# Client Alert

**November 26, 2013**

# DOD Issues Interim Rule on Supply Chain Security

**By Peter McLaughlin, Bradley Wine and Rick Vacura**

On November 18, 2013, the U.S. Department of Defense (DOD) published an interim rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) that will likely prove controversial through the inclusion of supply chain security considerations in bid awards and service and task orders relating to national security systems (NSS). The interim rule, effective on publication, fulfills a statutory mandate and laudable goal but contains numerous provisions that will be difficult for contractors to manage. Comments on the interim rule are due by January 17, 2014.

Information security concerns have been front and center over the past several years, including with regard to the effectiveness of the White House's Comprehensive National Cybersecurity Initiative; the discovery of evidence of illegitimate or malicious hardware in government laptops; and the increased globalization of the supply chain, particularly for information technology (IT) products. Even genuine IT components, which are often designed, manufactured and finally assembled in various countries, may contain parts that are not produced by legitimate actors. The ensuing risk is that government IT, which is not the subject of proper supply chain integrity, may undermine federal and DOD security.

The interim DOD rule is part of a five-year pilot program to mitigate supply chain risk, pursuant to section 806 of the National Defense Authorization Act for FY 2011, titled "Requirements for Information Relating to Supply Chain Risk" as well as section 806 of the DOD authorization for FY 2013. Section 806 allows the DOD to consider the impact of supply chain integrity on procurement related to national security systems.

Section 806 defines supply chain risk 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." Thus, the challenge for DOD procurement, and the contracting community, is to determine an appropriate mechanism for identifying and handling supply chain risk that meets legitimate security concerns while providing the contractors with sufficient compliance guidance and a means to understand and, where appropriate, challenge the DOD's determination of a contractor falling short of its commitment.

The interim rule applies to the acquisition of IT systems that relate to intelligence or cryptologic activities, military command/control system, or that are an integral component of a weapon system. Therefore, the rule would not apply to IT used outside NSS. Within the NSS scope, though, the rule will apply to both commercial off-the-shelf (COTS) and non-COTS products and services.

Contractors are likely to have significant concerns about how the DOD determines compliance, communicates short-comings and provides a due process environment for providers of all sizes. Specifically, the current rule provides no indication of what the DOD expects contractors to do above and beyond existing supply chain

integrity programs or guidance on what such programs should incorporate. The potential for a contractor's exclusion is not limited to the contractor itself, but may bar a firm from using a particular subcontractor or prohibit that subcontractor from submitting any bids related to national security systems.

When the DOD awards a contract, disappointed bidders may not be informed that their supply chain program was deemed insufficient. The lack of such information could prevent contractors from understanding or remedying inadequacies in their integrity program or responding to erroneous information otherwise relied upon by the DOD. Furthermore, if the DOD elects to withhold information about the insufficiency determination, that decision will not be subject to appeal and cannot be the subject of a bid protest.

The DOD rule does include a mechanism to reduce the potential for the incorrect determination that a contractor's supply chain integrity program is insufficient. Only the head of a covered agency can decide to exclude a source under section 806. That decision must be provided in advance to the appropriate congressional committees and only after concurrence from senior-most procurement and intelligence officials of the DOD, and a written determination must be made that the exclusion under section 806 is "necessary to protect national security by reducing supply chain risk" and "less intrusive measures are not reasonably available to reduce" such risk.

The terms of the current interim rule present myriad challenges to contractors delivering IT products and services related to national security systems. Contractors will want to clarify what is required to obtain an acceptable integrity program rating and may seek an appeals process with sufficient information about any possible mitigation that could cure the inadequate protections. While it is understandable that security concerns restrict the disclosure of certain information, such as the knowledge that a particular chip supplier has delivered unlicensed technology, there is no indication of what "less intrusive measures… not reasonably available" means.

Comments are due by January 17, 2014.

The interim rule and request for comments may be found in the November 18, 2013, Federal Register at 78 FR 69268, impacting regulations at 48 CFR parts 204 *et seq*.

**For further information, please contact:**

**Peter McLaughlin**
(212) 336-4290
pmclaughlin@mofo.com

**Brad Wine**
(703) 760-7316
bwine@mofo.com

**Rick Vacura**
(703) 760-7764
rvacura@mofo.com

**About Morrison & Foerster:**

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for 10 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

*Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.*