In the past few years, there's been a *lot* happening with respect to cyber-security and counterfeit electronic parts in program supply chains. At this point, if you don't have a decent idea about what government customer expectations are, you are not likely to fare well in either competitions or reviews of your Purchasing System.

The thing is, most of this stuff is far from new. Government contractors—especially DOD contractors—have known (or should have known) what the expectations are. We've been reporting a lot of those expectations in this blog. For example, our first suggestion that cybersecurity might be a topic of some import was published in 2009 and our first article on the risk of counterfeit electronic parts in the supply chain was published in April, 2010. That's roughly a decade ago. Our first notice of the final DFARS rule that required "defense contractors to incorporate established information security standards on their unclassified networks and to report cyber-intrusion incidents that result in the loss of unclassified controlled technical information from these networks" was published in November, 2013—nearly six years ago. So none of the focus on supply chain management, whether is be on preventing introduction of counterfeit electronic parts or preventing data breaches—is new, at least to readers of this blog.

What's new is that your management is finally paying attention.

Your management is paying attention because the DOD has gotten its act together (okay, *largely*
gotten its act together) and is starting to enforce rules and to penalize contractors that aren't complying with them.

Recently, Ms. Ellen Lord (USD, Acquisition and Sustainment) announced creation of the DOD's Cybersecurity Maturity Model Certification (**CMMC**), to be used to evaluate contractors' compliance with regulations and to evaluate their adoption of good cybersecurity practices. Use of the CMMC reflects Ms. Lord's belief that "security [is] the foundation to acquisition." In other words, contractors that are not secure, as defined by DFARS contract clause and by the CMMC, should not expect to win a lot of contracts for cutting-edge technology.

In fact, Ms. Lord stated that "by June 2020, industry will see CMMC requirements as part of requests for information [and] by fall of 2020, CMMC requirements will be included in requests for proposals and will be a go/no go decision." Essentially, she was telling DOD contractors that

they have about one year left to get their act together. A year from now, contractors who score at the bottom of their CMMC evaluations will be at a significant competitive disadvantage, unless they are selling pencils and paper clips.

Which may have caused a bit of panic in your management team, unless they had been on top of the issues and been addressing them for the past few years.

In fact, if you want a quick litmus test of the competency of your leadership team, find out *when* they started to take this stuff seriously. The earlier they got started, the more competent they are. (Obviously, this is not the only area they need to be worrying about. But it's turning out to be a critical one for defense contractors.)

As we **told** readers earlier this year, DCMA reviewers are going to be testing compliance with cybersecurity requirements as part of Contractor Purchasing System Reviews (CPSRs). Importantly, the reviewers are going to look at more than just the purchasing files; they are also going to be looking for examples—and evidence—of transfers of Controlled Unclassified Information (CUI) between prime and subcontractor. While several commenters believe these review activities extend beyond the DFARS adequacy criteria, that belief is not going to stop reviewers from executing their mission—nor will it stop them from failing your Purchasing System if you can't evidence compliance in this area.

If you want to tackle these issues, start with knowledge and training. Then move into investment. You will need to invest a *lot* of money to fortify your information technology infrastructure. Once you have your own act together, then you will need to move into your supply chain. Although the government reviews start with the Purchasing System, make no mistake: this is about far more than simply flowing down contract clauses to subcontractors. Prime contractors must actually validate their subcontractors are complying with the requirements, and must be able to provide evidence of that validation.

Finally, this subject is actually wider than achieving competitive advantage and maintaining adequacy of one's Purchasing System. It's also about False Claims Act risk.

Cisco recently settled a FCA *qui tam* suit for $8.6 million. Relators alleged that "improperly sold video surveillance software with known vulnerabilities to US federal and state governments."

This article
by Business Insider includes the following statement:

With many contracts including pledges that products meet cyber security standards set by the government, experts have long warned that the claims could expand into that area and punish vendors for the vulnerabilities that are present in many systems.

There is pressure on contractors coming from many fronts, and that pressure may cause some contractors to falsely claim compliance when, in fact, they are not complying with cybersecurity requirements. Prime contractors may falsely claim to be properly managing their subcontractors. Subcontractors may falsely claim (to either their primes or other reviewers) that they are complying with cybersecurity requirements. The pressure, and the propensity for some contractors to take the “easy road” of lying rather than the “hard road” of complying, is likely to lead to more suits under the False Claims Act.

While we are not experts in information technology or cybersecurity, we do know a thing or two about compliance, and risks associated with non-compliance, with contractual requirements. This is an area in which the risks are high, and the consequences are becoming ever more severe.

If you are a contract manager, a government accountant, an auditor, or a compliance professional, this is a topic in which you need to be actively engaged. We suggest you get on it.