Pepper Hamilton LLP
Attorneys at Law

SERA BRYNN
PCI QSA CYBER SECURITY SPECIALISTS

Government Contracts Cyber Café Series:
Cyber Incidents and Reporting Duties
September 18, 2018

SPEAKERS

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

Reminder: Our monthly series is intended to drill deeper into specific aspects of DOD's recently implemented, and now effective, cyber rules, which are embodied at DFARS 252.204-7012 and 252.239-7009. Our discussion topics are limited to DFARS, which covers DOD contracts.

Disclaimer: We do not address in these sessions the civilian agency counterpart regulations appearing at FAR subpart 4.19 and the clauses at FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems Jun 2016).

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

When it comes to cyber compliance, there is no-one-size-fits-all approach. Quite the contrary, every covered contractor information system should be viewed as unique, and achieving compliance will, more often than not, require a tailored approach.

Our goal is to help you sort out the knowns and the unknowns within your organizations so that you can make more informed business decisions.

To date, we have discussed the following topics:

- Supply chain considerations
- Cloud computing issues you can expect to encounter in dealing with internet service providers and cloud service providers (CSPs)
- Reducing the scope of your cyber compliance footprint
- Bid and proposal notifications: protecting your business with variance requests
- Self-assessment and re-validation: maintaining compliance and internal audits.

In this session, we discuss your duties and responsibilities regarding cyber incidents. Once you learn of a cyber incident impacting covered contractor information systems, you have multiple duties and continuing obligations, some of which are time sensitive.

In this session, we cover:

- Understanding segmentation and boundaries is key for incident response.
- What is required in the DFARS clause — forensics, etc.?
- Obtaining a certificate and making the report — before you can submit a report you must obtain a certificate that authorizes you to submit the report to the DOD portal (https://dibnet.dod.mil).
- What is included (in your incident report), and what you can prepare in advance?
- Which incidents must be reported?

Reminder, your reference resources are:

- DFARS 204-7300 and DFARS 252.204-7012 – Safeguarding Covered Defense Information and Cyber Incident Reporting
- DFARS 239.7600 and 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).

Some relevant definitions:

- Covered Contractor Information System (CCIS): Any unclassified information system that is owned by, or operated by or for, a contractor and that processes, stores or transmits covered defense information (CDI)
- Cyber Incident: Actions taken through the use of computer networks that result in a compromise of, or an actual or potentially adverse effect on, an information system and/or the information residing thereon
- Rapidly Report: Within 72 hours of discovery of any cyber incident.

Understanding Segmentation and Boundaries

- Do you receive or generate and process, store or transmit CDI?
- Do you have a single or multiple information systems? Is CDI segmented?

Foundational Assessment: *You must know which of your information systems are CCIS to determine the scope of your reporting obligations. A cyber incident that occurs on an information system that is not a CCIS should not trigger a report to DOD* — as long as the information system is properly segmented.

Ideally, you will learn of a cyber incident through your internal monitoring activities. It is also possible that you may learn of a cyber incident from federal monitoring activities.

Once you have determined that a cyber incident has occurred, and further determined that it is the sort of incident that requires reporting to DOD, what is next?

What is required per the clause? The following points are pulled from the primary DOD clause:

DFARS 252.204-7012(c): Cyber Incident Reporting Requirement. When the contractor discovers a cyber incident that:

> *1. AFFECTS (a) a CCIS or CDI residing therein, or (b) contractor's ability to perform the contract requirements identified as "operationally critical support" (OCS), the Contractor SHALL do several things:*
>
> *(i) Conduct a review for evidence of compromise of CDI,* ***including, but not limited to,*** *identifying compromised computers, servers, specific data and user accounts (this includes not only CCIS that were part of the cyber incident; but any other information systems that may have been accessed as a result if the incident, to identify compromised CDI or that affect contractor's ability to provide OCS.*
>
> *(ii) Rapidly report the cyber incident (72 hours) to: https://dibnet.dod.mil.*

Do not submit the report to the contracting officer, but you must notify the CO or the next higher-tier customer, if you are not the prime contractor, that you are filing such a report. To be clear, everyone files the report with DOD via the DIBNET portal and notifies their customer that the report has been submitted.

