Advanced ITAR Concepts

and Compliance Requirements
Technical Support & Asking Questions

• We will post the dial information in the chat window
• You may ask a question at anytime during the live presentation via the chat window on the lower right hand side of your screen
• Questions will be aggregated and addressed during the Q&A segment
• Please note, this call is being recorded for playback purposes
• If you’re already logged in to the online Webcast, we will post a link to download the files shortly

Send an email to service@webvent.tv for Technical Support
Christos Linardakis is an attorney with the Braumiller Law Group. He has served at several multibillion dollar publically traded companies, as well as in small-to-medium size export trading companies, as a Global Trade Compliance & regulatory attorney, ITAR Empowered Official, and V.P. & General Counsel for a German Export Trade Company. His experience in various Export Enforcement investigations and FBI cases, including the ARC Electronics Russian Spy case, has provided him with the skills and insight on the risks of global trade. He is a frequent speaker with various U.S. government agencies, including the Dept. of Commerce, SBA, and SBDC, as well as a member of Infragard.
About The Global Trade & Supply Chain Institute (GTSCI™)

• The Global Trade & Supply Chain Institute (GTSCI™) was established to incorporate a single resource that offers all modes of training, whether it be via webinar, in-person seminars, boot-camps, or on-site training for individuals and teams.

• Our Executive Team is made up of corporate and private subject matter experts (SME) in their respective fields

Disclaimer

• This presentation provides general information on the topic of ITAR, and it not intended to constitute legal advice

• Registering for this webinar only constitutes an agreement to attend the webinar, not a contract for legal advice and does not establish an attorney-client relationship

• *No reproduction, distribution or publication of this presentation is allowed, without the express written approval of GTSCI*
Agenda

- How to meet DDTC Guidelines for an effective ITAR compliance program
- What your company ITAR manuals and polices should encompass
- Key elements and best practices for an effective ITAR compliance program
- Developing ITAR manuals, policies and desk-top procedures
- Structuring and monitoring your ITAR compliance program, including IT controls for systems, technical data, personnel, sales and manufacturing
- How and what to include in your Technology Control Plan so it’s practical and effective, while still meeting DDTC expectations
Withstanding an “Attack” by DDTC
Key Elements and Best Practices for Effective ITAR Compliance

1. Management Commitment: The ITAR Empowered Official, along with Senior management must establish written ITAR compliance standards for the organization, commit sufficient resources for the ITAR compliance program, and ensure appropriate senior organizational official(s) are designated with the ultimate overall responsibility for the ITAR compliance program to ensure adherence to both export control laws and regulations.

2. Continuous Risk Assessment of the ITAR Program

3. Formal Written ITAR Management and Compliance Program: Effective implementation and adherence to written policies and operational procedures

4. Ongoing ITAR Compliance Training and Awareness
5. Cradle to Grave ITAR Compliance “Security”: Screening of employees, contractors, customers, products, and transactions and implementation of compliance safeguards throughout the product life cycle including product development, jurisdiction, classification, sales, license decisions, supply chain, servicing channels, and post-shipment activity

6. Adherence to Recordkeeping Regulatory Requirements

7. Internal and External Compliance Monitoring and Periodic Audits

8. Internal Program for Handling Compliance Problems, including Reporting ITAR Violations thru a hot-line

9. Completing Appropriate Corrective Actions in Response to ITAR Violations
• Using organizational charts you must initially identify employees in the ITAR process, who are then verified during plant audits. Then, assign an “SME” within each plant that is training and empowered at a higher level than local personnel.

• At a macro level, identify all of the offices and divisions that you think could possibly participate in your ITAR processes. This could include:
  • Accounting
  • Legal Counsel
  • Contracts
  • Licensing
  • Customer Service
  • Order Processing
Identifying and Empowering the Right Internal Resources and Personnel (cont’d)

• Engineering/R&D
• Physical Security
• Field Services
• Purchasing
• Finance
• Sales/Marketing - Export and Re-export
• Human Resources
• Shipping/Logistics
• Systems Management
• Information Technology
• Website Maintenance Group
Develop a set of formal written policies and procedures -- an ITAR Manual - that provides sufficient safeguards at each key step in the supply chain management to guard against sales of sensitive or dual-use technology to unauthorized parties or for unauthorized activities.

The policies and procedures should be applied throughout the entire organization of the company, including any divisions and subsidiaries, and cover, in step-by-step detail, each of the key elements that accompany your DDTC registration materials.

