# Procedures for Handling of ITAR-Controlled Technical Data

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

Maintained • USA (National/Federal)

Related Content

*A sample set of compliance procedures that a company can use for the transfer of technical data controlled under the International Traffic in Arms Regulations (ITAR). These procedures assume that the company participates in the manufacture, export, or sale of defense articles, has registered with the Directorate of Defense Trade Controls (DDTC) of the US Department of State, and employs both US and foreign persons. The procedures address physical, electronic, and verbal transfers of technical data both within the company and to other parties with the purpose of avoiding exports to foreign persons that violate the ITAR. This Standard Document has integrated notes with important explanations and drafting tips.*

## READ THIS BEFORE USING DOCUMENT

The International Traffic in Arms Regulations (ITAR) (22 C.F.R. §§ 120.1 to 130.17) are administered by the Directorate of Defense Trade Controls (DDTC) of the US Department of State (State Department). The ITAR controls the export, reexport, temporary import, and brokering of defense articles and defense services. The ITAR has requirements for licenses or other authorizations for transfers of defense articles and services. Companies generally must submit a license request before exporting any item that is included on the US Munitions List (USML) unless a specific license exemption applies. For a general discussion of the ITAR, the USML, and ITAR requirements, see Practice Note, Export Regulations: EAR, ITAR, and FTR: The International Traffic in Arms Regulations and Complying with US Export Control Regulations Checklist.

A company must register with DDTC and implement formal compliance policies and procedures if it:

- Determines that its goods, software, or technical data are subject to the ITAR.
- Exports, reexports, or temporarily imports defense articles.
- Provides defense services.
- Engages in brokering of defense articles.

Common violations of the ITAR occur as a result of:

- Sharing ITAR-controlled defense articles or technical data with a foreign person (whether in the US or abroad) without the required authorization.
- Exceeding the scope, terms, and conditions of an authorization.

In many cases, these violations occur because of a failure to implement and document effective compliance policies and procedures. DDTC publishes compliance program guidelines that outline the framework for an effective compliance program. Those guidelines include a methodology for identifying and tracking ITAR-controlled technical data handled by the company.

This Standard Document includes draft procedures that address common issues that arise when handling ITAR-controlled technical data. The basic concepts apply broadly but the procedures must be tailored to address the structure and needs of an organization.

To implement these procedures effectively, a company should establish a broader export compliance program that:

- Describes management commitment to export compliance.
- Implements an organizational structure that addresses all of the company's export activities.

Additional procedures may include:

- Physical security and facility access.
- Visitor screening and meeting processes.
- Restricted party screening.
- Embargoed and sanctioned country screening.
- Compliance with licensing, reporting, and recordkeeping requirements.

For a broad discussion of compliance with various US export laws, see Practice Note, Core Elements of an Export Compliance Program and Standard Document, Statement of US Export and Trade Compliance Policy.

ITAR-specific programs should include training on basic concepts, including:

- The definition of technical data.
- The activities that constitute an export.
- Persons that are foreign persons under the ITAR.

(See Drafting Notes, Important ITAR Definitions and Foreign Persons.)

### Consequences of Non-Compliance

A company's failure to comply with ITAR requirements can lead to civil and criminal penalties (see Civil and Criminal Penalties for ITAR Violations). Companies may also be debarred from contracting with the federal government and regulators may suspend a company's export privileges for periods of days to years depending on the severity of the violations. Companies that have committed export violations typically experience:

- Increased government scrutiny of their activities and license applications.
- Challenges contracting with other companies that work in the defense industry or contract with the US government.
- Negative publicity in press reports or agency press releases.

### Civil and Criminal Penalties for ITAR Violations

Civil penalties for violations of the ITAR can be a maximum of $1,163,217 per violation (22 C.F.R. § 127.10). Criminal penalties for willful violations of the ITAR consist of either or both:

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

The ITAR establishes criminal liability for persons engaging in prohibited conduct or failing to register or obtain a license or other authorization as required by the regulations or authorizing legislation (22 C.F.R. § 127.1).

The ITAR provides that:

- Persons that are granted a license or approval or are operating within an exemption are responsible for the acts of:
  - employees;
  - agents;
  - brokers; and
  - persons having possession of the items (22 C.F.R. § 127.1(c)).

- No person may knowingly or willfully, among other things, attempt, cause, induce, or permit acts prohibited the ITAR or the Arms Export Control Act (AECA) (22 C.F.R. § 127.1(e)).

### Assumptions

This procedure assumes that:

- It is part of a broader export compliance program and statement of policy that describes the company's commitment to export compliance (see Practice Note, Core Elements of an Export Compliance Program and Standard Document, Statement of US Export and Trade Compliance Policy).
- The company is either or both a manufacturer or exporter of defense articles and is handling items or technical data subject to ITAR control and has registered with DDTC as required (see 22 C.F.R. § 122.1 and Drafting Note, ITAR-Controlled Efforts).
- The company has employees falling within the definition of foreign persons (see Drafting Note, Foreign Persons).
- The company is not engaged in defense services or brokering activities, which may be subject to additional requirements (see 22 C.F.R. §§ 124.1 to 124.16 and §§ 129.1 to 129.11).
- The company intends to develop other plans and procedures that address the handling of ITAR-controlled data for specific projects, such as:
  - technology control plans;
  - technology transfer control plans (where warranted);
  - data categorization guidelines; and
  - other procedures, such as ITAR Physical and IT Security Procedures.