Upon receipt, DIBNET automatically assigns an incident report number for tracking and reference purposes.

> *2. Such a report, designated as a "cyber incident report" shall be treated as information created by or for DOD and shall include at a minimum the required elements at https://dibnet.dod.mil.*
>
> This is important because it affects your rights to protect information submitted to DOD. See DFARS 252.204-7102(j).

3. Obtain a medium assurance certificate (MAC). Contractors and subcontractors are required to obtain a DOD-approved MAC in order to report cyber incidents.

Continuing Duties

252.204-7012(d). Malicious software. When you identify malicious software in connection with a reported cyber incident, submit the malicious software to DOD Cyber Crime Center (DC3) as instructed by DC3 or contracting officer. DO NOT SEND THE MSW TO THE CONTRACTING OFFICER.

252.204-7012(e). Protect and preserve media. For at least 90 days after reporting the cyber incident, protect and preserve images of all known affected information systems identified to DOD and all relevant monitoring/packet capture data. This allows DOD sufficient time to assess the report and request or decline delivery of the preserved images and media.

252.204-7012(f). Access for forensic analysis. If requested by DOD, grant access to DOD personnel to inspect equipment and information to allow for forensic analysis by DOD.

252.204-7012(g). DOD Damage Assessment Activities. If DOD elects to conduct a damage assessment, the contracting officer will request that you furnish all damage assessment information prepared by you per paragraph 7012(e).

252.204-7012(k). Other duties. In fulfilling its duties under 252.204-7012, contractor is obligated to comply with all applicable laws and regulations concerning interception, monitoring, access, use and disclosure of electronic communications and data.

What this means is that your efforts to comply with the cyber incident reporting requirements should be coordinated with the active participation of legal counsel working alongside your forensic personnel and consultants who possess the requisite knowledge of the DOD cyber rules.

252.204-7012(l): Other obligations. In addition to the reporting and safeguarding requirements of this single clause, contractor is also required still to comply with

any other reporting and safeguarding requirements specified under other clauses or in government statutes or regulations.

What this means is that a contractor is obligated to conduct legal due diligence on the entire contract (and, by necessity, all DOD contracts) to identify **all** reporting and safeguarding duties recited in any other clauses or regulations/statutes applicable to the contract.

Obtaining a Mac or Other Reporting Certificate and Preparing the Actual Report

What is involved in obtaining a MAC? Should contractors obtain a MAC before a cyber incident occurs or wait until an incident has been discovered?

We always recommend contractors obtain a certificate for reporting before actually needing it. In our experience, clients have seen this take anywhere from a day to weeks. There may be processing delays. Three types of certificates are:

- A computer-based certificate, which is simplest to obtain but restricted to that specific workstation
- A hardware USB token from an External Certificate Authority (ECA)
- Common Access Card (CAC)

This external link on DIBNET portal (https://iase.disa.mil/pki/eca/Pages/index.aspx) will take you to the ECA program. There are two vendors.

Cleared contractors may find that their facility security officer (FSO) has the appropriate certificates. In that case, the FSO could make the report. Verify that certificates actually work before needing them.

What Information Is Including in the Cyber Incident Report?

The list is long, and much of this information can and should be gathered **before** an incident:

- Company name
- Company point of contact information (address, position, telephone, email)
- Data Universal Numbering System (DUNS) number

- Contract number(s) or other type of agreement affected or potentially affected
- Contracting officer or other type of agreement point of contact (address, position, telephone, email) for each affected or potentially affected contract
- USG program manager point of contact (address, position, telephone, email) for each contract
- Contract or other type of agreement clearance level (Unclassified, Confidential, Secret, Top Secret, not applicable)
- Facility CAGE code
- Facility clearance level (Unclassified, Confidential, Secret, Top Secret, not applicable)
- Impact to CDI
- Ongoing ability to provide operationally critical support (OCS) **if** your contracts specify that you are to provide OCS
- Date incident was first discovered
- Location(s) of incident — facility, department, network, server, devices
- Incident location CAGE code
- DOD programs, platforms or systems involved
- Type of incident — unauthorized access, unauthorized release (includes inadvertent release), malicious software, unknown, not applicable
- Description of technique or method deployed by infiltrators — what do you know about how they did it
- Incident outcome (full or partial compromise of CCIS and/or CDI, failed attempt, unknown)
- Incident/compromise narrative: This should be artfully drafted, factual, not speculative, and draw in the input of multiple stakeholders
- Any additional information.

