Pepper Hamilton LLP
Attorneys at Law

SERA BRYNN
PCI QSA CYBER SECURITY SPECIALISTS

# Government Contracts Cyber Café Series: Supply Chain and Third-Party Vendor Management April 17, 2018

## SPEAKERS

- Hilary S. Cairnie, partner and chair, Government Contracts Practice Group, Pepper Hamilton LLP
- Heather Engel, principal and co-founder, Sera-Brynn

## GOALS OF CYBER CAFÉ SERIES

Each Cyber Café webinar will cover specific cyber elements required in DFARS 252.204-7012 and provide practical insight on best practices and emerging trends. Webinars will be limited to 45 minutes and may feature guest speakers.

The 2018 Cyber Café Series will be Department of Defense-centric, with a majority of the time devoted to DFARS 252.204-7012 and the related clauses. Some topics will translate over to civilian contracting requirements and even to nonprocurement programs, but that is purely incidental.

## VERNACULAR

The DOD cyber clause is often referred to as the "DOD penetration clause." It includes many terms and definitions, such as:

- covered defense information
- controlled unclassified information
- cyber incident

## DOD FAQS

Within the last few days DOD has issued updated cyber guidance in an expanding list of frequently asked questions. The FAQs are available at https://dodprocurementtoolbox.com/cms/sites/default/files/resources/2018-04/Revision%20to%20Cyber%20DFARS%20FAQs%20-%20April%202%202018.pdf.

## OVERVIEW OF TOPICS COVERED

Today's session covers supply chain issues arising under the DOD cyber clauses.

**Who is in your supply chain?** Consultants, subcontractors, vendors and suppliers are included. But whether they should be covered by the DOD cyber rule depends on what they will be doing.

**Covered supply chain entities** include those whose "performance will involve" covered defense information (CDI) or those who will furnish "operationally critical support." Covered entities are required to be subject to the clause, even if the subcontract is for commercial items.

**Supplier Compliance:** *It is the responsibility of the prime contractor to include the cyber clause in any lower-tier orders, subcontracts and agreements.* Like all other government contract compliance requirements, the DOD cyber clause is not automatic — it has to be flowed-down during negotiations **and** included in the lower-tier contract in order for the supplier to actually be subject to the clause.

**Flowdown:** As with all mandatory flow-downs, it may be necessary to slightly alter the DOD cyber clause to allow for proper identification of parties.

**Foreign Suppliers**: Can the DOD cyber clause be enforced against covered foreign supply chain participants?

In a nutshell, foreign enforcement is a problem. There are numerous legal conflicts between the DOD cyber clause and the laws of foreign countries. Contractors should notify osd.dibscia@mail.mil for contracting assistance.

**Ownership of Responsibility**: As the prime contractor, you are accountable to the government for the cybersecurity of your supply chain. At every tier in the contracting chain, you are responsible for the cybersecurity of your supply chain.

**By signing the contract,** you are agreeing to comply with the terms of the contract, including the DOD cyber clause. Contractors are free to use whatever

mechanisms they may choose to audit and evaluate subcontractor compliance. That applies equally to vendors, suppliers and non-value-added resellers.

**Data Marking:** DoD will mark data in accordance with DoDM 5200.01 v4 and DoDI 5230.24.

**Large Business vs. Small Business Supply Chain:** It has been widely reported that small businesses lack the resources (*e.g.*, money, personnel, expertise, IT infrastructure, etc.) to effectively implement a cybersecurity compliance program as required under 252.204-7012.

Steps to mitigate small business risk:

- **MEP:** New legislation, the Enhance Cybersecurity for Small Manufacturers Act, amends the Hollings **Manufacturing Extension Partnership (MEP) Act**. The MEP Program is operated by NIST. The proposed legislation will (1) raise awareness of small business supply chain entities about DFARS 252.204-7012; (2) authorize MEP Centers to help small businesses conduct voluntary self-assessments to identify their cyber risks/gaps; (3) help small businesses develop and implement security measures to protect CDI.

- **MEP Centers:** Each state has one or more MEP Centers.
- **Procurement Technical Assistance Centers (PTAC)** are usually affiliated with Small Business Development Centers. DOD is actively working with PTACs to rollout cyber compliance information to assist small businesses.
- **Defense Industrial Base Cybersecurity Program**: Training and industry meetings.
- **Use cloud computing service providers to reduce risk.**
- **Use prime contractor facilities to leverage infrastructure investment.**
- **Keep up with DOD FAQs.**
- **Include cost of compliance investment** as a direct expense in subcontractor proposals that are covered by DOD rule.

## ATTENDEE QUESTIONS AND ANSWERS

***Q: What if my subcontractor refuses to accept DFARS 252.204-7012? Can I force it to accept the clause?***

A: If the subcontractor refuses to accept the DOD cyber clause, (1) it cannot receive, generate, touch, process, store, etc., CDI, and (2) it cannot provide operationally critical support.

You should look for a substitute subcontractor that will accept the clause **and** comply with it.

If the recalcitrant subcontractor is essential to performance, you should let the contracting officer know of the refusal and discuss approaches to resolve the controversy.

No matter how you might try to force the issue, assent must be voluntary; you cannot unilaterally impose the requirement absent assent.

***Q: If I am not the prime contractor, must my vendors and suppliers abide by 252.204-7012?***

A: If the prime contractor has, in fact, included the DOD cyber clause in its subcontract with you, then you must flow down to others the same clause if performance by those entities will involve CDI or operationally critical support.

But if the prime contractor failed to include the requisite clause in its subcontract, that will present a judgment call. There are good arguments on both sides of the issue as to whether you have a duty to include the clause in your supply chain.

***Q: Are you required under DFARS 252.204-7012 to validate compliance of lower-tier entities in the supply chain?***

A. DOD does not validate contractor systems or security and will not recognize third-party compliance assessments. Such an assessment, if obtained, will not excuse liability or responsibility for noncompliance with 252.204-7012.

What contractors should consider doing is auditing the supply chain. In its FAQs, DOD noted only that the usual means for supply chain management should be used; in other words, adapt what you already do to include cyber compliance. Auditing is a widely deployed way of identifying and mitigating risk.

## NEXT WEBINAR

May 15: Cloud Computing - FedRAMP Certification