Pepper Hamilton LLP
Attorneys at Law

SERA BRYNN
PCI QSA CYBER SECURITY SPECIALISTS

Government Contracts Cyber Café Series:
Bid and Proposal - Protect Your Business With Notifications
July 17, 2018

SPEAKERS

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

Reminder: 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).

Reminder: 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. 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.

OVERVIEW OF WEBINAR

In this session, we discussed DFARS 252.204-7012(b) and NIST SP 800-171, the importance of the system security plan and the related plan of action, the process for seeking a variance from NIST 800-171, and DOD's current guidance on these topics.

Our starting point was 252.204-7008 and 252.204-7012(b) and (m), all of which discuss the mechanism for obtaining a variance from the stated cybersecurity requirements. If you know that your current security plan has gaps or that you are

deploying a process, control element or other feature that fulfills the requirement, albeit in a manner that is not in line with the stated requirement, or if you believe that a stated cyber requirement is just not applicable to your organization, you must seek a variance in advance of the contract award.

The System Security Plan, Plan of Action and Milestones, and Mitigating Measures

We look to NIST 800-171 for important details about the scope and extent of needed controls. Two important road maps prescribed in 800-171: **The system security plan (SSP) and the plan of action (POA) (to correct deficiencies), sections 3.12.4, and 3.12.2, both of which DOD has assigned highest priority (5).**

- *So, where is your company right now? Do you have a written SSP?*
- *Have you identified deficiencies? Developed a written POA?*

According to DOD, "New entrants to DoD or federal contracting who are working to implement some of the NIST SP 800-171 requirements, **can be considered as having 'implemented NIST SP 800-171' if they identify in a system security plan the requirements that are yet to be implemented; develop associated plans of action to describe how unimplemented security requirements will be met, and any mitigations that are in place.** It is the responsibility of the requiring activity to determine the level of acceptable risk for requirements that are not yet implemented." DOD FAQ No. 53

If you do not already have it in your files, you should download the April 2018 FAQs issued by DOD; these FAQs provide the most detailed cybersecurity guidance to date issued by DOD. They are available at http://www.pepperlaw.com/resource/32778/19I2. Aspects of our discussion are addressed in FAQ Nos. 59-65.

Most contractors are most concerned about the covered contractor information systems (CCIS) that they operate within their organization; this refers to your internal networks that may store, process or transmit covered defense information (CDI). Where the CCIS is not part of an IT service or system *operated on behalf of the government*, you must comply with NIST 800-171 "Protecting

Controlled Unclassified Information in Nonfederal Information Systems and Organizations" and specifically the version of NIST 800-171 in effect when the solicitation is issued, unless otherwise directed by the contracting officer. DFARS 252.204-7012(b)(2).

NIST 800-171 sets forth 14 key areas of cybersecurity, each with several stated measures. The primary areas are:

(1) access control
(2) awareness and training
(3) audit and accountability
(4) configuration management
(5) identification and authentication
(6) incident response
(7) maintenance
(8) media protection
(9) personnel protection
(10) physical protection
(11) risk assessment
(12) security assessment
(13) systems and communication protection
(14) systems and information integrity.

In addition there are a total of 110 measures embodied under the 14 primary areas of cybersecurity. Hence, there are a lot of moving parts involved in complying with NIST 800-171, and therefore 252.204-7012. With so many moving parts, you can appreciate the importance of having a tracking tool to monitor the full measure of your compliance and identify the gaps: *That tracking tool is your SSP coupled with the POA and mitigating measures*.

The SSP and POA and mitigating measures are dynamic monitoring mechanisms and should change over time to reflect fewer gaps and reduced need for mitigating measures.

Process for Obtaining a Variance Under DFARS 252.204-7012

You must request a variance for any unmet NIST requirements unless "the contractor's policy, process, etc. does not allow the circumstances addressed" in a particular NIST 800-171 security requirement. DOD FAQ 62. Indeed, the policies, procedures or technologies that are used to prohibit certain functionality (e.g., remote access or connection of mobile devices, etc.) are considered by DOD to be an implementation of the NIST requirement. According to DOD, a variance request and adjudication is not required under those circumstances. That bears repeating: A systemic prohibition of a system capability or functionality that is otherwise covered by 800-171 may be considered by DOD to be compliant with 800-171 insofar as that specific requirement.

Additionally, "where specialized systems, such as medical devices, CNC machines, or other shop floor equipment, cannot by their nature meet the NIST 800.171 requirements," there is no need to request a variance for an alternative or a determination of nonapplicability. "These situations should be addressed in the contractor's system security plan." DOD FAQ 62.

