



What is ITAR?

Simplifying compliance using the end-to-end encryption carveout

INTERNATIONAL TRAFFIC IN ARMS REGULATIONS (aka ITAR) are designed to control the export of US defense and military products. Administered by the US State Department, ITAR's purpose is to safeguard US national security and advance US foreign policy objectives.

ITAR standards implement the Arms Export Control Act (AECA) and are administered by the US State Department. The Department of Defense (DoD), of course, has a strong interest in regulating military products as well, and so DoD works closely with the State Department on ITAR-related matters. Organizations doing work for DoD need to know about ITAR.

This brief explains the ITAR regulations and what they encompass, which is far more than what “Arms” in “ITAR” implies. It also offers guidance to help your organization achieve ITAR compliance. The security risks associated with improper export of US military products and the steep fines and serious business risks of violating ITAR, even if inadvertently, mean that compliance needs to be a high priority. We also explain an ITAR regulation released in 2020—the so-called “end-to-end encryption carveout”—that your organization can leverage to simplify ITAR compliance using tools like PreVeil.

ITAR applies more broadly than you may think

ITAR governs the export of a wide array of military products and services on the **United States Munitions List** (USML). Note that while many of the items on the list are clearly arms—such as guns, rockets and bombs—the list wraps up with a catch-all category, “Articles, Technical Data, and Defense Services Not Otherwise Enumerated”. Clearly, the list of articles subject to ITAR is comprehensive—and, notably, it includes technical data and defense services such as installation, repair, training and consulting related to items on the USML as well.

The USML is organized into 21 major categories of military products, running the gamut from Guns and Armament and Personal Protective Equipment, for example, to Spacecraft and Nuclear Weapons. The full USML list of categories is provided in Appendix A, and the Code of Federal Regulations (CFR) definitions of “technical data” and “defense services” subject to ITAR are provided in Appendix B.

Note that ITAR applies beyond what most would think of as “exports.” For example, if a foreign person¹ is employed in the United States at a lab working to produce an item on the USML list, and relevant technical data (e.g., blueprints) are shared with that person, that’s considered an export because the data was shared with a non-US person. If that happens without prior authorization per ITAR, it’s considered a violation even though the activity occurred on US soil. And if a US person² receives ITAR-controlled technical data while in a foreign country, that is also considered an export and so the exchange would need to either have prior authorization or meet the criteria for an exception if the data is end-to-end encrypted, as explained below.

ITAR: Mandatory registration with the State Department

Any US person engaged in the United States in the business of the manufacturing, exporting or brokering of US defense articles, furnishing defense services, or handling technical data related to items on the USML is required to register with the State Department’s [Directorate of Defense Trade Controls](#) (DDTC). Further, any US person or foreign person subject to the jurisdiction of the United States who engages in brokering activities with respect to US or foreign defense articles or services must also register.

If you are uncertain about whether the work your organization is doing is governed by ITAR, check with your in-house compliance officer if you have one, and carefully read your contract. If you’re still not certain if your work is subject to ITAR, check with your DoD (or other agency’s) contracting officer or the contractor above you in your supply chain.

Assuming your organization’s work is subject to ITAR regulations, your first step is to register with the DDTC. Registration needs to be renewed annually.

-
- 1 Per [22 CFR 120.63](#), “foreign person” means any natural person who is not a lawful permanent resident as defined by [8 U.S.C. 1101\(a\)\(20\)](#) or who is not a protected individual as defined by [8 U.S.C. 1324b\(a\)\(3\)](#). It also means any foreign corporation, business association, partnership, trust, society, or any other entity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments, and any agency or subdivision of foreign governments (e.g., diplomatic missions).
 - 2 Per [22 CFR 120.62](#), “US person” means a person who is a lawful permanent resident as defined by [8 U.S.C. 1101\(a\)\(20\)](#) or who is a protected individual as defined by [8 U.S.C. 1324b\(a\)\(3\)](#). It also means any corporation, business association, partnership, society, trust, or any other entity, organization, or group that is incorporated to do business in the United States. It also includes any governmental (Federal, state, or local) entity. It does not include any foreign person as defined in [§ 120.63](#).

