It has been awhile since we wrote about the importance of supply chain management. If you are a long-time reader (and, if so, thank you for that!) you know that, from time to time, we rant about the topic and implore you to *do something*.

Yeah, like that ever works.

If, for example, you had taken **our advice** posted in April, 2010, you might have started thinking about counterfeit parts and securing your supply chain, with the stated goal of a "product pedigree … through creating an unbreakable chain of custody from first source through the various manufacturing and fabrication and assembly and finishing steps." A few months later **we told** readers that effective management of their supply chain was the single most important driver of operational success. We also told readers about DOD positioning to "reward contractors for successful supply chain management." We have pointed out both the carrot and the stick, and too few of our readers gave a fig newton. It wasn't their issue.

More recently, we noted Section 818 of the 2012 National Defense Authorization Act (NDAA) and told readers that DCMA was considering "eliminating the 'Material Management and Accounting System (MMAS)' business system, and replacing it with a business system focused on detection and prevention of counterfeit parts (the "secure supply chain" system)."

Thus, nobody should be surprised to learn that the DAR Council recently issued an **interim rule** to implement Section 806 of the 2013 NDAA, which allows DOD customers to "consider the impact of supply chain risk" in evaluating proposals for certain types of national security system contract awards. According to the interim rule, the phrase "supply chain risk" is defined as "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."

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….

In **related news** , a final DFARS rule was published on the same day as the "supply chain risk" rule that requires "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."

You have been warned.