Brief: Obstacles Posed to Space Firms by ITAR

March 19th, 2021

Findings

Rotoiti interviewed experts in the International Traffic in Arms Regulation (ITAR), a US regulatory regime that affects the transmission of technologies between US and non-US persons. Based on those conversations, this report summarizes obstacles posed by ITAR.

Overview of the International Traffic in Arms Regulation

ITAR is a US regulatory regime that restricts the transmission of military- or defense-related technologies between the US and foreign markets. The regulatory regime stipulates that relevant technologies cannot be traded with non-US persons without authorization from the Department of State. Relevant technologies are primarily listed in the United States Munition List (USML). Civil penalties can include fines of up to $500,000 per violation. Criminal penalties can include fines of up to $1 million and imprisonment of up to ten years, per violation.

ITAR affects many business areas in the space sector. The USML has 21 categories, several of which are pertinent to space. Experts often noted ITAR affects launch services businesses, given their potential military applications – this is true for both "vertical" launch vehicles and "space planes." Additionally, "spacecraft" constitute a USML category (though "commercial" satellites are now controlled by another regulatory regime, the Export Administration Regulations). Other ITAR-subject technologies include subsystems relevant to launch vehicles or spacecraft.

Though often described as controlling "exports," ITAR restricts far more than simply the trade of hardware across borders. ITAR covers trade to non-US persons, trade of physical technologies and associated information, and "reexports" of technologies that have already been traded. An ITAR violation may thus occur in a wide variety of circumstances. For instance, an ITAR violation may occur if a US person sends an email to a non-US person, if that non-US person forwards the email to another non-US person, and if the US person has not acquired authorization from the Department of State for the final recipient to receive the email.

- **"Non-US":** ITAR controls transfer of technologies to non-US persons. US persons include citizens, lawful permanent residents, asylees, and refugees. If a US person sells technology to a non-US person in the United States, therefore, this is subject to ITAR.

- **Information:** ITAR not only covers physical hardware but also associated "technical data." Technical data in the "public domain" is not subject to ITAR (e.g. information contained in news stories or patents available at patent offices). Sending an email about a technology's private details to a non-US person could thus be considered a violation.

- **Reexports:** ITAR oftentimes applies to technologies and associated data that have already been exported. If a piece of technology is sold to a non-US person, in other words, this does not necessarily mean the new owner can share it with anyone they like.

ITAR also affects non-US firms; this includes firms buying from, selling to, or expanding into the United States. For non-US firms buying from the United States, US sellers must apply for authorization to sell them relevant technologies and data. Non-US firms may furthermore be unable to "reexport" their purchases. ITAR also affects non-US firms that sell to the United States. If, for example, a US buyer gives a non-US seller information about certain technologies, this may be subject to ITAR. Foreign firms that expand into the United States may also be affected by ITAR; ITAR regulates interactions between US persons and non-US persons, and expanding into the United States means a firm will likely employ both US and non-US persons.

- If a US firm seeks to buy a piece of hardware for a satellite, for instance, then it will likely need to tell potential sellers of that hardware about the satellite's technical details. If the US firm does not receive authorization to provide such information, then potential non-US sellers of the hardware will face hindrances selling to the US firm.

- If a non-US firm provides a piece of hardware to a US firm, and if the US firm then integrates the hardware into its own project, it may need to correspond with the non-US firm to support such integration. Correspondence will likely entail providing the non-US firm with details about the US firm's project, and may thus be subject to ITAR.

US authorities are especially sensitive to technology transmission to certain countries, and certain export destinations are thus less likely to be approved than others. Some countries are subject to more scrutiny or restrictions than others, whereas other countries are subject to less scrutiny or restrictions. There are more restrictions in place, for instance, for countries with which the United States has adversarial relations, such as China. There are also exemptions that apply to "friendly" countries, including NATO members, Japan, Australia, and New Zealand.

Implications of ITAR for Firms in the Space Sector

Firms in the space sector should consider developing and implementing ITAR compliance plans. Doing so mitigates exposure to ITAR violations. This can be done in-house or with outside support; there is a cottage industry of service providers that audit space firms to test their ITAR compliance. Experts noted that ITAR compliance programs can quickly "snowball" and become costlier than expected. The wide range of commercial transactions that may fall under ITAR means that compliance programs can quickly expand in scope beyond initial planning.

For startups in particular, it is important to signal plans for ITAR; this boosts legitimacy and helps garner investment. A common criticism of space startups is they overly focus on technology at the expense of failing to appreciate business reality. No matter how valuable a technology under development is, it must be sold for a startup to sustain a business around it. If a startup's goal is to sell its technology to US firms or non-US firms connected to the US market (which is often the case in the space sector, given the immensity of the US market), then ultimately startups will need to respond to ITAR. By demonstrating awareness of ITAR and preparedness to respond to it, a startup can improve its reputation among financiers.

If firms violate ITAR, they should proactively report the violation to relevant authorities. Experts repeatedly emphasized that it is important to report violations to authorities rather than be contacted by authorities who become independently aware of violations. It is better to approach authorities with a clear understanding of how the violation happened and an explanation of how the firm's compliance program will be improved to avoid future violations. Such initiative may lead to more leniency in terms of firms incurring penalties for violations.

Because navigating ITAR is costly, some firms tend to avoid certain business areas or partners. The costs of developing and implementing ITAR compliance are significant. The fines, reputational damage, and other consequences associated with ITAR violations are also expensive. As a result, many firms, particularly small ones, may avoid ITAR-connected business.

- **ITAR-connected technologies:** Some firms may avoid ITAR-connected technologies as a way of avoiding the costs associated with compliance programs and consequences for potential violations. This may be done at an early stage before a firm has decided to commit significant resources towards developing a particular type of technology.

- **International business activity:** Firms may avoid interactions between US and non-US persons to avoid ITAR. This may entail not hiring foreign citizens, working only with firms of the same nationality, or using cloud computing that does not "bounce" data to other jurisdictions. Some countries are generally seen as "off-limits" for US firms (experts mentioned China). Non-US firms may similarly opt for "ITAR-free" technologies.

- **Reputationally compromised firms:** If firms know another firm has violated ITAR or is at risk of violating ITAR, they may avoid working with it. Partnering with a reputationally compromised firm is seen as leading to the US government increasing scrutiny on partners; working with a reputationally compromised firm means a partner may be subject to more scrutiny, and more scrutiny implies more associated compliance costs.

Some firms impose blanket security clearance requirements on themselves and partners to ensure ITAR compliance. In the United States, certain security clearances are necessary for working with the government. Some firms prefer to have blanket security clearance requirements, which generally ensure against transfers between US and non-US persons. Security clearance requirements are more restrictive than simply being ITAR-compliant, but it is easier to implement a one-size-fits-all compliance program. This is generally easier for larger firms, since there are significant costs associated with acquiring security clearances.

The sorts of technology subject to ITAR change over time; firms should keep track of these changes to know implications for their business. Commercial satellites, for instance, were formerly under ITAR. They were removed from ITAR in the 1990s, became subject to ITAR again in the 1990s, and were recently put under the Export Administration Regulations (EAR); ITAR technology can now "integrate" into EAR spacecraft. It is generally easier to comply with EAR than with ITAR, according to experts. As jurisdiction over technologies shifts between ITAR and other regimes, this can significantly impact the viability of space firms' business strategies.