This is one of *those* articles where we say, "Told you so!" and "You should have listened" and suchlike and so forth. We almost didn't write it because of all the smugness in the air over at the vast cavernous spaces that are the Apogee Consulting, Inc., conference rooms. The smugness is so thick it might as well be the souplike fog of Victorian London; you know what we're saying? But then we thought, "Who's gonna know? It's not like these rants get much notice … so let's go for it!" And thus here we are with yet another polemic railing about secure supply chains and avoidance of counterfeit parts.

You may recall the prior discussion of same, **right here** , in which we *tsk'd-tsk'd* at our negligent readership, who had been hearing from Apogee Consulting, Inc. since April 2010 that it was time to jump aboard the "secure supply chain" bandwagon, and to circle those bandwagons to protect program supply chains from "the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."

We wrote "Contractors who have already created secure supply chain management systems, including not only policies and procedures, but also actual practices, will have an undeniable competitive advantage in evaluations where supply chain risk is a factor. Those who have not, will not. If you have been a long time reader, you have had more than three years to prepare for this day. Not that you took advantage of that advance notice, mind you. But the opportunity was there…."

Thus, while our November 2013 article pointed to the competitive advantage of a secure supply chain, now-six months later-we point to potential unallowable costs and a disapproved/inadequate Contractor Purchasing System as the price to be paid for failing to secure one's supply chain when required to do so. What happened? Well, the DFARS was revised via **Final Rule** that implemented aspects of the FY 2012 and FY 2013 National Defense Authorization Act (NDAA).

The DFARS revision establishes criteria for a system to "detect and avoid counterfeit electronic parts." It also establishes that those criteria will be evaluated as part of the Contractor Purchasing System Review CPSR). It established applicability and flow-down requirements. It is, in a nutshell, a very big deal.

First, the rule applies to CAS-covered prime contractors in which the applicable DFARS clauses are incorporated into their contracts. It does not apply to small business prime contractors, since those contractors are exempt from CAS. However, when a small business is a subcontractor to a prime that is subject to the new rules, then that small business subcontractor is also subject to the requirements and system criteria. According to the promulgating comments: "Suppliers, including small entities, will need to be able to trace the source of the electronic parts they are supplying to the original source if they are not the original manufacturer or current design activity, including an authorized aftermarket manufacturer."

So yeah, you small businesses may need to think about your supply chains as well. Our advice? *Think hard.*

With that out of the way, let's dig into the meat, shall we?

Counterfeit electronic part means an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

Electronic part means an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly (section 818(f)(2) of Pub. L. 112-81). The term "electronic part" includes any embedded software or firmware.

Obsolete electronic part means an electronic part that is no longer in production by the original manufacturer or an aftermarket manufacturer that has been provided express written authorization from the current design activity or original manufacturer.

Suspect counterfeit electronic part means an electronic part for which credible evidence

(including, but not limited to, visual inspection or testing) provides reasonable doubt that the electronic part is authentic.

More stuff from DFARS (Subpart 246.870, to be specific):

Contractors that are subject to the Cost Accounting Standards (CAS) and that supply electronic parts or products that include electronic parts and their subcontractors that supply electronic parts or products that include electronic parts, are required to establish and maintain an acceptable counterfeit electronic part detection and avoidance system. *Failure to do so may result in disapproval of the purchasing system by the contracting officer and/or withholding of payments* (see 252.244-7001, Contractor Purchasing System Administration).

Did you see that part above, the sentence we emphasized with italics? Did you see what happens to your Purchasing System if the DCMA reviewers don't think your Counterfeit Electronic Part Detection and Avoidance System is up to snuff? Yeah, go read that paragraph again, why don't you?

Okay, so the next step is to understand the criteria that determine whether your CEPDAS is up to snuff, or not. Here are the DFARS criteria associated with an adequate system:

A counterfeit electronic part detection and avoidance system shall include risk-based policies and procedures that address, at a minimum, the following areas (see 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System):

(1) The training of personnel.

(2) The inspection and testing of electronic parts, including criteria for acceptance and rejection.

(3) Processes to abolish counterfeit parts proliferation.

(4) Processes for maintaining electronic part traceability.

(5) Use of suppliers that are the original manufacturer, sources with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer or suppliers that obtain parts exclusively from one or more of these sources.

(6) The reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts.

(7) Methodologies to identify suspect counterfeit electronic parts and to rapidly determine if a suspect counterfeit electronic part is, in fact, counterfeit.

(8) Design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts.

(9) Flow down of counterfeit detection and avoidance requirements.

(10) Process for keeping continually informed of current counterfeiting information and trends.

(11) Process for screening the Government-Industry Data Exchange Program (GIDEP) reports and other credible sources of counterfeiting information.

(12) Control of obsolete electronic parts.

Piece of cake, right? No problemo!

So now you know how to establish an adequate CEPDAS and get it through a CPSR review. You might think you're home free. But wait a second; there's a bit more over in the DFARS Supplement Cost Principles. We now have a new Supplemental Cost Principle (231.205-71, entitled "Cost of remedy for use or inclusion of counterfeit electronic parts and suspect counterfeit electronic parts." That new Cost Principle states:

The costs of counterfeit electronic parts or suspect counterfeit electronic parts and the cost of rework or corrective action that may be required to remedy the use or inclusion of such parts are unallowable, unless-

(1) The contractor has an operational system to detect and avoid counterfeit parts and suspect counterfeit electronic parts that has been reviewed and approved by DoD pursuant to 244.303;

(2) The counterfeit electronic parts or suspect counterfeit electronic parts are Government-furnished property as defined in FAR 45.101; and

(3) The contractor provides timely (i.e., within 60 days after the contractor becomes aware) notice to the Government.

So not only is your Purchasing System at risk; not only do you face potential payment withholds; but you also face potential cost disallowance for what might otherwise be perfectly allowable direct and/or indirect costs. You best get on this right away.

Don't take our word for it. Here's a **client advisory** from the deeply knowledgeable attorneys over at McKenna Long & Aldridge. The advisory concludes with the following advice: "Contractors should immediately begin the process of comparing their existing systems to the counterfeit part detection and avoidance requirements to ensure that they are in compliance with these new requirements."

Yeah, what they said.