When a variance request is required, however, you must use the process established in the clauses. 252.204-7008, 252.204-7012(b)(ii). There is no standardized form or template.

There is no explicit time limit specified in the contract clause for considering and deciding your variance request, but, implicitly, it is supposed to be adjudicated by the DOD CIO before the contract award. According to DOD, the typical turnaround for adjudicative decisions is about five days after all needed information has been furnished. Accordingly, you should submit any variance request at the earliest occasion in the bidding process.

The chain of communications is always through the contracting officer; DOD CIO personnel are not supposed to communicate directly with the contractor. The decision is routed to the contracting officer for distribution to the contractor. DOD FAQ 60.

If you have received a favorable adjudication of your variance request, you "shall" provide a copy of that approval decision to the contracting officer in order for it to be recognized under a contract. The approved variance is required to be included in the contract, but, seemingly, the burden is on the contractor to make sure that the procuring agency has the decision on file and includes it in any contract award.

The variance mechanism applies to prime contractor under 7012(b)(2)(ii)(B), as follows:

> *252.204-7012(b)(2)(ii)(B): Contractor shall submit requests to vary from NIST SP 800-171in writing to the Contracting Officer, for consideration by the DOD CIO. The contractor need not implement any security requirement adjudicated by an authorized representative of the DOD CIO to be (i) nonapplicable, or (ii) to have an alternative, but equally effective, security measure that may be implemented in its place.*

And there is 252.204-7008(c)(2):

> *The offeror shall submit [ ] a written explanation of –*
> *(A) why a particular security requirement is not applicable; or*
> *(B) How an alternative but equally effective , security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.*

And, it applies to all subcontractors under 7012(m), by virtue of mandatory flowdown, as follows:

> *Subcontractors are required to: notify the prime contractor (or next higher tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)B) of this clause.*

The Variance Request: Form and Content

Common sense suggests that in your written request you should:

> *1. Identify. Identify each NIST security requirement for which you seek a variance. For example, NIST 3.1.14 – Route remote access via managed access control points.*
>
> *2. State. Clearly state your reason(s) for seeking the variance, for example, the company does not permit its employees to have remote access to the company's IT system setup to collect, develop, receive, transmit, use or store CDI. Therefore this security requirement is not applicable to our organization.*
>
> *3. Explain. Provide additional details to demonstrate that your stated reason for nonapplicability or variance is well-founded. For example: (1) We have a written policy prohibiting employees from using any remote access applications to access our CDI servers. (2) We have installed firewall protection (name the program, application) on our CDI server which prohibits remote access, issues an alert, etc.*
>
> *4. Provide. Do include supporting documentation to educate DOD CIO more fully about the prohibition and protection against remote access and be prepared to provide additional information if requested. This might be a good place to include your SSP, POA and mitigating measures.*

Artful Drafting. Writing a good proposal is hard enough under the best of circumstances. With the inclusion of DOD's cyber requirements, that task becomes even more challenging for many companies because they are not yet fully compliant with those requirements and they may not even know the extent to which they are not compliant.

There are several takeaways:

1. Closely examine your processes, policies and technology, and identify all specialized systems that cannot, by their nature, meet a NIST requirement to determine the particular NIST requirements for which you will need to submit a variance request.
2. Until DOD CIO approves your variance request, you are still subject to the full extent of NIST 800-171 security requirements, save only those requirements that cannot be implemented on specialized systems.
3. Your variance request is submitted to the contracting officer directly, not to the prime contractor or next higher-tier subcontractor.

4. Subcontractors must notify the next higher-tier customer that a variance request has been submitted or is pending.
5. Submit your variance request at the earliest possible occasion.

ATTENDEE QUESTIONS AND ANSWERS

Q: Do you have any thoughts on third-party relationships that do not have direct impact on DOD-related contracts but where there could be potential risks due to said relationship with DOD-contracted entity?

A: Third-party relationships absolutely can impact your overall compliance with DOD cyber requirements, even if those third parties do not participate in performance of unrelated DOD contracts or unrelated DOD subcontracts. Remember that scoping the environment is critical to understanding how third parties can impact the security of CDI.

Q: We are not fully compliant with the DFARS cyber clause or NIST 171, should we include a section in our proposal highlighting the steps taken to comply to date and calling out the various elements that have not yet been implemented?

A: Probably not. With regards to cyber compliance, a proposal discussion that admits to not being fully compliant will not likely protect the company and may well result in rejection of the proposal. The regulations provide a process for seeking a variance from the stated requirements when full compliance may not be achievable. That is the best approach for mitigating risk.