Bloomberg BNA

Federal Contracts Report™

DOD

New DOD Cybersecurity Program Expected To Significantly Affect IT Contractors

The Defense Department is implementing a new pilot program under which it will screen information technology contractors for work involving national security systems and block those whose supply chain risk-management approaches it deems inadequate, all without explaining why.

The program is required under section 806 of the fiscal year 2011 National Defense Authorization Act (Pub. Law No. 111-383), which called on the DOD to weigh the impact of supply chain risk during the procurement process when national security systems are involved.

A Nov. 18 rule amending the Defense Federal Acquisition Regulation Supplement to authorize the program says the new mitigation steps are necessary to reduce supply chain risk in the acquisition of sensitive information technology systems that are:

- used for intelligence or cryptologic activities;
- used for command and control of military forces; or
- from an integral part of a weapon system.

The rule aims to avoid ''sabotage, maliciously introducing unwanted functions, or other subversion of the design, integrity, manufacturing, production, installation, operation or maintenance of systems.''

The rule applies to contractors involved in the development or delivery of any IT acquired by the DOD both as a service and as a supply. It covers purchases of commercial and commercial off-the-shelf (COTS) services or supplies.

Contractor Evaluations. Supply chain risk management can be included in contractor evaluations, and failure to achieve an acceptable rating can result in exclusion from contract awards and task or delivery orders issued under contracts. Contractors also can be barred from subcontracting with a particular source or directed to exclude a particular source from consideration for a subcontract when work on national security systems is involved.

The rule prohibits the disclosure to unsuccessful offerors of information related to the exclusion of contractors in pre-award, post-award notifications and post-award briefings. Contractors are barred from contesting the decision not to disclose information in these instances either in bid protests before the Government Accountability Office or in court.

Use of section 806 authorities is limited to the procurement of national security systems or of covered items of supply used within national security systems.

In addition, the rule limits use of section 806 by requiring that:

- the decision to exclude a source under section 806 be made only by the ''head of a covered agency'';
- the head of a covered agency seeking to exercise the authority of section 806 obtain a joint recommendation from the under secretary of defense for acquisition, technology and logistics (USD (AT&L)) and the DOD chief information officer, based on a risk assessment from the under secretary of defense for intelligence;
- the head of a covered agency, with the concurrence of the USD(AT&L), make a written determination that the use of section 806 authority is ''necessary to protect national security by reducing supply chain risk'' and that ''less intrusive measures are not reasonably available to reduce such supply chain risk''; and
- notice of each determination to exercise section 806 authorities is provided in advance to the appropriate congressional committees.

The rule took effect Nov. 18; the pilot program is set to expire Sept. 30, 2018.

Cybersecurity Threats. A leading analyst, Robert Metzger of the Washington, D.C., office of Rogers Joseph O'Donnell, commented that what appears to be a ''supply chain'' rule really has its principal purpose in defending the supply chain against cybersecurity threats. That is why the rule focuses on specially defined ''national security systems,'' he said.

The specific threat is that the supply chain that supports the DOD's critical intelligence, cryptological, national command and key military systems could be infiltrated with ''tainted'' electronic parts that harbor malicious code or hostile software in national security systems. While there is good reason for the government to protect against this threat, the new rule undoubtedly will be controversial and likely will end up the subject of litigation, according to Metzger.

As applied to contractors, the rule works by requiring new purchases of information technology supplies and services to include recognition of ''supply chain risk management'' as an evaluation factor or award criteria, Metzger explained. But the rules does not dictate specific supply chain risk management approaches or impose reporting, record-keeping or compliance requirements, Metzger said.

Some in industry had feared a ''worst case'' scenario of overly prescriptive rules. Instead, Metzger said, the

rule takes a flexible approach but it covers a broad swath of IT suppliers and service providers, including commercial and COTS purchases.

Detecting Tainted Source of Supply. The original intent of section 806 was targeting the source of bad parts, as the law permitted the exclusion of known or suspect sources. The new rule has a much broader reach across the supply chain, Metzger said. It can affect not only those that are the source of bad parts but also higher tier companies that may fail to detect a tainted source of supply. Still, Metzger said, contractors will find that application of the rule ''very much depends on what they supply, to whom they supply it, and for what purpose.'' In this sense, it is flexible in application, because it leaves much to contractor judgment and risk assessment.

But the rule also does not detail how supply chain risk management will be considered as an evaluation factor, Metzger said. The rule presents a quandary for contractors because it puts companies at risk of exclusion, if they have a poor history of mitigating risk in the supply chain, but the government is under no obligation to inform them of the source or nature of the problem.

In fact, ''companies can receive negative evaluations, lose contract awards, or be forced to jettison suspect vendors, without the government sharing any information as to 'why,' '' Metzger said.

The secrecy reflects the original terms of section 806, and respects the sensitivity of supply chain threat and vulnerability intelligence, Metzger said. However, it means that companies at many tiers of the information technology supply chain have neither information nor remedy if the rule is applied against them. Undoubtedly, legal challenge will come to those aspects of the rule, Metzger said.

Metzger added that he expects the DOD to provide more details about implementation in particular solicitations subject to the rule. Ultimately, he said, it will be up to the DOD buyer to include the new contract clause and to establish what it requires for compliant supply chain risk management.

BY DEBORAH BILLINGS

To contact the reporter on this story: Deborah Billings in Washington at dbillings@bna.com

To contact the editor responsible for this story: Jeff Kinney at jeffkinney@bna.com

Comments on the rule are due Jan. 17. The rule is available at: http://www.gpo.gov/fdsys/pkg/FR-2013-11-18/pdf/2013-27311.pdfv.

  FCR ISSN 0014-9063