SERIOUS PENALTIES FOR ITAR VIOLATIONS

Penalties for ITAR violations include civil fines of up to \$500,000, criminal fines of up to \$1,000,000, and imprisonment up to 10 years per violation. Penalties may apply to individuals as well as organizations. Examples of ITAR penalties abound, as the State Department has substantially increased its ITAR enforcement efforts over the past two decades.

In 2020, Airbus reached an agreement to settle the largest corruption enforcement action in history by agreeing to pay nearly \$4 billion in penalties for bribes aimed at winning large aircraft contracts, which compromised the US defense industry (among others). The ITAR-related violations of the settlement totaled \$233 million. Major defense contractors also penalized for ITAR breaches include Lockheed Martin, Boeing, and Northrup Grumman, among others.

But enforcement is not confined to just prime contractors. In 2022, for example, the State Department banned 10 people from future ITAR-related activities for conspiring to violate ITAR regulations. At US universities, professors have been prosecuted for breaching ITAR regulations by sharing ITAR technical data without prior authorization as required. And in an important signal to small to mid-size businesses in the Defense Industrial Base, in 2017, Bright Lights USA, a manufacturer of basic spare parts for the DoD (e.g., rubber stoppers and grommets) with approximately 100 employees was penalized with a civil fine of \$400,000 for ITAR violations.

ITAR: Prior authorization is the key

After registration with DDTC, your next step is to identify all the ITAR-controlled defense articles, defense services, and related technical data that your organization handles. Once you've identified those items, you'll need to obtain prior authorization for any related transactions you wish to engage in. Prior authorization is your only possible course of action; there is no after-the-fact approval.

Pursue one of the following two avenues to receive prior authorization:

- Review the **exemptions** to ITAR, which are clearly delineated in the rules. If the transaction your organization wishes to engage in meets the conditions for an exemption, then you can consider the transaction to have prior authorization and may proceed.
- If your organization doesn't qualify for an exemption, you will need to file a request for authorization (which often comes in the form of an export license) for the transaction you wish to make. If DDTC grants the request or license, that serves as your prior authorization.

Any exports that occur in the absence of prior authorization are violations of ITAR, are illegal, and are subject to penalties, including substantial fines and jail time.

DDTC strongly advises organizations engaged in the defense trade to establish and maintain an ITAR compliance program, and has issued [guidelines](#) to help them do so. Clearly, it's in your organization's best interests to establish policies and procedures to track the ITAR-controlled items—defense articles, defense services, and related technical data—that you work with at all times.

ITAR AND CUI OVERLAP

Not all ITAR is CUI (Controlled Unclassified Information), and not all CUI is ITAR. CUI can only be created under a contract to the federal government, whereas ITAR data can be created by a company without any contract. That said, many organizations that handle ITAR data also handle CUI. And organizations that handle CUI could find themselves subject to ITAR due to contract changes or modifications in the USML.

In addition to ITAR regulations, organizations handling ITAR data and CUI should be familiar with two DFARS clauses:

- For CUI, there's [DFARS 252.204-7012](#). It focuses on the safeguarding of defense information and cyber incident reporting.
- For ITAR data, there's [DFARS 252.225-7048](#). It focuses on the safeguarding of information in international collaborations (and refers defense contractors to both ITAR and AECA regulations).

ITAR carveout: Exception when using end-to-end encryption

In 2020, the State Department simplified compliance with ITAR with the release of [22 CFR 120.54](#), which stipulates exceptions to ITAR regulations when technical data is shared using end-to-end encryption.

With this exception—or carveout, as it's commonly known—the State Department recognized that advances in cybersecurity could be leveraged without compromising national security goals. Prior to the end-to-end encryption carveout, organizations subject to ITAR had to use specialized and expensive on-premise servers and software that is difficult to deploy, maintain and administer. The carveout enables them to leverage the cloud and streamline their ITAR data handling practices. Transactions that meet the carveout's criteria are not considered exports and so do not need an export license.