  See Drafting Notes, Technology Transfer Control Plan and Data Categorization Guidelines.

### Bracketed Items

Bracketed items in ALL CAPS should be completed with the facts relevant to the organization. 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.

## PROCEDURE FOR TRANSFERS OF ITAR-CONTROLLED TECHNICAL DATA

**Purpose**

[COMPANY NAME] ("**Company**") recognizes that certain of its business operations handle defense articles and technical data subject to the International Traffic in Arms Regulations (ITAR) (22 C.F.R. §§ 120.1 to 130.17). Under the ITAR, transferring technical data electronically, verbally, or physically to a foreign person is considered to be an export to the home country of the foreign person and requires export authorization prior to doing so. The purpose of this procedure is to provide personnel with specific direction to compliantly transfer such technical data:

- Electronically, verbally, and physically.
- Within and outside of the Company.

The Company employs both US and foreign persons. As such, Company employees must take reasonable steps to protect ITAR-Controlled technical data, even while this data is being transferred internally, so that the data is not inadvertently exposed to the Company's foreign person employees or external foreign person recipients for which export authorization has not been obtained.

## PURPOSE

This section briefly conveys the scope of the ITAR's application and uses terms defined in the ITAR. It notes that certain ITAR controls must be implemented. The company must:

- Obtain prior authorization from DDTC or identify an applicable license exemption before exporting to a foreign person.
- Implement processes to prevent foreign persons from accessing ITAR-controlled technical data.

The bulleted items emphasize that these requirements apply both internally and externally and to various types of transfers.

### Important ITAR Definitions

The ITAR's broad definitions of **technical data, export,** and **release** create the risk of unintended exports, especially technical data transfers. To ensure effective compliance, companies should train employees on certain terms defined in the ITAR.

Employees need to understand which details are subject to restriction and when they need to take precautions before they share information (see Technical Data). Employees may not appreciate these risks unless given examples of potential violations. The company should identify the organizational functions that require training and how issues may arise for different types of employees. For example:

- **Marketing and sales discussions**. Staff may want to share information about current or past work with prospective customers. This may include basic system descriptions or a product's basic functions, which are generally permissible. However, the company may need to seek prior authorization from DDTC for more detailed discussions.
- **R&D and manufacturing communications**. Research and development engineers or manufacturing operations staff may wish to subcontract certain work or request help from colleagues within the company. The employee must be diligent and take precautions to safeguard that information before sharing items, such as:
  - product plans;
  - drawings; or
  - other manufacturing or design know-how.

  See Drafting Notes, Know the Recipient and Non-Disclosure Agreements.

#### Technical Data

The ITAR defines **technical data** broadly to include:

- Information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles. This includes:
  - blueprints;
  - drawings;
  - photographs;
  - plans;
  - instructions; or
  - records.
- Classified information relating to defense articles and defense services on the USML and 600-series items controlled by the Commerce Control List (for more information on the Commerce Control List, see Practice Note, Export Regulations: EAR, ITAR, and FTR: The Export Administration Regulations).
- Information covered by an invention secrecy order.
- Software directly related to defense articles.

Notably, technical data **does not** include:

- Basic marketing information on function or purpose or general system descriptions of defense articles.
- General scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities.
- Certain telemetry data and other information in the public domain, as further described in the ITAR.

(22 C.F.R. § 120.10.)

#### Export and Release

The ITAR's broad definition of export and release raises the risk of unintended exports or deemed exports. As a result, a US firm with foreign affiliates or personnel must take precautions to limit access to ITAR-controlled technology to both:

- US persons.
- Foreign persons licensed to receive access under the terms and the time periods specified by DDTC.

The ITAR definition of **export** includes:

- An actual shipment or transmission out of the US.
- A release or transfer of technical data to a foreign person in the US or abroad.

(22 C.F.R. § 120.17.)

The ITAR defines **release** as either:

- Visual or other inspection by foreign persons of a defense article that reveals technical data to a foreign person.
- Oral or written exchanges with foreign persons of technical data in the US or abroad.

(22 C.F.R. § 120.50.)

### Foreign Persons

Companies that handle ITAR-controlled technical data must consider potential transfers or releases to:

- Their foreign employees or contractors, including:
  - full-time employees;
  - part-time employees;
  - temporary employees;
  - interns; and
  - contingent workers.
- Employees or contractors of their foreign affiliates.
- Foreign recipients at firms with which they do business.

The ITAR defines foreign person to include:

- A natural person that is not a US citizen, US permanent resident, or a protected individual (for example, asylum seekers or refugees).
- A foreign entity not organized to do business in the US.

(22 C.F.R. § 120.16.)

Any release in the US 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 permanent residency (22 C.F.R. § 120.17(b)). US persons employed by a foreign entity must be treated as a foreign person. However, US persons employed by a US subsidiary of a foreign entity can be treated as a US person.

