Lexology
By: Steven A. McCain, Amy M. Conant, and Erica L. Bakies | May 22, 2019

# Policy Changes Highlight Contrasting National Security Acquisition Goals

A proposed policy change and an Executive Order issued in the past week highlight government contractors' need to stay abreast of the opportunities and restrictions resulting from a rapidly changing national security policy landscape. On Friday, May 10, 2019, the Federal Acquisition Regulatory Council ("FAR Council") published a proposed rule that would amend the definition of a "commercial item" to allow suppliers of nondevelopmental items ("NDIs") sold to foreign governments to take advantage of certain streamlined acquisition procedures afforded to commercial item contractors, thereby decreasing the barriers to entry associated with the federal marketplace. On May 15, 2019, the president released an Executive Order entitled "Securing the Information and Communications Technology and Services Supply Chain," to further his commitment to minimizing vulnerabilities in information and communications technology infrastructure and services in the United States. These two changes highlight an escalating tension in national security policymaking: whether the government needs to quickly and efficiently acquire the next and greatest technological advancement, or enhance safety and security of its supply chain, which can be compliance intensive and time-consuming. For companies actively involved in—or merely affected by—the government's national security agenda, it reinforces the need to keep up with the rapidly changing regulatory and policy landscape in order to achieve their federal business development objectives.

### Proposed Rule Expanding the Definition of "Commercial Item" to Include NDIs Sold to Foreign Governments

The proposed revision to the definition of "commercial item" implements statutory changes made by the National Defense Authorization Act for Fiscal Year 2018[1] The proposed rule would expand the definition of a "commercial item" to encompass certain NDIs sold to foreign governments, in addition to the domestic state and local government NDIs currently covered in the definition.[2]

FAR § 2.101 defines an NDI as "any previously developed item of supply used exclusively for governmental purposes by a Federal agency, a State or local government, or a foreign government with which the United States has a mutual defense cooperation agreement." NDIs also include items that meet this definition and require only minor modifications to meet the requirements of the procurement agency. Currently, the FAR states that "commercial items" include NDIs (1) that were developed exclusively at private expense, (2) that are sold to governmental entities in substantial quantities and on a competitive basis, and, notably here, (3) where such sales are limited to domestic governments (i.e., U.S. state and local governments). This definition matched the definition of "commercial item" found previously in 41 U.S.C. § 103. However, Section 847 modified 41 U.S.C. § 103 to include NDIs sold in substantial quantities on a competitive basis to multiple foreign governments, in addition to the current allowance for state and local governments. The FAR Council's proposed rule would modify the FAR clause to reflect this statutory expansion of items.

If finalized, the proposed rule could benefit vendors of NDIs that regularly sell goods in substantial quantities to foreign governments on a competitive basis. First, the rule would allow these NDIs to benefit from certain preferences for commercial items. Congress requires federal agencies to purchase commercial items "to the maximum extent practicable."[3] As a result, the proposed rule would allow vendors of NDIs sold to foreign governments to take advantage of this statutory preference and compete in acquisitions in which agencies solicit only for commercial items. Second, acquisitions for commercial items can contain significantly less "red tape" than traditional government contracts. To facilitate the purchase of commercial items, the U.S. Government eliminated a number of recordkeeping, reporting, and compliance requirements for commercial item contractors. For example, commercial item contractors are exempt from certain cost and price disclosures and implementing Cost Accounting Standards; they also have reduced audit rights and

are subject to fewer mandatory FAR clauses. Instead, the FAR explicitly provides that only those clauses "[d]etermined to be consistent with customary commercial practice" should be included in the solicitations for commercial items.[4]

### Executive Order on Securing the Information and Communications Technology and Services Supply Chain

The recent executive order seeks to mitigate vulnerabilities in the information technology supply chain by prohibiting transactions that pose unacceptable risks to national security. The order declares a national emergency "to deal with the threat posed by unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries." [5]More specifically, the order prohibits acquisition or use of information technology or services "where the transaction involves any property in which any foreign country or a national thereof has any interest" if the Secretary of Commerce has determined that:

- The transaction involves information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and
- The transaction:
    - Poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;
    - Poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or
    - Otherwise poses an unacceptable risk to the national security of the United States or the security and safety of U.S. persons.[6]

Notably, the order acknowledges the divergence between national security policies encouraging the use of the commercial marketplace, such as the proposed rule described above, and national security policies focused on increased supply chain security: "Although maintaining an open investment climate in information and communications technology, and in the United States economy more generally, is important for the overall growth and prosperity of the United States, such openness must be balanced by the need to protect our country against critical national security threats."

### National Security Policy Considerations

While these policy changes may only affect a small number of vendors that sell certain items to government entities, these changes highlight two competing views among national security policymakers. On one hand, certain policymakers are focused on improving the U.S. warfighter's capabilities by seeking more agile acquisition methods, which will theoretically facilitate better and greater access to the latest technology. The Section 809 Panel, which Congress tasked with identifying ways to enhance, streamline, and improve the defense acquisition system, states that this approach is needed: "DoD must put its acquisition system on a war footing and adopt a mission-first approach."[7] According to the Panel, this means "rapidly and effectively acquiring warfighting capability and delivering it to Service Members," which must take "precedence over achieving other public policy objectives."[8] As a result, the Panel's vision for the defense acquisition system will reduce "barriers that deny DoD opportune access to innovative technology and creative solutions from nontraditional companies."[9] In certain instances, the government has already taken this approach. For example, DoD has recently increased its use of procurement tools that allow it to act more like a commercial entity and at a faster pace, such as 10 U.S.C. 2371b Other Transaction Authority, which are agreements that are protest-proof and aimed at nontraditional government contractors.

On the other hand, national security policymakers are concerned about the U.S. government's supply chain and emphasize the security of systems, data, and communications. Allowing certain vendors to take advantage of decreased compli-

ance requirements present in a commercial competition may further a quick acquisition process, but this approach also reduces supply chain security by allowing products into the government's supply chain that are subject to less stringent oversight and inspection. The recent MITRE Corporation report, "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War," states that DoD has not effectively used its resources "to identify, protect, detect, respond to, and recover from network and supply chain threats."[10] MITRE contends that to thwart supply chain threats, DoD will have to "require improved relations with contractors, new standards and best practices, changes to acquisition strategy and practice, and initiatives that motivate contractors to see active risk mitigation as a 'win.'"[11] All of these recommendations require either the government or a contractor to invest energy and resources, and therefore time, in securing their own supply chains.

## Conclusion

The proposed FAR rule could provide new opportunities for vendors who supply NDIs in substantial quantities to foreign governments by relaxing certain compliance requirements from which commercial item acquisitions are exempt. At the same time, the recent executive order tightens the restrictions on the information technology and services supply chain, thereby increasing compliance and monitoring requirements for a number of suppliers. These policy changes serve as an illustrative example of the tensions between conflicting national security concerns and remind industry partners of the need to stay agile to adapt to the government's evolving national security needs.

## Notes:

[1] Pub. L. 115-91.

[2] *See* 84 Fed. Reg. 20607 (May 10, 2019).

[3] 41 U.S.C. § 3307; 10 U.S.C. § 2375.

[4] FAR § 12.301(a)(2).

[5] President Donald J. Trump, *Message to the Congress on Securing the Information and Communications Technology and Services Supply Chain* (May 15, 2019).

[6] Donald J. Trump, *Executive Order on Securing the Information and Communications Technology and Services Supply Chain* (May 15, 2019).

[7] Advisory Panel on Streamlining and Codifying Acquisition Regulations, *A Roadmap to the Section 809 Panel Reports* (Feb. 2019).

[8] *Id.*

[9] *Id.*

[10] Chris Nissen, John Gronager, Robert Metzger, & Harvey Rishiof, *Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War*, THE MITRE CORPORATION (2018), https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-8AUG2018.pdf.

[11] *Id.* at ii.