Specifically, ITAR's end-to-end encryption carveout allows organizations to send, receive or store technical data without an export license provided they meet the following criteria:

- The data is unclassified;
- The data is secured using end-to-end encryption;
- The cryptographic modules used for end-to-end encryption are compliant with **FIPS 140-2** or its successors;
- The data is not unencrypted at any point between the originator and the recipient;
- The means of decryption are not provided to any cloud service provider or other third party, i.e., no person or organization other than the recipient has access to keys, network access codes, or passwords that enable decryption;
- The recipient is a US person, or a person authorized to receive the unclassified technical data per ITAR;
- The data is not purposely sent to or stored in **restricted countries** specified by ITAR (e.g, Russia, China, North Korea, and many others); and
- The data is not purposely sent from restricted countries specified by ITAR.

The carveout also makes it easier to comply with ITAR when employees access ITAR data while in foreign countries. Previously, organizations had to apply for licenses for their employees to access ITAR data while abroad. The carveout frees them of the burden of that compliance overhead, making it easier for their employees operating overseas to do their job.


PreVeil Drive and Email meet the ITAR carveout standards

PreVeil understands the challenges that small to mid-size contractors must overcome to comply with ITAR. Its platform is easy to use and cost effective for organizations with limited cybersecurity expertise and compliance resources. PreVeil meets each of the technical components of the ITAR carveout:

- PreVeil Drive and Email are grounded in world-class end-to-end encryption that meets FIPS 140-2 standards.
- With PreVeil, files, emails and data are only ever encrypted and decrypted on a user's device. Information is never decrypted on any server anywhere. If attackers breach a server, all they will get is useless gibberish.³


³ PreVeil also captures every file sharing and email transaction that contains ITAR data in immutable logs, which support ITAR compliance per DDTC guidelines.

- PreVeil has no access to keys, network access codes, or passwords that enable decryption. Private keys are stored only on user devices, assuring that no one other than the sender and intended recipients can ever access your sensitive data—not even PreVeil.


PreVeil Drive  enables ITAR-compliant end-to-end encrypted file sharing and data storage. Users can access files stored on PreVeil Drive from any of their devices, or share files with other users who have the appropriate access permissions through PreVeil's Trusted Communities.


PreVeil Drive is easy to use and functions like Dropbox, Google Drive or OneDrive. But unlike those alternatives, which allow the server to access your decrypted data, with PreVeil Drive only you and the people with whom you've explicitly shared files can decrypt them. PreVeil servers store only encrypted data and have no ability to access keys to decrypt it.

PreVeil Drive automatically integrates with Windows File Explorer and Mac Finder and has no impact on your existing file servers. It's available for Windows, Mac and, with PreVeil's mobile app, for smartphones, iPads and tablets.

PreVeil Email  lets your employees send and receive encrypted emails containing ITAR-controlled technical data using their existing email address. It integrates seamlessly with Outlook and Gmail and works on browsers and mobile devices. The installation process automatically creates a new set of mailboxes for your encrypted messages. Messages in these new mailboxes are end-to-end encrypted. There are no changes to the mailboxes already in your mail program and no impact on the servers that store your regular, unsecure messages.

PreVeil security features include, among others:

Advanced key management  PreVeil's key management system meets ITAR standards by eliminating key servers and the central points of attack they present. PreVeil enables sharing, storage and revocation of encrypted data from user devices while hiding the complexities of key management, because the process occurs automatically. On the other hand, some encryption systems centralize the storage of decryption keys in a key server. Doing so undermines the benefits of encryption because attackers can focus their efforts on penetrating the key server, which if successful would ultimately compromise all of the encrypted data. That's why the ITAR carveout specifies that companies will be held liable if "access information"—such as decryption keys, network access codes, and passwords—is used by unauthorized persons to gain access to unencrypted technical data. PreVeil eliminates that possibility.

Elimination of passwords  PreVeil also eliminates passwords, another common point of vulnerability. Instead of relying on passwords, PreVeil authenticates users via strong cryptographic keys that are automatically created and stored on users' devices. Replacing passwords with cryptographic keys shuts down the many significant security risks that flow from phishing and password-guessing attacks, including the use of compromised passwords for unauthorized access and malicious activity. And again, because the keys are stored on user's devices, hackers cannot remotely log into user accounts.