#### Internal Considerations

ITAR-mandated controls create challenges for US companies with foreign employees. Companies need to:

- Consider ITAR-requirements when:
  - soliciting work;
  - making hiring decisions; and
  - staffing projects.

- Remain mindful that they cannot discriminate based on immigration status (for more information on the laws prohibiting discrimination based on immigration status, see Practice Note, Discrimination: Overview: IRCA).

For example, if a company is going to handle ITAR-controlled data at a facility, leadership should assess the cost to:

- Establish physical barriers (for example, access controls) and information technology controls that prevent the unintentional sharing of technical information among employees.
- Obtain, maintain, and comply with licenses from DDTC that allow certain foreign person employees to access data for specific projects.

The cost-benefit analysis can be nuanced and companies may wish to seek advice of counsel that specializes in labor and employment matters and ITAR compliance to develop policy and internal guidance.

**Dealing with Potential Customers or Vendors**

When dealing with external communications, companies should:

- Perform diligence to ensure that they are not sharing technical data with foreign persons in violation of ITAR (see Drafting Note, Know the Recipient).
- Place the other party on notice that it may be receiving ITAR-controlled technical data by:
  - including appropriate contract language (see Drafting Note, Non-Disclosure Agreements); and
  - marking documents (see Drafting Note, Labeling and Marking ).

**ITAR-Controlled Efforts, Technology Control Plans (TCPs), and Technology Transfer Control Plans (TTCPs)**

The Empowered Official [or [TITLE OF DESIGNATED PERSONNEL]] will conduct a commodity jurisdiction review and classification determination for all new "**Company Efforts,**" which include:

- Programs.
- Products.
- Contract deliverables.
- Internal research and development projects.

The commodity jurisdiction review and classification determination processes establish whether a Company Effort is subject to the EAR or the ITAR and how potential exports must be handled. Company Efforts subject to the ITAR are deemed "**ITAR-Controlled**."

It is the responsibility of [PROGRAM MANAGEMENT/OTHER FUNCTION] to:

- Request that the Empowered Official [or [TITLE OF DESIGNATED PERSONNEL]] conduct a commodity jurisdiction review and classification determination for new Company Efforts.
- Develop a Technology Control Plan ("**TCP**") to document the access controls and security measures the Company has implemented to prohibit the unauthorized access by foreign persons to classified and unclassified defense articles, technical data, and defense services controlled under the ITAR.
- Develop a Technology Transfer Control Plan ("**TTCP**") [and Data Categorization Guidelines ("**DCG**")] specific to the ITAR-Controlled Company Effort in collaboration with:
  - the Empowered Official [or [TITLE OF DESIGNATED PERSONNEL]]; and
  - [ENGINEERING/OTHER FUNCTION].
- Provide the TCP[,] [and] TTCP [and DCG] to all Company employees that support an ITAR-Controlled Company Effort.

The TCP emphasizes the corporate requirements for complying with the ITAR, documenting the Company's specific information technology and physical security measures, and identifying the roles and responsibilities of the functional departments within the organization.

The TTCP provides the means by which ITAR-Controlled items and technical data can be properly safeguarded.

All employees are required to:

- Know whether they support ITAR-Controlled Company Efforts.
- Review the TTCP and execute a TTCP Acknowledgment before accessing items, systems, or collaboration tools for a Company Effort.
- Handle any technical data in accordance with the applicable TTCP [and DCG].

If employees have any questions regarding the status of a Company Effort or need guidance with respect to a TTCP [or DCG] they should contact either:

- [PROGRAM MANAGEMENT/OTHER FUNCTION].
- The Empowered Official [or [TITLE OF DESIGNATED PERSONNEL]].

For purposes of this procedure, the term "**employees**" includes, but is not limited to:

- Full-time employees.
- Part-time employees.
- Temporary employees; and
- Interns.

[PROGRAM MANAGEMENT/OTHER FUNCTION] shall collaborate with the [LEGAL DEPARTMENT] to ensure that appropriate contracts are in place to make the relevant portions of the TTCP binding on:

- Subcontractors and vendors.
- Consultants and advisors.
- Agents and representatives.
- Contingent workers.

The Empowered Official [or [TITLE OF DESIGNATED PERSONNEL]] shall maintain a record of the TTCP Acknowledgments executed by employees and contracts with other parties.

## ITAR-CONTROLLED EFFORTS

US companies are expected to know whether the ITAR covers their products or activities. For a broader discussion of which export regulations apply, see Complying with US Export Control Regulations Checklist: Establish Whether the Export is Subject to ITAR or EAR. US companies are also expected to know the export classifications of their items. For a detailed discussion of ECCNs, EAR99, and USML Categories, see Practice Note, Export Regulations: EAR, ITAR, and FTR: Category of Export and US Munitions List.

Organizations must establish formal processes for determining the classifications of their products. Most organizations create classification databases or matrices to house these determinations. Written documentation of the classification processes should identify:

- Personnel responsible for determining the classification of items.
- Reference tools and information relied on for making determinations.

For a broader discussion of which export regulations apply, see Practice Note, Core Elements of an Export Compliance Program: Export Classification.

