General Contract Clauses: Confidentiality (EAR and ITAR)

by Melissa Proctor, Miller Proctor Law PLLC, with Practical Law Commercial Transactions

Maintained • USA (National/Federal)

Related Content

Standard Clauses addressing obligations related to the confidential exchange of technology or technical data subject to the Export Administration Regulations (EAR) and the International Traffic in Arms Regulations (ITAR). These Standard Clauses also include optional indemnification language. These Standard Clauses have integrated notes with important explanations and drafting tips.

READ THIS BEFORE USING DOCUMENT

US Export Laws and Regulations

The US has several export laws and regulations. Two primary sets of export control regulations that address the exchange of information and technology are:

- The Export Administration Regulations (EAR) (15 C.F.R. §§ 730.1 to 774.1) (see Export Administration Regulations).
- The International Traffic in Arms Regulations (ITAR) (22 C.F.R. §§ 120.1 to 130.17) (see International Traffic in Arms Regulations).

The EAR and ITAR prohibit unauthorized exports of technology or technical data related to certain products, deliverables, software, and technology. Those prohibited exports include exchanges of technology and technical information with foreign persons without prior authorization from the Bureau of Industry and Security (BIS) of the US Department of Commerce and the Directorate of Defense Trade Controls (DDTC) of the US Department of State.

For more information on other areas of US export control, see Practice Notes:

- Export Regulations: EAR, ITAR, and FTR: The Foreign Trade Regulations.
- Export Regulation: OFAC Economic and Trade Sanctions.
- Export Regulation: US Antiboycott Laws.

Export Administration Regulations

The EAR control the transfer, export, and reexport of:

- Purely commercial items.
- Items that have dual commercial and military applications (for example, dual-use items).
- Certain munitions items that have been transferred from the ITAR's US Munitions List to the EAR's Commerce Control List because of the recent export control reform effort.

The US Department of Commerce issued the EAR under the authority of the Export Administration Act of 1979 (EAA) (50 U.S.C. §§ 4601 to 4623). Although the EAA lapsed in 2001, the EAR remained in force by virtue of the President's issuance and continuation of Executive Order

13222 under the International Emergency Economic Powers Act (50 U.S.C. §§ 1701 to 1707).

The Export Control Reform Act of 2018 (ECRA), enacted as Title XVII, Subtitle B of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. No. 115-232, 132 Stat. 1636), repealed the EAA, with limited exceptions. ECRA provides permanent statutory authority for the EAR.

For more information about the EAR, see Practice Note, Export Regulations: EAR, ITAR, and FTR: The Export Administration Regulations.

International Traffic in Arms Regulations

The ITAR control the export, reexport, temporary import, and brokering of defense articles and defense services. The ITAR were implemented under the authority of the Arms Export Control Act (22 U.S.C. §§ 2778 to 2780).

For more information about the ITAR, see Practice Note, Export Regulations: EAR, ITAR, and FTR: The International Traffic in Arms Regulations.

Requirements for Companies

The EAR and ITAR require that companies:

- Determine when either set of regulations applies to:
  - their products;
  - their technology or software; or
  - information or technical data that they generate or receive that is related to their products, technology, or software.
- Determine when license requirements are triggered and properly utilize license exceptions or exemptions for exports, if applicable.
- Obtain required disclosure authorizations from BIS or DDTC when no license exceptions or exemptions apply.
- Safeguard certain technical data, software, and technology from unauthorized access or release to foreign persons (see Exports Under the EAR and ITAR).

For more information on these and other EAR and ITAR requirements, see Practice Note, Core Elements of an Export Compliance Program and Complying with US Export Control Regulations Checklist.

Exports Under the EAR and ITAR

The EAR and ITAR restrict companies from making certain exports without prior authorization from BIS or DDTC. Under the EAR, these transfers are referred to as deemed exports, which are releases or transfers of technology or source code to a foreign person in the US. Those releases and transfers are deemed exports to the foreign person's most recent country of citizenship or permanent residency. Under the ITAR, these transfers are treated as exports. The EAR and ITAR have similar approaches to describing:

- When technology, software, and technical data are subject to export controls.
- What activities constitute an export or reexport.

For more information on key terms in the EAR and ITAR, see Practice Note, Export Regulations: EAR, ITAR, and FTR: Scope of the EAR and Important Definitions and Important Definitions Under the ITAR and Standard Document, Procedures for Handling of ITAR-Controlled Technical Data: Drafting Notes: Technical Data.