In closing

If your organization handles ITAR-controlled technical data—or CUI that contract changes or modifications to the USML could make subject to ITAR—then you need to be aware of ITAR standards. Fortunately, the end-to-end encryption carveout simplifies ITAR compliance. PreVeil's secure platform offers a straightforward solution to take advantage of that carveout.

Moreover, PreVeil is easy to deploy and use, and is cost effective:



Easy to deploy

PreVeil Drive and Email deploy in a matter of hours, as a complementary system with no impact on existing file and email servers—making configuration and deployment simple and fast. Because it deploys so easily alongside your existing systems, PreVeil can save months of business disruption and expense.



Easy to use

PreVeil is easy for end users to adopt because it works with the tools they already use. File sharing works like DropBox and is integrated with the Windows File Explorer and Mac Finder. Email can be integrated with Outlook, Gmail, or Apple Mail clients. Users keep their regular email address, which keeps it simple.



Cost effective

PreVeil's file sharing and email platform is a fraction of the cost of alternatives. Moreover, PreVeil needs to be deployed only to users handling ITAR data, whereas alternatives often require deployment across an entire organization. And because PreVeil does not impact existing file and email servers, configuration and deployment are simple and inexpensive.

To learn more, sign up [here](#) for a free 15-minute consultation with our compliance team to answer your specific questions about ITAR.

Appendix A

United States Munitions List (USML)–Major categories excerpted

CFR 121 The United States Munitions List

- Firearms, Close Assault Weapons and Combat Shotguns
- Guns and Armament
- Ammunition/Ordnance
- Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs, and Mines
- Explosives and Energetic Materials, Propellants, Incendiary Agents, and Their Constituents
- Surface Vessels of War and Special Naval Equipment
- Ground Vehicles
- Aircraft and Related Articles
- Military Training Equipment and Training
- Personal Protective Equipment
- Military Electronics
- Fire Control, Range Finder, Optical and Guidance and Control Equipment, Night vision goggles
- Materials and Miscellaneous Articles
- Toxicological Agents, Including Chemical Agents, Biological Agents, and Associated Equipment
- Spacecraft and Related Articles
- Nuclear Weapons Related Articles
- Classified Articles, Technical Data, and Defense Services Not Otherwise Enumerated
- Directed Energy Weapons
- Gas Turbine Engines and Associated Equipment
- Submersible Vessels and Related Articles
- Articles, Technical Data, and Defense Services Not Otherwise Enumerated

Appendix B

ITAR definitions of technical data and defense services

CFR 120.33 Technical data

(a) **Technical data** means for purposes of this subchapter [i.e., ITAR]:

- (1) Information, other than software as defined in § 120.40(g), which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions, or documentation;
- (2) Classified information relating to defense articles and defense services on the U.S. Munitions List and 600-series items controlled by the Commerce Control List;
- (3) Information covered by an invention secrecy order; or
- (4) Software (see § 120.40(g)) directly related to defense articles.

(b) The definition in paragraph (a) of this section does not include information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities, or information in the public domain as defined in § 120.34 or telemetry data as defined in note 3 to Category XV(f) of § 121.1 of this subchapter. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles.

CFR 120.32 Defense service

(a) **Defense service** means:

- (1) The furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing, or use of defense articles;
- (2) The furnishing to foreign persons of any technical data controlled under this subchapter, whether in the United States or abroad; or
- (3) Military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice.

About PreVeil

PreVeil makes military-grade security accessible to everyone. Its encrypted Drive and Email platform helps organizations improve their cybersecurity, reduce their compliance burdens, and achieve ITAR compliance and CMMC Level 2 certification. PreVeil Drive works like DropBox for file sharing and collaboration, but with far better security. PreVeil Email works with existing apps like Outlook or Gmail, letting users keep their regular email addresses. Because it works with your existing tools, PreVeil is easy to implement and use. All documents and messages are automatically encrypted end-to-end, which eliminates central points of attack and means that no one other than intended recipients can read or scan your sensitive information—not even PreVeil.

More than 750 companies in the Defense Industrial Base trust PreVeil for their cybersecurity needs. Visit www.preveil.com to learn more.

Additional copies of this paper can be downloaded at preveil.com/itar-whitepaper.