This section is structured to reflect that export compliance personnel intend to collaborate with other functions to:

- Make initial determinations regarding jurisdiction.
- Develop guidance for the handling of ITAR-controlled technical data.

Companies typically have different organizational structures. The bracketed terms "Program Management/Other Function" and "Engineering/Other Function" are intended to provide examples of common functions that exist in companies that design and manufacture

defense articles. Common functions include:

- Program management or product management.
- Engineering.
- Research and development.
- Manufacturing operations.
- Quality.
- Information technology.
- Marketing and sales.
- The legal department and contract management.

The drafter should work with company leadership to determine which functions should have the responsibilities described in this section. An export compliance department can be a separate function or fall within one of the other functions. However, the ITAR requires that the Empowered Official have certain authority (see Empowered Official).

### Empowered Official

The ITAR requires that companies formally designate in writing employees to be "empowered officials" who have the independent authority to submit license applications and set company policy. In many companies, the Empowered Official collaborates with, and delegates tasks to, trained designated personnel.

The drafter can include bracketed language to identify a delegate by job title (for example, export administrator or compliance officer). The company should provide employees with access to an organizational chart that identifies the Empowered Official and any persons in positions that report to the Empowered Official. The company may also describe the responsibility of designated personnel in a technology transfer control plan or other related policies (see Technology Transfer Control Plan).

An Empowered Official must be a US person (citizen, permanent resident, or protected person) directly employed by the company:

- With management authority and the ability to set organization policy.
- That is legally empowered in writing to sign license applications or other requests for approval for the company.
- That understands both:
  - the provisions and requirements of the various export control statutes and regulations; and
  - the criminal liability, civil liability, and administrative penalties for violating the AECA and the ITAR.
- With the **independent authority** to:
  - inquire into any aspect of the company's activities;
  - verify the legality of the transaction and the accuracy of the information to be submitted; and
  - refuse to sign any license application or other request for approval without prejudice or other adverse recourse.

(22 C.F.R. § 120.25.)

The Empowered Official's responsibility is significant. The ITAR requires that **both** the company and the Empowered Official ensure and certify that a qualified person has been:

- Appointed using the appropriate corporate or organizational formalities (for example, board **resolutions** and records of any delegated responsibilities).
- Trained on the requirements of the qualified person's role.
- Provided with the resources to execute the qualified person's responsibilities.

### Technology Control Plan

Companies engaged in ITAR activities are expected to implement a formal Technology Control Plan (TCP) that, in general terms, outlines the processes and procedures that have been established to prevent unauthorized access to ITAR-controlled technical data by foreign persons, and also identifies the roles and responsibilities that the various functional departments within the organization play in preventing unauthorized technical data transfers or releases. The organization and structure of a TCP can vary depending on the type and size of the company. They are typically enforced by the Empowered Official. TCPs generally address:

- General security infrastructure and access controls (information technology and physical security).
- Foreign visitors to the facility.
- Offsite meetings with foreign persons.
- The responsibilities of specific functional groups, for example, Compliance, Security, Human Resources, Information Technology, Legal, Research and Development, Manufacturing, Transportation and Logistics, Warehousing, Purchasing/Procurement, Sales, Marketing, and Customer Service.

### Technology Transfer Control Plan

An ITAR-specific Technology Transfer Control Plan (TTCP) ensures that items and technical data that are subject to a specific project or program are controlled as required by the ITAR. The organization and structure of a TTCP can vary with the type and size of the organization. The plans are typically the responsibility of a cross-functional group and are implemented and enforced by:

- The Empowered Official or a delegate (for example, an export compliance officer).
- Technology control officers that primarily work in another organizational function and have been trained in the ITAR. These persons can implement processes within their function (for example, engineering or program management).

TTCPs generally address:

- Classification of which types of data in the effort are ITAR-controlled and the rationale supporting the designation.
- The persons that require access to the data.
- Specific controls and recordkeeping regarding the sharing of data.

The TTCP aligns with this procedure and other procedures to addresses the specific controls for a project, including:

- Access to the ITAR-controlled items and technical data.
- Unauthorized access to the ITAR-controlled items and technical data as well as designated ITAR-restricted areas to be used for the project.
- Physical security processes.
- Tracking of technology transfers.
- Administrative and management responsibilities, including employee training and auditing.

A company may adopt one TTCP if it has many similar projects or it may adopt multiple TTCPs if there are significant differences, such as:

- Types of technology and data involved.
- The involvement of different facilities.
- The use of different groups of staff within the organization.

As they develop the plan, the TTCP authors must assess issues such as:

- Project scope.
- Staffing needs.
- Expected external communications.

If they determine that expected activities require prior authorization from DDTC, they should inform organizational functions so that it can be factored into:

- Contractual commitments.

- Program management timelines.
- Supply and demand forecasts.

### Required Contracts and Employee Acknowledgments

Companies should seek contractual obligations that require suppliers and vendors to comply with the TTCP or handle materials in a manner that is consistent with the TTCP. The company's legal department or contract management staff must structure the contractual obligations so that they are consistent with the TTCP. By including those contractual obligations, the company may obtain remedies for material breach of contract, including:

- Termination.
- Damages
- Indemnification.