Who Gets the Report?

The DOD contractor makes one report to the DIBNET. FAQ 50 informs that contracting officers are not to add unique cyber reporting requirements for DOD contracts.

But here, again, you need to know what is in all of **your** government contracts. If you perform work for DOD, DOE, VA, DHS and other agencies, the non-DOD agencies may have agency-specific reporting requirements, and a report submitted to DOD could trigger, for example, the need to report separately to the VA or another agency.

The actual cyber incident report is not submitted to the contracting officer. The CO is an informational conduit between the contractor and the DOD cyber shop.

QUESTIONS

Q. If my organization uses cloud storage how does that affect my cyber incident reporting obligations, if at all?

A. Refer to DOD FAQ 103. You are required to include the DOD clauses in your lower-tier vendor and subcontractor agreements that involve CDI. Assuming you have done so, the cloud service provider has the same reporting obligations as you — your cloud service provider must comply with the requirements in paragraphs 252.204-7012(c) – (g). And, for cloud service providers, there is the additional clause at 252.239-7010, which reiterates many of the same requirements.

Q. How do I know if a cyber incident that occurs on my IT network is actually a reportable incident under DOD rules?

A. It is complicated, but the answer is rooted in the terms and conditions of your government contracts **and** in the organization of your information system(s). There are several steps involved:

- Do you have DOD contracts that include 252.204-7012?
    - If no, check for FAR clause coverage and agency-specific cyber clauses (VA, SSA, others).
    - If yes, do you receive, generate, process, transmit or store CDI as part of your required performance?
        - If yes, is your information system segmented or consolidated?
        - Did the cyber incident occur on a CCIS?
            - If yes, you must disclose to DOD.

- If no, you probably do not have to disclose to DOD, but check for supplemental and tailored clauses to be sure that there are no other reporting duties.

Q. Does the government have duties stemming from a cyber incident report?

A. Yes, the government has certain duties primarily relating to the handling and disclosure of contractor attributional/proprietary information provided in support of a cyber incident report. In a nutshell, the government must protect as confidential any and all such contractor-furnished attributional/proprietary information from public dissemination, but the government has a degree of latitude if the information in question was created by or for DOD vs. created by the contractor for reasons other than cyber incident reporting.

But note that the contractor shall, to the maximum extent practicable, mark all attributional/proprietary information.

A further analysis of the government's duties and the permissible or prohibited disclosures is beyond this seminar's scope. Just be mindful that there are rules in place any time the government may have to disclose contractor attributional/proprietary information.

How can you mitigate the risk of having to report a cyber incident? There are two kinds of cyber incidents — those that are reportable and those that are not. Not every cyber incident will trigger a reporting obligation.

Back tracking to an earlier seminar, it is **highly** advisable for contractors and subcontractors performing DOD contracts to consider segmentation of information systems to reduce the number and size of CCIS that will be subject to 252.204-7012 requirements. If you operate a fully integrated information system that captures CDI and non-CDI, a cyber incident that is directed at non-CDI may well trigger a duty to submit to DOD a cyber incident report. But if you segregate CDI to a standalone information system, it is far less likely that a cyber incident on a non-CDI information system will trigger a cyber incident reporting obligation.

Here are some things to consider in trying to reduce your risk:

- Capture, store, process and transmit CDI on an information system that is separate from all other commercial and nongovernmental information systems.
- Use cloud computing resources to capture, store, process and transmit CDI.
- Reduce the in-house CDI storage footprint.
- Consider the possibility of using government-owned-and-operated information systems at government facilities; performance off-site.

Separate and apart from the cyber incident reporting requirements and your continuing interactions with DOD officials and investigators, you may be faced with a public relations crisis. Recall the OMB cyberattack of several years ago — a public relations nightmare.

Join us on October 16, 2018 when we will discuss “Crisis Management – Managing the Aftermath of a Cyber Incident.” Our guest speaker will be Loren Dealy-Mahler of Dealy Mahler Strategies.