovernmental function or essential physical characteristics of an item or component, or change the purpose of a process.
- Any combinations of the above items, or the service items described below, that are of a type customarily combined and sold in combination to the general public.
- Installation services, maintenance services, repair services, training services and other services if
  - Such services are procured for support of an item referred to above, regardless of whether the sources are provided by the same source or at the same time as the item; and
  - The source of such services provides similar services contemporaneously to the general public under terms and conditions similar to those offered to the federal government.
- Services of a type offered and sold competitively in substantial quantities in the commercial marketplace based on established catalog or market prices.
- Any item or combination of items or services described above, even if transferred between separate divisions, subsidiaries or affiliates.
- A nondevelopmental item determined by the procuring agency to have been developed exclusively at private expense and sold in

substantial quantities on a competitive basis to state and local government entities.

- "COTS item" means any item of supply (including construction material) that is:
  - A commercial item (as defined above);
  - Sold in substantial quantities in the commercial marketplace;
  - Offered to the government under a contract or subcontract at any tier — without modification — in the same form in which it is sold in the commercial marketplace; and
  - Does not include bulk cargo, such as agricultural or petroleum products.
- Under DFARS 204.7304(c), if you are offering a commercial item that does not qualify as COTS, DOD is required to "use" the clause at 252.204-7012 in all solicitations and contracts.
- If you are offering a commercial item that meets the more restrictive requirements of COTS — and the procurement is solely for purposes of acquiring COTS items — then the procuring agency is not required to include the Cyber Clause.
- For the contractor that is only offering COTS items, you should be proactive at the pre-award stage to make sure the Cyber Clause is not included in the award.
  - Check solicitation and, if the Cyber Clause is included, push back, ask a question, seek to have it excluded.
  - Do not assume that the clause is self-deleting — it is not.
  - Subcontractors at any tier should similarly push back and refuse to accept the Cyber Clause if they are only offering COTS items and nothing else. Reference DFARS 252.7012(m) — subcontract flow-down criteria — no mention of flow down for COTS items in supply chain.
  - Seek legal counsel before submitting your offer.
  - Refer to 252.204-7012(b)(2)(ii)(B) – Variance Request.
- The Christian Doctrine: If the agency neglects to include a required FAR/DFARS clause, it will be deemed to be included in the contract — there is no corollary for inclusion of a FAR/DFARS clause that is expressly not

required in the contract. Nonmandatory clauses are still part of the contract.

- If you accept the Cyber Clause and it is not required for inclusion in the contract, you are subject to the cyber requirements. If you fail to comply with the Cyber Clause, you are at risk of breach of contract and a possible enforcement action for false statements, false certifications and false claims.

CYBERSECURITY IN 2020

Although this is a government contracting series, you cannot ignore the implications of privacy legislation.

In 2020, cybersecurity is now often about data privacy. The California Consumer Privacy Act (CCPA) is now in effect, and the European Union General Data Protection Regulation (GDPR) has been for more than a year.

In early January, legislation was introduced to the Virginia General Assembly – the Virginia Privacy Act (HB473).

All of these and other state regulations will impact how your company collects, manages and maintains consumer data. Even if consumer data is not your primary business, companies have to be aware of these regulations and understand how regulations impact day-to-day operations.

And, in the government contracting world, Supply Chain Risk Management (SCRM) was the reason cited for a lot of policy in 2019, including CMMC. A number of our clients have undergone or will shortly be going through the DCMA audit process. Now is the time to get a handle on your supply chain, flow down contract clauses where required, and understand how your suppliers impact your ability to deliver.

CMMC: CURRENT STATUS

We have included the prior discussion of the COTS clause because as the industry looks ahead to complying with CMMC, understanding your regulatory responsibilities (DFARS) is important to understanding your place in the supply chain, as well as the level of CMMC certification you may be required to obtain.

On December 6, 2019, DOD issued CMMC DRAFT Version 0.7 – 190 pages, inclusive of seven appendices, four figures and four tables.

What is CMMC?

For review, CMMC is the Cybersecurity Maturity Model Certification.

It combines various standards and best practices to create maturity levels ranging from Level 1 – Basic to Level 5 – Advanced.

Starting later in 2020 for selected contracts, defense contractors will now be required to undergo an audit that certifies they have met a minimum level of cybersecurity maturity. You will choose to certify at a level between 1 and 5. Most companies will attempt Level 3. A company that will require Level 4 or 5 will typically be working on specific government technologies, and you will be expected to have a substantial and proactive cybersecurity program (Level 4 definition). A company at Level 1 likely will not use or access any Controlled Unclassified Information.

What is the purpose of CMMC?

CMMC is intended to add a verification component to DOD cybersecurity requirements. Under DFARS 252.204-7012, contractors self-attested that the acquisition clauses were met through acceptance of and continued work on the contract. Under CMMC, a third-party audit will be required.

How does my company get certified?

Wait until a process exists for certification. There are plans to stand up an accreditation body that will then identify and certify auditors who will conduct CMMC audits. The accreditation body is a work in progress, with several working groups. **There are no certified auditors at this time.**

Does CMMC replace FAR or DFARS cyber clauses?

No. CMMC is contractual; DFARS cyber clauses are regulatory. DFARS is not going away, and the CMMC requirement for third-party audit is in addition to DFARS compliance.

Does CMMC replace NIST controls?

Again the answer is no. DFARS requires implementation of NIST 800-171 controls, and the NIST controls informed the model versions, but CMMC Level 3 is not a one-for-one mapping to 800-171. There are additional controls and specific interpretations in CMMC Level 3. The DFARS cyber clause also includes specific procedures for incident reporting and use of cloud services.

That said, continuing to work on implementing NIST 800-171 is a great way to mitigate risk and prepare for CMMC.

If I am a DOD contractor, am I included in DOD's defense industrial base (DIB)?

Yes. At this time, CMMC is required even if your company does not handle Controlled Unclassified Information (https://www.acq.osd.mil/cmmc/faq.html, Question 20).

What steps can I take to prepare for CMMC?

We have two recommendations.

1. First, if you know your security maturity could be better or you are working towards full DFARS compliance, keep going. Auditors will not only be looking at documented procedures but will also look to see if your employees are following the procedures as written. The model version 1.0 is expected by the end of January.
2. Second, run a tabletop exercise to see how CMMC might impact your supply chain. For example, if you build something for the government and you have a sole-source supplier, what is the impact on delivering that product if your sole-source supplier cannot or will not get certified? A supply chain working group that represents subcontracts, contracts, legal, internal program managers and others will not only help with CMMC but with supply chain risk management.

PROGRAM TAKEAWAYS

- Homework Assignment: If you believe that you are solely offering COTS items to the government, either as prime contractor or subcontractor:
    - Before proposal submission, check all solicitations and push back on the Cyber Clause.

    - If the Cyber Clause already applies to a population of DOD contracts in your portfolio, seek counsel to develop a mitigation strategy.
- Even though CMMC is coming, it is not yet here. The best way to prepare for the expected CMMC implementation is to continue to comply or work towards compliance with DFARS 252.204-7012, NIST 800-171 and any associated cyber requirements while, in parallel, conducting a fresh self-assessment against anticipated CMMC requirements.