For more information on risk allocation provisions, see Practice Note, Risk Allocation in Commercial Contracts. The Empowered Official should retain a copy of each contract that addresses the exchange and track specific exchanges (see Drafting Note, Recording Transfers of Technical Data).

If the TTCP is a stand-alone document, it should contain an acknowledgment statement to help ensure compliance and maximize its enforceability. This procedure is drafted with the expectation that employees involved in a TTCP will execute an acknowledgment that they:

- Are receiving export-controlled technical data.
- Have reviewed the TTCP.
- Intend to handle the technical data in compliance with the ITAR and the TTCP.

The Empowered Official or export compliance staff should obtain an acknowledgment when the TTCP is circulated and when a new employee is added to the TTCP.

This procedure expands the definition of employee for purposes of the procedure. One of the intentions is to ensure that those persons are covered by the TTCP and transfers within the internal distribution groups (see Drafting Note, Electronic Transfers of Technical Data). When drafting an acknowledgment, companies should consider whether the employees are employed at will, have written employment agreements, are unionized, or have other employment arrangements. For more information on drafting acknowledgments, see Standard Documents:

- Stand-Alone Policy Acknowledgment.
- Employee Handbook Acknowledgment.
- Unionized Employee Stand-Alone Policy Acknowledgment.
- Unionized Employee Handbook Acknowledgment.

If a company seeks and receives an authorization from DDTC to share technical data with a foreign-person employee, the company should have that employee execute a non-disclosure agreement that addresses the scope and requirements of that authorization.

The Empowered Official or that official's delegate should retain a signed copy of each employee's acknowledgment.

### Data Categorization Guidelines

A company's information security policies usually include data categorization guidelines that classify information and describe safeguards that must be applied to each category of information (see Practice Note, Developing Information Security Policies: Data: Information Classification and Risk-Based Controls).

Common categories for types of data include:

- Public information.
- Company or customer confidential information.
- **Trade secrets** or highly sensitive information.

The Empowered Official and the authors of the TTCP should work with the company's information technology staff to determine if either:

- The ITAR designations fall within the restrictions applied to an existing category.
- An additional category needs to be created, implemented, and described to employees.

For example, a company that has not previously handled ITAR-controlled data may need to add new controls that limit network access by employees that are foreign persons (see Drafting Note, Foreign Persons). Those controls should supplement the safeguards for Electronic Transfers of Technical Data. Information technology personnel and export compliance staff should document processes for access approval and approved user lists.

For an example of an information security policy, see Standard Document, Information Security Policy.

**General Requirements Prior to Any Transfer of ITAR-Controlled Technical Data**

Employees must take the actions listed below prior to initiating any transfers of ITAR-Controlled technical data. In general, all transfers and releases of ITAR-Controlled technical data outside of the Company are subject to prior review and approval by the Empowered Official [or [TITLE OF DESIGNATED PERSONNEL]]. Under no circumstances should technical data be transferred outside of the Company without the prior approval of the Empowered Official [or [TITLE OF DESIGNATED PERSONNEL]].

- **Labeling and Marking**: Employees must label all ITAR-Controlled technical data to indicate its ITAR-Controlled status prior to transferring that data to anyone (internally and externally) by any means. This includes:
  - any items, technology, technical data, or software received under the terms of an export license; and
  - all materials created from ITAR-Controlled technology, technical data, or software, such as designs, drawings, shop procedure documents, or software.

  All ITAR-Controlled materials must be stored in a Secure Facility and, in the case of hard copies, contained in a color folder or other container that is labeled "**ITAR-Controlled**" and the cover, cover page, or sleeve must include the following statement:

  "**This document contains Technical Data whose export is restricted by the Arms Export Control Act (22 U.S.C. §§ 2778 to 2781) and the International Traffic in Arms Regulations (22 C.F.R. §§ 120.1 to 130.17). Violations of these laws and regulations are subject to severe criminal penalties.**"

  This marking must also be placed on ITAR-Controlled materials that are viewed on the company's information technology systems. [For more information on Company Secure Facilities, see the Company's ITAR Physical Security Procedures.]

### LABELING AND MARKING

Companies should require that employees immediately mark all materials containing ITAR-controlled technical data. The marking notifies personnel of the controls and consequences of violations. The markings can prevent unintended exports. Companies must restrict access to materials on shared drives to US persons or foreign persons with prior authorization from DDTC to access specific materials (see Drafting Notes, Data Categorization Guidelines and Electronic Transfers of Technical Data). A similar marking should be placed on materials that are viewed on the company's computers and information technology systems.

The bracketed language references a company ITAR Physical Security Procedure, which establishes Secure Facilities. This procedure addresses issues such as:

- The location of ITAR-restricted areas within company facilities that limit access to:
  - US persons, which includes citizens, permanent residents, or persons protected under US immigration laws and regulations; and
  - foreign persons authorized by DDTC to receive the technical data.
- Physical barriers to access-restricted areas.
- Precautions taken to adequately store ITAR-controlled data or protect it from view.

