November 6, 2015

On October 30, 2015, the Department of Defense ("DoD") issued a new rule, **Requirements Relating to Supply Chain Risk**, requiring its agencies to evaluate cybersecurity risks when considering contractors who provide Information Technology ("IT") that may affect National Security Systems. Under this rule, agencies must evaluate the Supply Chain Risk for a particular contractor offering to supply IT or related services, and may exclude the potential contractor if that contractor presents an unacceptable Supply Chain Risk to National Security Systems.

National Security Systems, defined by 44 U.S.C. 3542(b), are generally information systems that relate to intelligence or military activities, but do not include systems that are only used for "routine administrative and business applications, including payroll, finance, logistics, and personnel management applications."[1] The new rule 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 National Security System so as to surveil, deny, disrupt, or otherwise degrade the function, use or operation of the system."[2]

The new rule may be particularly challenging for IT contractors because it does not articulate specific factors agencies will consider when evaluating security risks. Additionally, companies that in the past have been considered merely vendors and suppliers will now be required to address these security risks even though they do not have privity of contract with the United States, the prime government contractor, or the first tier subcontractor. Contractors may be excluded from the bidding process on a case-by-case basis, and the factors agencies may consider can change from one opportunity to the next. Moreover, the agencies may not be able to share the information that leads them to exclude a contractor due to national security concerns.

The final rule was issued under Section 806 of the National Defense Authorization Act for Fiscal Year 2011. It was originally announced as an interim rule in 2013. The rule amends several sections of the Defense Federal Acquisition Regulation Supplement.

Defense contractors who provide IT services should consider whether their cybersecurity infrastructure provides adequate protection in order to reduce the risk of exclusion from potential opportunities with DoD agencies and maximize the chances of winning future bids.

Notes

1. 48 CFR Part 239.7301.
2. *Id.*

notices.

Key Contacts

Andrew Lustig Reston	alustig@cooley.com +1 703 456 8134
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090