Hogan Lovells

ADG Insights

No, it's not only about China:

Why EU businesses need to know about US Department of Defense and other US Government supply chain requirements

August 2019

The export of military equipment from the European Union (EU) to the United States (US) is substantial. From 2014 to 2016, arms exports from the EU to the US totaled $7.6 billion, a figure that does not include the sale of other supplies, including communications equipment, to the US Department of Defense (DoD) and other government agencies.

In order to maintain competitiveness to sustain or even to grow these exports, EU manufacturers of equipment and supplies for sale to US government entities must track the emerging supply chain requirements, develop programs to ensure supply chain integrity, and be ready and able to engage with the US DoD and other US agencies to explain how their supply chain integrity programs protect US national security and meet emerging regulatory requirements.

Supply chain integrity has become a hot topic in US defense circles and in US trade policy. Supply chain integrity is ensuring that supply chain risks are minimized. The definition of supply chain risk according to DoD Instruction 5200.44 is "the risk that an adversary may sabotage, maliciously introduce an unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."[1] Harm can come from parts that do not meet specifications and, therefore, provide diminished performance. In addition, harm can come from components that include an "unwanted function" that allows an adversary to sabotage functionality or that beacons back to an adversary, providing invaluable insights on the activities and whereabouts of the equipment into which the component is incorporated.

Understanding US policy concerns about China and why they matter to your company

The publicly-reported focus has been largely on China, and on the transformative role that 5G technology is expected to play, along with the potential for Chinese equipment manufacturers to imbed espionage capabilities into that equipment. But Chinese parts are widely-used in manufacturing processes around the world, including in EU countries. For this reason alone, it is essential that forward-looking businesses in Europe and their legal advisors become familiar with emerging US supply chain integrity programs. In addition, the emergence of security as a possible "fourth pillar" in the DoD acquisition process – along with the current pillars of price, performance, and schedule – may have effects that go well beyond the Chinese origin of particular parts, and may affect procurement beyond that by the DoD.

The focus on China, particularly on Chinese companies that are state owned or subject to state control, reflects multiple underlying policy concerns. First, there is a generalized concern that China is rapidly becoming a technological equal of the United States and that it has a goal of achieving technological superiority. Buying from China, even indirectly, through parts incorporated in products sold by others, could thus contribute to the United States' relative decline. Another, and more forceful, concern relates to the ability of the Chinese and other foreign governments to corrode the integrity of the supply chain. An illustrative example, involving a Russian company, is the rationale underpinning the ban on US government purchases of Kaspersky's anti-virus software. Machines running that software would necessarily be in regular contact with the Kaspersky servers located in Russia, in order to receive the frequent software updates necessary to keep the anti-virus service effective and to report on new viruses encountered, providing Russia, through Kaspersky, the opportunity to closely monitor the activities and content of the computers on which the software is running. Parts, particularly those subject to firmware updates, can present similar risks when communications flow to and from the equipment without the control or knowledge of the owner of the equipment. Trusting the creator of software, in the case of Kaspersky, or the manufacturer of parts, in the case of manufacturers subject to Chinese or other state control or influence, is believed by US defense and intelligence personnel to be a risky proposition.

Of course, not all parts pose the same magnitude of risk. Work is underway in the United States to

1. DoD Instruction 5200.44, Incorporating Change 3, 10/15/2018, Glossary, available here.

prioritize the parts that pose the greatest risks of creating a "back door" to potentially sensitize information. Work is also underway on developing criteria for determining which manufacturers of parts pose the greatest risks. There are a number of open questions, including:

Should the level of concern be the same for western companies operating in China as for Chinese government owned companies?

Some argue that all entities with locations within China, even if the company itself is owned elsewhere, are subject to state control, directly or through local employees.

Are there protections that could be established by those western companies that would be credible, but which if established by a Chinese-owned company, would not?

Western companies and some of their key employees could be easier to reach for civil or criminal enforcement actions than would be the case with Chinese-owned companies and their key employees. Commitments backed by robust consequences for their violation could be more credible than the commitments that could be provided by Chinese-owned companies.

Are there measures that could be taken by manufacturers utilizing Chinese manufactured parts that could credibly ensure that those parts pose no threat?

The testing of Huawei components by the United Kingdom might be a model that holds promise as an alternative to a flat ban.

The practices of your subcontractors present an additional risk

A recent civil settlement between Sapa Profiles and NASA illustrates another kind of supply chain risk that manufacturers need to be aware of and be able to address. Sapa agreed to pay almost $50 million for improperly certifying to a rocket manufacturer that the metal components it provided met contract requirements. Problems with the metal resulted in the loss of two space launch vehicles and of their payloads worth $700 million.[2] The prime contractor required the subcontractor to certify compliance. Although the subcontractor did so, the product did not comply. In this case, the subcontractor's personnel reportedly truly believed that the metal was excellent and fully up to the task, so what would the harm be in certifying that it met specifications when those specifications, they thought, were unnecessary?

This is a cautionary tale. The prime contractor lost years of business when NASA ceased using the rockets to determine the cause of the mission failures, and the subcontractor faced criminal charges as well as civil liability. The lesson here is that compliance certification is a necessary but insufficient step and false certifications can have serious adverse consequences. Contractors must convince their own suppliers of the seriousness of their intent to hold them to the standards to which they have committed.

Conclusion

Requirements are in flux. Now is the time to work to understand the concerns of the DoD and other US government customers as well as develop the tools and internal practices that can resolve those concerns without undercutting the strengths of the global supply chain. Bringing those tools and approaches to the attention of the relevant policy makers now, before new requirements are imposed, may shape the development of requirements in ways that protect US security interests and are consistent with a robust market for European defense equipment in the US.

Hogan Lovells is a global firm with deep knowledge of aerospace, defense, and government services companies around the world. The deep bench of lawyers in our Global Regulatory Practice group has unequalled knowledge of the DoD's policies and US concerns. We are superbly postured to guide companies through the challenges and opportunities presented by the US government's focus on supply chain integrity.

Robert Taylor
Senior Counsel | Washington, D.C.
T: +1 202 637 5657
bob.taylor@hoganlovells.com

2. Stringer, D. (2019, May 1). NASA Says Metals Fraud Caused $700 Million Satellite Failure, available here.

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rio de Janeiro
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

*Our associated offices
Legal Services Center: Berlin

www.hoganlovells.com