- **Know the Recipient**: It is the responsibility of each employee and [PROGRAM MANAGEMENT/OTHER FUNCTION] to determine whether or not the intended recipients of technical data are US or foreign persons. The TTCP [and DCG] will identify which employees may access ITAR-Controlled technical data internally for a Company Effort. [PROGRAM MANAGEMENT/OTHER FUNCTION] will ensure that the TTCP [and DCG] for each Company Effort establishes a list of "**Authorized Employees**" that consists of employees who are either:
  - US persons (citizens, permanent residents, or persons protected under US immigration laws and regulations); or
  - foreign persons that the Directorate of Defense Trade Controls ("DDTC"), which administers the ITAR, authorized to receive technical data for the Company Effort.

  For transfers outside of the company, employees must request written or verbal confirmation that all proposed recipients of technical data are US persons. If it is unclear as to whether an intended recipient is authorized to receive ITAR-Controlled technical data, [PROGRAM MANAGEMENT/OTHER FUNCTION] [or ENGINEERING/OTHER FUNCTION] must immediately contact the Empowered Official [or [TITLE OF DESIGNATED PERSONNEL]] to seek guidance. The Empowered Official [or [TITLE OF DESIGNATED PERSONNEL]] will determine whether the Company must obtain formal authorization from DDTC.

  ### KNOW THE RECIPIENT

  The company has an obligation to perform diligence before sharing technical data internally or externally. The TTCP should identify which employees can access technical data for a project. The company should verify these employees are US persons or foreign persons that the DDTC authorized to receive the ITAR-Controlled technical data. The company should keep records of this verification to support the TTCP.

  Before sharing technical data with vendors or other outsiders, employees must inform the recipient that they intend to send ITAR-controlled data and request confirmation that all of the recipients are US persons or that receipt does not violate the ITAR. This is often done using questionnaires given to vendors and potential customers. An employee should coordinate these efforts with Program Management or other responsible functions to ensure that their efforts align with the TTCP. Program Management or the employee must contact the Empowered Official or that official's delegate if the employee:

  - Does not receive verification from the recipient.
  - Otherwise has reason to believe that the recipient is not a US person.

  The company should maintain a record of its diligence efforts in a tracking log (see Drafting Note, Recording Transfers of Technical Data).

  As part of its broader export compliance efforts, the company should engage in restricted party screening required by various US export control laws. This process should complement precautions taken to ensure that recipients are US persons or are otherwise receiving the information in compliance with the ITAR. For more information on restricted party screening, see Practice Note, Core Elements of an Export Compliance Program: Restricted Parties List Screening and Restricted Party Screening Checklist.)

- **Non-Disclosure Agreement (NDA)**: It is the responsibility of [PROGRAM MANAGEMENT/PRODUCT MANAGEMENT], along with the assistance of [LEGAL DEPARTMENT], to confirm that an NDA is on file for [all companies with whom the Company is doing business] [all companies with whom the Company is doing business related to defense articles]. In order to address export compliance, it is critical that an NDA is in place prior to transferring technical data. The NDA ensures that the signatory has read and agrees to abide by the export compliance requirements contained therein and that the signatory has been screened against the restricted parties lists.

  ### NON-DISCLOSURE AGREEMENTS

  Companies that handle ITAR-restricted data should ensure that they have non-disclosure agreements (NDAs) in place with all outside parties involved in that business. The NDA should include clauses where the parties agree to, among other things:

  - Abide by the ITAR.
  - Register with DDTC, if necessary.
  - Seek consent from the other party before disclosing any information to third parties.

- Indemnify the other party for losses incurred in connection with violations of the ITAR.

Many companies enter into NDAs with all of the companies with which they do business while others choose not to do so, especially if most projects do not involve confidential information. The bracketed language provides options to addresses both circumstances. For more information on confidentiality agreements generally, see Confidentiality and Nondisclosure Agreements Toolkit.

As a general matter, companies should contract to ensure that recipients of ITAR-controlled data handle it in a manner consistent with the TTCP (see Drafting Note, Required Contracts and Employee Acknowledgments).

**Verbal or Visual Transfers of Technical Data**

When employees provide verbal descriptions of, or allow other persons to view, technical data it can be a deemed export that requires prior authorization from DDTC. ITAR-Controlled technical data can be verbally or visually transferred in a number of settings, including:

- Face-to-face meetings with customers or vendors.
- Views of parts in fabrication in company facilities.
- Technical exchanges during a phone call.
- Over the internet (for example, during a program review that can take place both in person and over the internet).

Employees must plan all of these transfers in advance to:

- Determine the type of information that will be shared.
- Confirm attendance lists and ensure that no additional prior authorizations are required.

(See General Requirements Prior to Any Transfer of ITAR-Controlled Technical Data.)

Employees are prohibited from conducting verbal or visual transfers of ITAR-Controlled technical data in informal settings at Company facilities such as a hallway, common area, or lobby. Employees are required to conduct telephone or online discussions of ITAR-Controlled technical data in a Company Secure Facility.

