There are those who listen and prepare, and there are those who do not listen and are therefore surprised. Which are you?

Which is your company?

Let's find out.

Question #1: How long has Apogee Consulting, Inc. been warning its clients and blog readers about the importance of cyber-security?

Answer: *Nearly 10 years.* Our **first article** that mentions cyber-security was posted in November, 2009. We wrote: "We frequently report on advances in aerospace and defense technology. As the AW&ST article reminds us, our adversaries are making advances as well, perhaps in areas in which we are vulnerable to exploitation. In 21st century warfare, securing the lines of command, control, communications, and computers (C4) and making effective use of ISR information may be more important than securing the lines of supply."

It would not be our last article on the topic. Just a few months later, we **discussed** some proposed DFARS contract clauses and opined that "it seems entirely appropriate for the DOD to consider issuing basic standards of minimum cyber protection to its industrial base, and to require reporting (including root cause analyses) when network breaches occur and data is compromised. And we applaud the opportunity offered industry to help shape the rule and its implementation. We hope knowledgeable companies will help DOD craft a good rule that is easily implementable. After that, companies will need to comply with the requirements of the new contract clauses, or else risk accusations of breach of contract (or worse)."

Those early articles were followed by many more. Our point is: had you listened and acted, you would have had nearly a decade to get ready for DOD's current emphasis on cyber-security.

Question #2: Is your Purchasing System cyber-ready?

Answer: *Probably not.* It caught many folks by surprise when DOD decided to verify contractors'

cyber-readiness and cyber-compliance via reviews of contractor purchasing systems (CPSRs). It was only last month that DOD's approach became apparent. We **told you** about the situation almost immediately.

Question #3: Forget cyber-security. Let's talk about good ol' supply chain management. You know: interaction with suppliers after award of a subcontract. Does your company place the proper emphasis on that aspect of program management?

Answer: *Almost certainly not.* And it's a shame, too. Apogee Consulting, Inc. is not just a bunch of beancounters; we have chops in the program management space as well. And with respect to supply chain management, we have been exhorting readers to focus on this area for, quite literally, *years*. Here's one good **example** from 2010, where we told readers "*The risks demand a serious and near-term response. Our goal should be to establish a "product pedigree" for our supply chain through creating an unbreakable chain of custody from first source through the various manufacturing and fabrication and assembly and finishing steps.*" That was nine years ago. And that wasn't even our first article on the topic! We continued to beat that drum over the past nine years, including **this straight-in-your-face posting** (also from 2010) that opined: "Listen, folks: *Whether you call it Supply Chain Management, supplier management, or subcontractor management, it is the key to success.* Period." (Emphasis in original.)

And so, having recited the litany of our reporting on this issue, having clearly supporting the assertion that "we told you so," we now tell readers that the latest DCMA CPSR Guidebook has been **updated** . In the words of one contractor's purchasing compliance lead, the result is "ugly" for contractors. Appendix 24 of the Guidebook 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 [and] (b)The contractor's procedures to assure Tier 1 Level Supplier compliance with DFARS Clause 252.204-7012 and NIST SP

800-171.

That bit above is not really anything new; it is almost a verbatim recitation of the policy letter we discussed last month. But what may be “ugly” is the following direction to CPSR teams:

The PA should ask the contractor to demonstrate their ability to protect CUI in accordance with DFARS 252.204-7012 and NIST SP 800-171. The PA will review subcontracts/POs to determine if the contractor has flowed down DFARS 252.204-7012 in all applicable procurement files within the selected sample. The PA should validate that CUI is properly marked in procurement files containing DFARS 252.204-7012 and be aware that no CUI should be present in procurement files where DFARS 252.204-7012 is not included. *The contractor must demonstrate how the CUI was transferred to their subcontractor. The PA should request that the contractor provide prime contracts containing CUI which was transferred to a subcontractor. The contractor must exhibit examples of CUI data transfers to demonstrate their ability to comply with this requirement.*

(Emphasis added.)

But wait. There’s more:

- The prime contractor must validate that the subcontractor has a Covered Contractor Information System (CCIS) that can receive and protect CUI. The prime contractor must show documentation that they have determined that the subcontractor has an acceptable CCIS to include an adequate System Security Plan (SSP).

- The PA must ask the contractor to demonstrate how they are managing and documenting their subcontractors’ request for variances.

-

The PA must ask the contractor to demonstrate how they are managing and documenting their subcontractors' incident report numbers.

It is becoming clear that the ability of a contractor to comply with DFARS 242.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting) is going to affect how the CPSR team scores compliance with Purchasing System adequacy criteria associated with supply chain management.

To wrap this all up, you and your company *should* be ready for the CPSR review team's questions in this area. You *should* do fine.

Unless, of course, you haven't been reading this blog. In which case, this sudden emphasis on cyber-security and secure supply chains may be coming as an unpleasant surprise demanding quick and expensive action.

Or—and this would be worse—you've been reading our warnings in these areas and you've been ignoring them. These posts have just been rants for your amusement, not to be taken seriously. In which case, shame on you.