Pepper Hamilton LLP
Attorneys at Law

SERA BRYNN
PCI QSA CYBER SECURITY SPECIALISTS

Government Contracts Cyber Café Series:
Oversight Is Coming: How to Prepare for a DCMA Supply Chain Audit
April 16, 2019

SPEAKERS

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

OVERVIEW OF WEBINAR

In a January 21, 2019 memorandum, the Department of Defense delegated to the Defense Contract Management Agency (DCMA) the responsibility for validating contractor compliance with marking and distribution statements on controlled unclassified information flowing through the supply chain, as well as the responsibility for assessing contractors' policies and procedures for supply chain management.

In this session, we explore how this new oversight role for DCMA may impact your organization.

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.

Reference Resources

The DOD memo issued on January 21, 2019 is titled "Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review" (hereafter, the CPSR Memo). For ease of reference, below are links to the CPSR Memo, the Contractor Purchasing System Review Guidebook, and two additional DFARS clauses, all of which pertain to DCMA's new oversight role in relation to monitoring contractor cybersecurity compliance. This new oversight role is a first

step on a path that is expected to lead to a much broader spectrum of DCMA activities in the cyber realm.

- Jan 21, 2019 Memo (https://www.acq.osd.mil/dpap/pdi/cyber/docs/USA000140-19%20TAB%20A%20USD(AS)%20Signed%20Memo.pdf)
- CPSR Guidebook (https://www.dcma.mil/Portals/31/Documents/CPSR/CPSR_Guidebook_022619.pdf)
- DFARS 252.244-7000 – Subcontracts for Commercial Items
- DFARS 242-244-7001 – Contractor Purchasing System Administration
- 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 FA (https://dodprocurementtoolbox.com/cms/sites/default/files/resources/201804/Revision%20to%20Cyber%20DFARS%20FAQs%20-%20April%202%202018.pdf)

GENERAL OBSERVATIONS OF THE CPSR MEMO

The CPSR Memo reminds us that DFARS 252.204-7012 and NIST 800-171 are required to protect and safeguard controlled unclassified information (CUI) that flows under most DOD prime contracts. Recall, DOD's cyber clause(s) became mandatory in contracts awarded on January 1, 2017 and thereafter.

And, remember that flow-down of DOD's cyber clauses to supply chain vendors and subcontractors is mandatory. Now would be a good time to review your lower-tier contracting forms, terms and conditions, and addenda to make sure that you are flowing down these clauses.

If you are a prime contractor or subcontractor under DOD contracts, then you are already subject to DCMA administrative oversight. Under the CPSR Memo, DCMA is tasked with two additional compliance activities that are focused solely on cybersecurity requirements:

1. *review of contractors' procedures for marking and distribution statements on flow down to Tier 1 suppliers*
2. *review of contractors' procedures for **assessing cyber compliance** of their Tier 1 suppliers.*

The first requirement (marking and distribution) is, in reality, an extension of what you are already doing in connection with marking and distribution of deliverable data requirements (CDRLs). The second requirement, however, actually constitutes a new contractor duty. Now, instead of relying solely on a subcontractor's representations and certifications relative to cybersecurity, the contractor has a duty to look behind the representations and certifications to validate compliance.

Note that for contracts **not** overseen by DCMA (*e.g.*, civilian agencies, NASA), the CPSR Memo mentions DCMA collaboration with the services and communities to implement similar validation procedures, but for this discussion, we are **only** talking about DOD contracts overseen by DCMA.

Marking and Distribution of Technical Documents Containing CUI

Procedures for marking and distribution should be based on the marking guidance provided at 32 C.F.R. part 2002, the CUI Registry, and DOD Instruction 5230.24, Distribution Statements on Technical Documents.

Procedures for marking and distribution are specifically addressed as a requirement under NIST 800-171, Controls 3.8.4 – marking media. However, we also recommend reviewing the definitions for "**controlled technical information**" and "**covered defense information**" in DOD's cyber clause 252.204-7012, as these may help guide your thinking as you establish or supplement your procedures for marking and distribution of CUI to lower-tier supply chain participants.