Employees must seek the prior review and approval of the Empowered Official [or [TITLE OF DESIGNATED PERSONNEL]] prior to sharing technical data at meetings outside of the Company, including customer or vendor facilities. Employees are prohibited from transferring technical data outside of the Company without such prior approval.

Employees must send the request for approval to [EMAIL ADDRESS FOR EMPOWERED OFFICIAL OR DESIGNATED PERSONNEL] [two (2) days in advance of the proposed transfer]. Employees must include:

- The business purpose of the transfer.
- A description of the technical data to be transferred and the applicable TTCP.
- A list of expected recipients.
- The location and means of the transfer.

Employees must appropriately mark all materials that are approved to be shared visually (see General Requirements Prior to Any Transfer of ITAR-Controlled Technical Data).

[For more information on Company Secure Facilities, visitors, and offsite meetings, see the Company's ITAR Physical Security Procedures and ITAR Visitor and Offsite Meeting Procedures.]

## VERBAL OR VISUAL TRANSFERS OF TECHNICAL DATA

Sharing technical data verbally or visually can constitute a deemed export under the ITAR (see Drafting Note, Export and Release). This section describes:

- Prohibited conduct.

- Actions to be taken before visual and verbal transfers.
- Common circumstances to be addressed.

The paragraph regarding the process for requests for approval describes common information to be included in those communications. The bracketed optional language describing two days' advance notice can be included to provide the Empowered Official with sufficient time to conduct diligence and address any concerns in the least disruptive manner.

The bracketed language regarding policies refers to common policies that describe:

- Areas within company facilities where ITAR-controlled technical data can be exchanged.
- Procedures for handling visits to company facilities or employee visits to customer or vendor facilities.

**Physical Transfers of Technical Data**

Employees must seek the prior review and approval of the Empowered Official [or [TITLE OF DESIGNATED PERSONNEL]] prior to physically transferring ITAR-Controlled technical data inside or outside of the US. Employees are prohibited from physically transferring technical data outside of the Company (including to foreign affiliates of the Company) without such prior approval.

Employees must send a traffic request for approval to [EMAIL ADDRESS FOR EMPOWERED OFFICIAL OR DESIGNATED PERSONNEL] [two (2) days in advance of the proposed transfer]. Employees must include:

- The business purpose of the transfer.
- A description of the technical data to be physically transferred and the applicable TTCP.
- A list of expected recipients.
- The destination and means of the transfer.

Employees must appropriately mark all materials that are approved for transfer (see General Requirements Prior to Any Transfer of ITAR-Controlled Technical Data) and must include the following statement in any shipping documents or cover page for any approved physical transfer:

**"The materials contained herein may be subject to the Arms Export Control Act (22 U.S.C. §§ 2778 to 2781) and the International Traffic in Arms Regulations (22 C.F.R. §§ 120.1 to 130.17). "**

[All Company employees that support any programs or products involving ITAR-Controlled hardware, software, or technology and who will be traveling overseas should refer to the Company's International Travel and Hand Carry Procedure.]

## PHYSICAL TRANSFERS OF TECHNICAL DATA

Physical transfers of technical data can be exports under the ITAR even if within the US (see Drafting Note, Export and Release). This section describes:

- Actions to be taken before physical transfers.
- Common circumstances to be addressed.

The paragraph regarding the process for requests for approval describes common information to be included in those communications. The bracketed language describing two days' advance notice can be included to provide the Empowered Official with sufficient time to conduct diligence and address any concerns in the least disruptive manner.

This section **does not** address documentation for the export of items out of the US. For more information on shipments of items out of the US, see Standard Document, Destination Control Statements.

The bracketed language references an International Travel and Hand Carry Policy, which is a common policy that addresses precautions to be taken by employees supporting ITAR-Controlled Projects who need to travel with company property.

**Electronic Transfers of Technical Data Generally**

Technical data may be electronically transferred in several ways, including:

- Posting data to a secure File Transfer Protocol ("**sFTP**") site.
- Email utilizing either:
  - a laptop/desktop computer; or
  - a smartphone or a cell phone.
- Sending a fax or text message.

All electronic transfers must be in English and executed by Authorized Employees. Employees are prohibited from making electronic transfers to employees who are not Authorized Employees or outside the company without the approval of the Empowered Official [or [TITLE OF DESIGNATED PERSONNEL]] (see General Requirements Prior to Any Transfer of ITAR-Controlled Technical Data).

Approved methods are described in:

- Electronic Transfers within Secure Facilities.
- Electronic Transfers Outside of Secure Facilities.

To prevent ITAR-Controlled technical data from being seen, copied, or intercepted by a foreign person, any alternate solutions for the electronic transfer of ITAR-Controlled technical data must first be reviewed and authorized by the Empowered Official [or [TITLE OF DESIGNATED PERSONNEL]] [[PROGRAM MANAGEMENT/OTHER FUNCTION], and [INFORMATION TECHNOLOGY]].

Employees must send the request for approval to [EMAIL ADDRESS FOR EMPOWERED OFFICIAL OR DESIGNATED PERSONNEL] [[PROGRAM MANAGEMENT/OTHER FUNCTION], and [INFORMATION TECHNOLOGY]] [two (2) days in advance of the proposed transfer]. Employees must include:

- The business purpose of the transfer.
- A description of the technical data to be transferred and the applicable TTCP.
- The proposed means of the transfer and the reason that other approved methods cannot be used.

