COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Government Contracts
National Security & Defense

January 21, 2014

APPROPRIATIONS ACT PROVISIONS ON INFORMATION SYSTEM PROCUREMENT FOR CERTAIN AGENCIES

On January 17, 2014, President Obama signed into law the Consolidated Appropriations Act of 2014 ("the Act"), which appropriates $1.1 trillion dollars to fund the Government through September 2014. The Act includes a supply chain-related provision authored by Representative Frank Wolf (R-VA), chairman of the Appropriations Committee subcommittee that funds the Departments of Justice ("DoJ") and Commerce ("Commerce"), the National Science Foundation ("NSF"), and National Aeronautics and Space Administration ("NASA"). The Wolf provision — which is found in section 515 of the Act — specifically requires those agencies to review and evaluate the supply chain risk associated with any acquisition of so-called "high-impact" or "moderate-impact" information systems, according to criteria established by the National Institute of Standards and Technology. In connection with the supply chain risk assessment, the agencies must evaluate the risk of cyber-espionage or sabotage associated with systems being produced or assembled by one or more entities that the government identifies as posing a cyber-threat.

Section 515 represents a modification of earlier language that Rep. Wolf included in last year's continuing resolution that temporarily funded the government. While that earlier provision was specifically focused on potential information technology ("IT") procurements from China, the revised approach still highlights potential risk from China but also broadens the requirement such that it may impose heightened supply chain standards for a broader array of suppliers.

BACKGROUND - CONTINUING RESOLUTION LANGUAGE

In the March 2013 Consolidated and Further Continuing Appropriations Act of 2013 ("the 2013 Act"), Rep. Wolf inserted a provision that precluded DoJ, Commerce, NASA, and NSF from acquiring IT systems from entities "owned, directed, or subsidized by the People's Republic of China." The extent and reach of this provision was unclear. In particular, the 2013 Act failed to define either what it meant to be "owned, directed, or subsidized" by China or what constituted "information technology." This ambiguity lingered throughout the funding period authorized by the 2013 Act.

The provision also was subject to considerable criticism and pushback from U.S. industry. On April 4, 2013, a coalition of technical associations wrote to Rep. Wolf to express its concern with the language in the 2013 Act. The coalition argued that the 2013 Act would impede the Government's ability to protect itself because it would be limited in its procurement of cutting-edge IT, put civilian agencies at odds with Department of Defense cybersecurity reforms, lead to retaliation from the Chinese government, and encourage similar legislation in other countries. A similar coalition again wrote to Rep. Wolf on December 10, 2013 and requested he substitute the language in the 2013 Act with more neutral language requiring agencies to conduct supply chain risk assessments based on NIST standards. The coalition also noted that the law would "unnecessarily slow[] federal purchases of key technology, leaving government IT systems vulnerable.

SECTION 515 OF CONSOLIDATED APPROPRIATIONS ACT OF 2014

Confronted with the criticism of last year's approach — and in particular, the clear discrimination against China and the potential risk, in turn, for retaliation against U.S. companies in Chinese procurement — Rep. Wolf undertook a revised approach in the Consolidated Appropriations Act of 2014. The revised approach provides for an arguably narrower scope of the types of systems subject to the requirement, but also expands the suppliers that may be subject to the supply chain assessment and requires procurement officials to provide a certification to Congress — an extremely high administrative bar that may well have a tempering effect on procurements that involve supply from certain countries, including China.

Specifically, section 515 of the Act prohibits the acquisition of high or moderate-impact information systems[1] unless contracting officials for DoJ, Commerce, NSF, and NASA comply with the following acquisition standards.

First, section 515(a) requires the affected agencies to: (1) review the supply chain risk using criteria developed by the National Institute of Standards and Technology ("NIST"); (2) review the supply chain risk from the presumptive awardee against threat information available from the FBI; and (3) conduct an assessment in conjunction with the FBI to determine any cyber-espionage or sabotage risk associated with the acquisition of the information system, including "any risk associated with such system being produced, manufactured, or assembled by one or more entities identified by the United States Government as posing a cyber-threat, including but not limited to, those that may be owned, directed, or subsidized by the People's Republic of China."

