Article Information

Authors: Tim O'Callaghan, Travis Shueard
Service: Employment & Labour, Foreign Investment & Trade, Intellectual Property, Intellectual Property Litigation
Sector: Defence

ITAR 101 – Fundamentals and Practice

The International Traffic in Arms Regulations (ITAR) is a US regulatory regime that restricts and controls the export of defence and military related technologies to safeguard US national security and further US foreign policy objectives.

ITAR is a complex regime that is often the source of confusion, particularly for those businesses just beginning to deal with US defence organisations and technology. ITAR is part of the larger Arms Export Control Act of 1976 (US).

Why was ITAR created?

ITAR was borne out of the Cold War in 1976 and created to implement unilateral arms export controls on US defence technology. In short, the US Government has to permit equipment and information being handed over to non-US citizens or companies or governments.

What does ITAR cover?

ITAR covers, broadly, the three categories of "defense articles", "technical data" and "defense services":

1. "Defense articles" are those items described in the US Munitions List (USML), which is also part of ITAR – these items cannot be exported to foreign persons without authorisation from the US Department of State.
2. "Defense services" means furnishing the assistance to foreign persons in the design, development, etc.
3. "Technical data" means classified information relating to Defence articles / defence services.

The USML comprises 20 categories of defense articles, defense services and their associated technical data. These categories cover everything from firearms (Category I) to ballistic missiles (Category IV) to nuclear weapons (Category XVI).

A simple example to explain the different categories:

1. A rifle is a "defense article"
2. Furnishing assistance with the design and development of the rifle is a "defense service"; and
3. The classified information that makes up the design of the rifle is "technical data".

What does ITAR not cover?

Broadly speaking, ITAR does not cover:

1. information in the public domain;
2. certain satellite technology (except in regards to particular proscribed countries); and
3. basic systems descriptions.

There is nuance to these exceptions, given the complexity of ITAR and the breadth of the "defense articles", "defense services" and "technical data" – for example, satellites which serve a military purpose are still covered by ITAR, while some countries are still wholly proscribed from dealing with US satellite technology.

Who is affected by ITAR?

ITAR applies to persons or organisations conducting business with US defence organisations. In essence, US organisations which want to "export" ITAR controlled defence technology to "foreign persons" are generally covered by ITAR.

"**Export**"

The word export is broadly defined and is intended to capture most methods of transfer or transmission. An "export" includes:

1. An actual shipment or transmission out of the United States;
2. transferring registration or ownership of an aircraft, vessel or satellite;
3. releasing technical data or performing a defense service for a foreign person, whether in the US or abroad; and
4. performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad.

This means that even giving information verbally or sending emails to a foreign person can be deemed an "export" under the regulations. Accidental disclosures of this type make up a high proportion of ITAR breaches.

Export of US defence technology is also prohibited to certain countries that the US maintains an arms embargo etc., which adds a further layer of complexity to interpreting these regulations.

"Foreign Persons"

Under ITAR a "foreign person" is any person who is not a lawful permanent resident of the US, which includes foreign corporations, business associations, international organisations and diplomatic missions and consulates. This definition also includes dual and third country nationals.

Any release in the United States of technical data to a foreign person is deemed to be an export to all countries in which the foreign person has held or holds citizenship or holds a permanent residency.

ITAR expects a certain level of discrimination against employees, which is where it becomes difficult. This conduct may fall foul of Australia's anti-discrimination and equal opportunity workplace laws if not handled correctly.

However, most States' legislation allows for exemptions to be granted to a business for ITAR purposes. Piper Alderman's employment team is able to assist with advice on how to seek those exemptions.

Authorisation

In order for a foreign person to be authorised to deal with ITAR technology and information, they must be authorised by and registered with the US Directorate of Defense Trade Controls (DDTC). This can be a lengthy process.

The type of export authorisation granted by the DDTC is dependent upon the category of the ITAR-controlled material, the nature of the export (permanent or temporary) and any national security classifications. The export of "Defense services" (which may also include "technical data" and/or "defense articles") requires a statutorily prescribed agreement (or contract) be entered into, a common form of which is a Technical Assistance Agreement (TAA).

What is a TAA?

A TAA is an agreement for the performance of a defence service or disclosure of technical data and stipulates the information to be disclosed between the parties

A TAA is required to include various statutorily prescribed provisions, including the following which states:

> "This agreement is subject to all United States laws and regulations relating to exports and all administrative acts of the US Government pursuant to such laws and regulations."

Effectively, this means that the foreign party, when signing the TAA, submits to the jurisdiction of the United States when dealing with ITAR covered information and technology. This is an important consideration, as a party is permitting itself to be bound to the laws and regulations of a foreign jurisdiction which it may not be familiar.

Common Breaches

Even if all efforts are made to prevent them, ITAR breaches unfortunately do happen. The most common form of breaches

which happen include:

1. Accidental disclosure (such as email or telephone conversation);
2. Intentional and flagrant violations, where a party intentionally breaches ITAR requirements; or
3. Omitting required information from the application for authorisation or agreement, whether accidentally or by design.

What if you detect a breach?

If you detect a breach, ITAR requires you to self-report within 60 days of detecting the breach. Prompt and fulsome self-reporting can be considered a mitigating factor for any penalties. Likewise, if you do not do so, this can be considered an adverse factor.

Consequences of Non-Compliance

Both civil and criminal penalties can apply to those which violate ITAR. Violations can result in fines and other penalties, such as imprisonment, "blacklisting" from export privileges, mandatory export process reform, etc.

In the case of civil violations, fines can range up to USD$1 million per violation for entities or individuals. In the case of criminal violations, fines can range up to USD$1 million per violation and up to 20 years of imprisonment for wilful violations, for each violation.

Piper Alderman can assist Australian defence organisations with ITAR related matters including:

1. presentations on ITAR
2. reviewing agreements for ITAR compliance; and
3. preparing a checklist for steps to take in the event of a breach of ITAR

For further information, please contact **Tim O'Callaghan**, Partner, on 08 8205 3450 or **Travis Shueard**, Senior Associate, on 08 8205 3433.