A natural starting point for expanding your marking and distribution policies and procedures to include supply chain participants is to look at your mechanism for marking and distribution of CDRLs (the data items that you are required to deliver to the government). Most prime contracts will specifically call out the applicable legends and distribution instructions when delivering to the government. In turn,

to the extent that your lower-tier subcontractors routinely contribute to the development of contract CDRLs, at least theoretically, they will already be subject to marking and distribution requirements for work product deliverables and therefore should have experience with those sorts of requirements.

The CPSR Memo now covers the reverse flow of information trickling down through the supply chain of vendors, consultants, subcontractors and the like. Hence, the upstream contractor must now expand its procedures to include all CUI, regardless of which direction it may flow, to include more than just final CDRLs.

Validation of Lower-Tier Cyber Compliance

Now let's look at part 2 of the CPSR Memo. DFARS 252.244-7001(c) states that the contractor's purchasing system shall establish and maintain policies and procedures to ensure purchase orders and subcontracts contain mandatory and applicable flow-down clauses, as required by the FAR and DFARS. *This clause provides the basis for DCMA reviewing the contractor's assessment of its supply chain*.

Another document to be aware of is the Contractor Purchasing System Review (CPSR) Guidebook. It was recently revised, effective February 26, 2019, with a specific change to emphasize the DFARS 252.204-7012 requirements for supply chain management.

CPSR Appendix 24 states:

> *When DFARS 252.204-7012 is applicable, the contractors must implement the security requirements specified in the National Institute of Standards and Technology (NIST) Special Publication (SP)800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. The Contractor's purchasing system will be evaluated to assess that:*

> *(a) The contractor's procedures ensure contractual DOD requirements for marking and distribution statements on DOD Controlled Unclassified Information (CUI) flow down appropriately to their Tier 1 Level Suppliers.*
>
> *(b) The contractor's procedures to assure Tier 1 Level Supplier compliance with DFARS Clause252.204-7012 and NIST SP 800-171.*

This appendix is a valuable read, but in this discussion we only focus on the note where it specifically states that your procedures must have the flow-down language.

Once onsite, the DCMA procurement specialist will be looking for evidence of supply chain compliance validation, to include things like vendor ratings, site reports and course of dealing exchanges in connection with all manner of cybersecurity topics, issues and concerns, to include, but not limited to, marking and distribution of CUI.

If we break down the CPSR guidance, there are five discrete elements that we recommend contractors address in order to be able to "assure supplier compliance:"

> 1. *Have a procedure to categorize suppliers so you know which are Tier 1 and which are not.*
> 2. *There must be procedures in place to **assess** Tier 1 suppliers. Who does it, how often, what are the assessment outputs, what are the follow-up measures, and how is the assessment documented?*
> 3. *There must be procedures to deal with and address suppliers that are not compliant. What are the next steps? What remedies are reflected in your written subcontract? What measures will be used to motivate, incentivize and obtain compliance? What impact does lower-tier noncompliance have on the contractor?*

4. *There must be a risk threshold defined for using a supplier that may not be compliant (in other words, when do we stop doing business with a supplier).*
5. *There must be documentation demonstrating that the contractor's procedures are being followed and are effective.*

Step 1: Categorize Suppliers as Tier 1 or Not

Tier 1 suppliers are typically viewed as those entities with whom you directly subcontract (this includes any kind of contract – vendor agreement, master service agreement (MSA), task orders, consultant agreements, etc.).

Tier 2 and lower-level entities are one or more levels of contracting removed from you (your subcontractor's subcontractors).

Step 2: Assess Tier 1 Suppliers

How does you assess your suppliers? There are a variety of methods. In the commercial marketplace, the "contractor" is often subjected to a numerous questionnaires and surveys from their clients or potential clients. A simple questionnaire is a potentially viable approach, but this can very quickly get out of hand any time there are multiple participants in the supply chain, with everyone giving and receiving questionnaires.

In the DOD marketplace, there is a convenient starting point. Assuming that the operative cyber clause (252.204-7012) has been flowed down from the prime contractor to its Tier 1 subcontractors, and so on down the supply chain, then everyone in the DOD supply chain is subject to NIST 800-171. In turn, anyone in the supply chain must also have a System Security Plan (SSP) and a Plan of Action and Milestones (POAM).