Second, once contracting officials have conducted the assessments required by section 515(a), the agency head must: (1) develop a mitigation strategy for any identified risks in consultation with NIST; (2) determine that the acquisition of such a system is "in the national interest" of the United States; and (3) report that determination to the Committees on Appropriation of the House of Representatives and the Senate.

As noted above, these acquisition standards apply only to the acquisition of high-impact and moderate-impact information systems, which are defined by NIST Federal Information Processing Standard Publication 199 ("FIPS 199"). FIPS 199 defines high and moderate impact information systems as follows:

- High-impact Information Systems: The loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic adverse effect on organizational operations, organizations, assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries. High-impact information systems typically hold the Government's classified information.
- Moderate-impact Information Systems: The loss of confidentiality, integrity, or availability is expected to have a serious adverse effect on organizational operations, organizational assets, or

[1] FIPS 199 describes a low-impact information system as one where there would only be a limited adverse impact from a compromise such that the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

> individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries. Moderate-impact information systems typically hold much of the Government's unclassified information.

Significantly, although the Act sets the threshold for allowing acquisitions from entities posing a cyber-threat as "in the national interest," it does not define or specify how an agency head is to determine whether an acquisition is "in the national interest."

POTENTIAL PROCUREMENT ISSUES

Although it is not yet clear how the affected agencies will implement the new acquisition standards, those standards are likely to create a number of potential procurement issues.

First, the new Act places a high burden on contracting officials and agency heads and adds additional steps into an already long procurement cycle. To acquire information systems, agency heads must make a determination that the acquisition of that system is "in the national interest," and must report that determination to Congress. Although there is no explicit prohibition on acquiring information systems from entities posing a cyber-threat to the United States, contracting officials may be less willing to procure moderate or high-impact information systems from companies proposing products that originate in China or other countries that could be perceived as presenting a risk because they will not be willing to make the determination that the acquisition in question is "in the national interest" and/or reporting that determination to Congress.

Second, the broad applications and lack of definitions in the Act make it difficult to determine how section 515 will be interpreted by the affected agencies. For example, although the Act does not limit the prohibition to China, the naming of China in section 515 could adversely impact contractors who manufacture in or source parts from China, but also leaves contractors wondering which other manufacturing locations will present a similar risk in the eyes of the Government. Likewise, the lack of clarity as to what constitutes "in the national interest" may also dissuade agency heads from making that determination.

Third, section 515 imposes additional compliance obligations on contractors for managing their supply chains. As noted above, section 515 applies only to four agencies: DoJ, Commerce, NSF, and NASA. Enhanced procurement authority, which imposes similar supply chain restrictions, has been granted to the Department of Defense as to the acquisition of National Security Systems ("NSS"), to the Intelligence Community for the acquisition of "mission-critical products, materials, and services," and to the Department of Energy with regard to NSS, items related to nuclear weapons, and the components of such weapons. *See* New Intelligence Community Directive Addresses Supply Chain Risk Management (Jan. 9, 2014); New DFARS Rules Address Supply Chain Risks and Unclassified Information (Nov. 21, 2013). As a result, contractors are faced with the challenge of implementing varying compliance obligations for their supply chains, which may differ depending on the product or service being procured, as well as the agency conducting the procurement.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our government contracts and national security and defense practice groups:

Susan Cassidy	+1.202.662.5348	scassidy@cov.com
David Fagan	+1.202.662.5291	dfagan@cov.com
James Garland	+1.202.662.5337	jgarland@cov.com
Roger Zakheim	+1.202.662.5959	rzakheim@cov.com
Catlin Meade	+1.202.662.5889	cmeade@cov.com