All employees who handle ITAR-Controlled technical data must include the following language in internal and external electronic transfers related to that Company Effort:

"**The recipient of this email acknowledges and understands that certain information contained in this email or in an attachment to this email may be subject to export controls and restrictions including, but not limited to, the International Traffic in Arms Regulations (ITAR). The recipient agrees not to disclose, transfer, or otherwise export or reexport any technical data or other restricted information to any Foreign Person (including any foreign national, foreign business, or foreign government), whether in the United States or abroad, without fully complying with the ITAR, including obtaining any necessary license or other prior authorization required by the US government**."

[For more information on Company Secure Facilities, visitors, and offsite meetings, see the Company's ITAR Physical Security Procedures and ITAR Visitor and Offsite Meeting Procedures.]

**Electronic Transfers Within Secure Facilities**

The following are compliant options for Authorized Employees transferring ITAR-Controlled technical data to one another electronically at Secure Facilities without further protecting the data prior to transfer:

- Email from an Authorized Employee to another Authorized Employee.
- Fax from an Authorized Employee to another Authorized Employee.
- Uploading data to a stand-alone server, hosted in the US and supported by Authorized Employees ("**ITAR Server**").

**Electronic Transfers Outside of Secure Facilities**

Authorized Employees have the following options to transfer ITAR-Controlled technical data to authorized persons outside of Secure Facilities and to external recipients that have been approved by the Empowered Official [or [TITLE OF DESIGNATED PERSONNEL]]:

- **sFTP sites.** sFTP sites may be used for electronic transfers so long as site access is restricted to Authorized Employees or approved external recipients with username and password requirements. Any Company IT support personnel must also be Authorized Employees.
- **Encrypted or Password Protected Email**. The following describes the process for technical data transfers to Authorized Employees or approved external recipients via email:
  - encrypt or password-protect the ITAR-Controlled technical data;
  - send the encrypted or password-protected file to an Authorized Employee or approved external recipient; and
  - send the key or password under separate cover to an Authorized Employee or approved external recipient.

  The second and third steps may be performed in any order, but must be separated either in time or by method.

### ELECTRONIC TRANSFERS OF TECHNICAL DATA

Electronic transfers of technical data can be exports under the ITAR even if within the US (see Drafting Note, Export and Release). This section describes:

- Actions to be taken before electronic transfers.
- Common circumstances to be addressed for transfers at company secure facilities and when sending electronic transfers outside of secure facilities.

The paragraph regarding the process for requests for approval describes common information to be included in those communications. The bracketed language describing two days' advance notice can be included to provide the Empowered Official and other required functions with sufficient time to evaluate the alternative means of communication.

The bracketed language regarding policies refers to common policies that describe:

- Areas within company facilities where ITAR-controlled technical data can be exchanged.
- Procedures for handling visits to company facilities or employee visits to customer or vendor facilities.

**Reproduction Projects**

**Onsite**. Authorized Employees are the only employees authorized to conduct onsite reproduction projects for ITAR-Controlled technical data and the reproduction must be carried out only in Company Secure Facilities.

**Offsite.** Certain reproduction projects may not be able to be supported onsite. These include production of oversize posters or printing in large quantities. Authorized Employees must obtain prior approval from the Empowered Official [or [TITLE OF DESIGNATED PERSONNEL]] before beginning any offsite reproduction effort.

[For more information on Company Secure Facilities, see the Company's ITAR Physical Security Procedures.]

### REPRODUCTION PROJECTS

Reproduction efforts can involve Visual, Electronic, and Physical transfers. These can raise the risk of unauthorized exports or deemed exports under the ITAR (see Drafting Note, Export and Release). This section briefly outlines requirements and requires that export compliance staff be contacted so that appropriate precautions can be taken before an offsite reproduction effort is started.

The bracketed language regarding policies refers to common procedures that describe areas within company facilities where ITAR-controlled technical data can be exchanged.

**Recording Transfers of Technical Data**

If an electronic, verbal, or visual transfer of technical data is subject to an export license or license exemption under the ITAR (for example, transferred from a US person to a foreign person/country), then the record of such transfer must be recorded in a Technical Data Transfer Log by the Empowered Official [or [TITLE OF DESIGNATED PERSONNEL]] [PROGRAM MANAGEMENT/OTHER FUNCTION].

For physical shipments of ITAR-Controlled technical data for which a traffic request has been reviewed and approved by the Empowered Official [or [TITLE OF DESIGNATED PERSONNEL]], the Empowered Official [or [TITLE OF DESIGNATED PERSONNEL]] will record the subject transfer in the **Technical Data Transfer Log**.

## RECORDING TRANSFERS OF TECHNICAL DATA

DDTC has not provided specific guidance for technical data logs. A log should include:

- The name and location of the recipient.
- The applicable authorization or exemption.
- The name of personnel responsible for handling the transfer.
- The date of the transfer.

**PRODUCTS**

PLC US Commercial Transactions, PLC US Law Department