Recall that the SSP is supposed to document your compliance with each of the 110 controls established in NIST 800-171, mark them as compliant or not, and describe how they are implemented and how they address risk. Invariably, there are judgment calls to be made for many of the controls when it comes to how risk is mitigated. Too much control and the system will be cumbersome, clumsy, not

user-friendly and inefficient. Too little control and the system is not really effective at mitigating risk.

Any NIST controls that are not implemented or not fully implemented must be documented for further action in the POAM.

The SSP and the POAM are two critical documents demonstrating the current status of your control framework and the areas that require attention.

From each of your Tier 1 subcontractors, consider requesting and vetting their SSP. This might be a good first step, but remember that simply receiving the SSP will not be enough — a file copy, without more, will not demonstrate to DCMA how you actually assessed compliance. Someone internal or external to the organization who is competent to analyze the SSP will have to conduct due diligence and comment on its adequacy. So a copy of the SSP, coupled with an assessment summary and follow-up actions with the subcontractor, will put you in a much better position to demonstrate the adequacy of your assessment efforts.

Also bear in mind that the subcontractor may not agree to give up its SSP and/or POAM to anyone other than the government. After all, it likely contains sensitive information about the subcontractor's systems, procedures and weaknesses. Even with an ironclad nondisclosure agreement in place, once something is shared digitally, there is greater risk that it will be disseminated to unintended recipients.

There is no optimum, one-size-fits-all approach. But, whatever you decide for your policy and procedures, in order to implement them, you must include rights and remedies in your subcontract (purchase order, MSA, etc.) in order to be able to enforce those on your subcontractors. Every supply chain contract you sign going forward needs to account for data sharing, site visits, audits and delivery of objective evidence for supply chain assessment and incident response.

Step 3: Deal With Suspected Noncompliant Suppliers

Once you have a general idea of who in the supply chain is compliant and who is not, you need to decide what your next steps will be and what paper trail is to be created, communicated and filed.

Let's say you have decided to review SSPs and flag potential noncompliant suppliers for a more in-depth review. The protocols for doing so should be documented, and we would also recommend a description of what you are actually going to do during that deeper dive. This is synonymous with the "scope of audit" letters typically issued by the Defense Contract Audit Agency before conducting an audit. Among other things, think about:

- Will you request system vulnerability scans? Ask to perform your own scans of the supplier infrastructure? Request additional written artifacts?
- What if you identify one or more instances of noncompliance? Are they trivial or material? Does it even matter?
- Does noncompliance mean work should stop? If so, when? Does your contract allow you to do that?
- Should you confer with your government customer and request guidance?

For those NIST controls that are not fully compliant, recall that under DFARS 252.204-7012(b)(2)(ii)(B), contractors can request a variance from DOD CIO to determine whether the control in question is inapplicable or satisfied by an alternative but equally effective security measure. For your protection, you must be able to demonstrate your ability to manage and document subcontractor requests for variance, as well as incident response.

Step 4: Risk Thresholds

We have heard from many contractors big and small that smaller companies in the supply chain have chosen to opt out of defense work rather than deal with the hassle of implementing DFARS 7012. Assuming that is not you, we recommend including a section on risk in your supply chain management procedures.

For example, let's say you have a supplier that is critical to your business and that is clearly noncompliant. You will not be able to deliver the promised goods or services to the government without this supplier. How will you assess the risk of continuing to do business with this supplier if it is noncompliant with 252.204-7012 or NIST 800-171? Are you even able to contractually continue despite the noncompliance of this supplier?

The CPSR Guidelines list several areas to evaluate the supply chain management process, and knowing critical suppliers is number one. An approved supplier list (ASL) and a problem supplier list (PSL) or vendor rating system are ways to manage risk.

Step 5: Provide Proof Positive

Procedures or policies are not worth the paper they are written on if they are not demonstrably being followed. CPSR clearly identifies 12 questions that will be evaluated by DCMA during an audit to test, among other things, whether the contractor is actually doing what it says it will. When preparing your procedures, keep it simple — you do not need a fancy dashboard or other type of system, but whatever approach you adopt must be capable of producing the needed information on demand.

CONCLUSION

If you have not met the guidelines or are unclear on how to implement something in your organization, time is running out, and sooner or later DOD will become more rigorous in its efforts to enforce. The CPSR Memo is another step in DOD's efforts to put it in a position to enforce the cyber requirements.