Civil and Criminal Penalties for Export Violations

The EAR imposes civil penalties for violations. The maximum civil penalty under the Export Control Reform Act of 2018 is the greater of $300,000 or twice the value of the underlying transaction, per violation.

Civil penalties for violations of the ITAR can be a maximum of $1,163,217 per violation.

Criminal penalties for willful violations of the EAR and ITAR consist of either or both:

- Fines of up to $1 million per violation.
- Imprisonment for up to 20 years.

For more information on export control penalties generally, see Practice Note, Export Regulation: OFAC Economic and Trade Sanctions: Penalties for Violations. For a discussion of potential individual liability under the EAR and ITAR, see Practice Note, Core Elements of an Export Compliance Program: Personal Liability for Violations of the US Export Laws and Regulations.

Scope of Standard Clauses

These Standard Clauses are contract provisions designed for confidentiality agreements. These provisions can also be used in other agreements involving disclosures of confidential information subject to the EAR and ITAR, such as:

- Services agreements.
- Outsourcing agreements.
- Consulting agreements.
- Custom manufacturing agreements.

The disclosing party can include these provisions to help manage the risk of violating the ITAR and EAR by:

- Providing notice to recipients that the disclosed information may be subject to the EAR and ITAR.
- Obligating the recipient to comply with the EAR and ITAR.
- Requiring consent before the recipient:
  - shares confidential information with third parties; or
  - subcontracts out work that arises from the disclosure of confidential information.

For more information on confidentiality provisions and the protection of confidential information generally, see Confidentiality and Nondisclosure Agreements Toolkit. For a contract provision that addresses export compliance risk in sales agreements with customers, see Standard Clause, General Contract Clauses: Export Regulation (EAR and ITAR). For contract provisions specific to US economic and trade sanctions and antiboycott requirements, see Standard Clauses, General Contract Clauses: Export Regulation (OFAC General Requirements) and General Contract Clauses: Export Regulation (US Antiboycott Law).

Assumptions

These Standard Clauses assume that:

- **There are only two parties to the agreement.** The parties should adjust the provisions as necessary if additional parties, such as the customer's affiliates, also have rights or obligations under an agreement.
- **The parties to the agreement are US entities and the transaction takes place in the US.** If any party is organized or operates in, or any part of the transaction takes place in a foreign jurisdiction, these terms may need to be modified to comply with applicable laws in the relevant foreign jurisdiction.
- **These terms are being used in a business-to-business transaction.** These Standard Clauses may not be suitable for a consumer contract or a government contract, which may involve legal and regulatory requirements and practical considerations that are beyond the scope of this resource.
- **These terms are not industry-specific.** These Standard Clauses do not account for any industry-specific laws, rules, or regulations (other than the EAR and ITAR) that may apply to certain transactions, products, or services.
- **Capitalized terms are referenced elsewhere in the agreement.** Certain terms are capitalized but not defined in these Standard Clauses because they should be defined elsewhere in the agreement (for example, Agreement, Confidential Information, Discloser, and Recipient).

Bracketed Items

Bracketed items in sentence case are either optional provisions or include alternative language choices to be selected, added, or deleted at the drafter's discretion.

General Contract Clauses: Confidentiality (EAR and ITAR)

1. Export Regulation. Recipient agrees that certain of Discloser's Confidential Information may be subject to US export control laws and regulations implemented in the Export Administration Regulations ("**EAR**") and the International Traffic in Arms Regulations ("**ITAR**"). Recipient agrees:

1.1 not to violate any laws or regulations implemented in the EAR and the ITAR[./;] [and]

EXPORT REGULATION

In Sections 1 and 1.1, the recipient:

- Acknowledges that the confidential agreement may be subject to the EAR and ITAR.
- Agrees not to violate the EAR and ITAR or their authorizing legislation.

By including those sections, the disclosing party imposes a contractual obligation that helps safeguard the information. The disclosing party should consider taking additional precautions before making the actual release or transfer (see, for example, Standard Document, Procedures for Handling of ITAR-Controlled Technical Data: Drafting Note: Labeling and Marking).

An export violation by one party can have consequences for the broader network of companies involved in a project (for example, a DDTC investigation of the supply chain). Optional Sections 1.2 to 1.4 give the disclosing party greater control and influence over how the recipient conducts its business and handles the information. However, the disclosing party should assess whether the rights are necessary and practical in each circumstance. The recipient may also object to:

- The additional administrative burden.
- The disclosing party's interference with its regular business operations.

1.2 [to register with the Directorate of Defense Trade Controls[, as required by the ITAR][./;] [and]]

DDTC REGISTRATION

The ITAR require that all persons or entities that engage in the manufacture, export, and brokering of defense articles and services register with DDTC (22 C.F.R. § 122.1). The failure to register is a violation covered by Section 1.1, but the disclosing party can also include Section 1.2 to:

- Notify the recipient of the registration requirement and reduce the risk of a violation.
- Demonstrate its own diligence efforts for ITAR compliance.

The disclosing party can use the optional language when the confidentiality agreement covers a series of exchanges, and the parties do not know whether:

- ITAR-controlled technical data will be shared.
- The recipient will be required to register with DDTC.

1.3 [not to, without limitation, disclose, transfer, or export Discloser's Confidential Information to third parties, including foreign persons or entities, whether or not related to or affiliated with Recipient, without first receiving express written consent from Discloser and as required by contract or by law[./;] [and]]

CONSENT FOR FURTHER DISCLOSURES

Confidentiality agreements usually prohibit disclosure of confidential information to third parties. Recipients often want to include an exception to the general nondisclosure obligations to address disclosures to specified employees, representatives, or affiliates made to

evaluate information (see Practice Note, Confidentiality and Nondisclosure Agreements: Nondisclosure Obligations). Disclosing parties often agree to those disclosures if the recipient must:

- Inform the representatives of the confidential nature of the information.
- Ensure that the representatives are subject to confidentiality duties that are no less restrictive than those included in the confidentiality agreement.

Section 1.3 prohibits the recipient from disclosing further confidential information to third parties, including foreign persons or entities, without the disclosing party's written consent.

A recipient's disclosure to a foreign person may require a license or other prior authorization from BIS or DDTC (see Practice Note, Export Regulations: EAR, ITAR, and FTR: Scope of the EAR and Important Definitions and Important Definitions Under the ITAR). Section 1.3 is designed to reduce the risk of an export without required prior authorization from BIS or DDTC. The disclosing party should consider whether it is beneficial to require written consent and assume the burden of reviewing proposed disclosures. For example, there may not be much additional value if the recipient:

- Is highly experienced in the handling of controlled technology or data.
- Has agreed to Section 2.

1.4 [not to subcontract out any work or orders arising from this Agreement, without first receiving express written consent from the disclosing party and as required by contract or by law.]

CONSENT TO SUBCONTRACTS

Section 1.4 explicitly prohibits subcontracting out work that arises from disclosures covered by the confidentiality agreement. Many subcontracting provisions start with a general prohibition and include certain negotiated exceptions.

By including an explicit prohibition on subcontracting, the disclosing party:

- Ensures that the party with whom it contracted, rather than a third party, performs.
- Has a claim for breach if the party with whom it contracted subcontracts out its obligations.

As with Section 1.3, this provision also helps reduce the risk of an export without required prior authorization from BIS or DDTC. The disclosing party should consider whether it is beneficial to require written consent and assume the burden of reviewing potential subcontracts. For example, there may not be much additional value if the recipient:

- Is highly experienced in the handling of controlled technology or data.
- Subcontracts out this type of work frequently.
- Has agreed to Section 2.

For sample clauses prohibiting subcontracting, see Standard Clause, General Contract Clauses: Subcontracting.

2. Indemnification. [If Recipient does not comply with its obligations under this Section 1 or any terms specified in the Agreement, Recipient will indemnify, defend, and hold harmless, Discloser as to any violations that Recipient may cause under the EAR and ITAR, including but not limited to the payment of civil and criminal penalties, all costs and expenses, and attorneys' fees.]

INDEMNIFICATION

If the confidentiality agreement or commercial agreement includes an indemnification clause, the disclosing party should:

- Ensure that it covers any breach of this provision by the recipient. For an example of an indemnification clause in a confidentiality agreement, see Standard Document, Confidentiality Agreement: General (Short Form, Unilateral, Pro-Discloser): Section 10.

- Carefully consider whether this type of breach should be subject to any liability cap, given the significant costs that a seller may incur for any violation (see Drafting Note, Civil and Criminal Penalties for Export Violations).

If the confidentiality agreement or commercial agreement does not include an indemnification clause or the clause does not adequately address this issue, the disclosing party can include Section 2. The disclosing party should also ensure that this provision survives the termination or expiration of the confidentiality agreement or commercial agreement.

For a general discussion of indemnification, see Practice Note, Indemnification Clauses in Commercial Contracts.

PRODUCTS

PLC US Commercial Transactions, PLC US Intellectual Property and Technology, PLC US Law Department