The Manual should serve as the standard operating procedure guidelines for all company employees.

A written Manual is also critical to ensuring consistent training and education for employees throughout the company.
Policies, Procedures and Controls

- Secured server – Controls access to ITAR data. Deploy for each business unit involved in military/aerospace/defense work for securing all data, drawings, etc. This can be tied into your corporate ERP system which is managed by U.S. citizens only.

- ITAR training via On-line learning – ITAR employees must be identified and trained. Automated training process once employee is identified as working with ITAR (leveraging your HR dept.). Yearly notifications for refresher courses. Provide global accessibility, if needed. Training material is updated as ITAR regulations are revised/updated.

- Yearly audits of ITAR locations – Provides details on plant compliance to ITAR regulations. Also highlights areas which may be weak points in the ITAR process. Audit is revised as changes to ITAR regulations are identified.

- Human Resources – Specific policies and procedures must be developed for the recruiting and hiring of Foreign Nationals. Citizenship form; ITAR letter of Assurance; Foreign National hiring form.

- All encompassing ITAR manual – Developed for use during a government audit.

- Subscribe to publications which monitor ITAR regulations – ITAR policies and procedures are updated as changes to ITAR regulations are identified.
Policies, Procedures and Controls (cont’d)

• Recordkeeping - The record keeping system should be developed in a manner that allows accessibility and retention of the documents in the event Customs or other government agencies request them

• Any ITAR-controlled technical data should be conspicuously marked with clear language identifying the document as ITAR

• IT - On-site and off-site Foreign National(s) IT staff are not permitted to work on an ITAR employee’s computer. This includes outsourced level 1 Helpdesk agents that are blocked from remotely accessing employees’ laptops

• Must be able to support and provide proof of disk erasure and/or destruction in the event of an audit by the Department of State. If it is a PC that went to a recycler, IT should be provided with the certification (or similar notification) that unit was wiped cleaned using Department of Defense standard utility (or similar method) of all data. If it is a PC that is to be redeployed, IT will need to erase the machine. Documentation/certification of process completion to be retained for 5 years

• Policies/Procedures should be written to provide specific methodology which adheres to each ITAR compliance regulation (again, you look at each and every “recommended” compliance area of your DDTC registration and aim to meet each one)
The Scope of Your ITAR Programs Based on Operations Today

- How much you need to spend: Tailoring your compliance program to your company operations, industry risks and geographic scope
  - Program should be tailored to all “business units” within your company
  - Additional foreign manufacturing site(s), i.e. Mexico, raises the “bar” on your compliance program
  - Develop and deploy policies/procedures based on the key elements recommended by the DDTC, but also aligned to both your business models and the level of technology of your products. As your business changes, so does your ITAR compliance programs and policies
  - Look at the products and technology you are offering, to determine the scope, depth and extent of capital investment within your ITAR program (i.e. SME products should require a higher level of controls)
Structuring and Monitoring a TCP

• Primary objectives when addressing the effectiveness of your TCP:
  • Protecting export controlled technical data and/or ITAR information from inadvertently being exported or forwarded while at rest or being used (file sharing system for your workers, unprotected databases)
  • Ensuring multiple layers of protection (i.e. passwords, 2-factor authentication, encryption) in order to maintain control over the security and confidentiality of data from inadvertent exposure
  • Segregating & securing technical data, including work areas (physical and IT controls)
  • Identifying Foreign Nationals within your organization that may need access to export controlled data (“look into the future”—what/when will a project “cross the line” triggering export licensing?)
  • IT system to track access to export controlled technical data, including historical auditing (i.e. reports as to who, when, date/time of users accessing export controlled designated servers or drivers)
  • Written procedures to protect proprietary, confidential, and export controlled information against unauthorized intra-company exports and to 3rd parties
• Define and identify the following as a “checklist” in your program:
  1. What information and data that must be managed and controlled?
     - NPI (new product introduction)
     - development phase (R&D)
     - manufacturing production (particularly when ITAR)
     - Quality control, test & evaluation (careful of software and test results)
  2. Identify data storage locations, document retention & email retention policies, and IT system applications containing technical data
  3. Policies and procedures you will enforce (make them practical).
  4. Reporting, auditing, and periodic review processes designed to keep your TCP active and reflective of your current business model/operations (you need to change with the times)
  5. Define what technology decisions are required, when, and employee responsibilities by position
• Cyber security and physical authentication
• Traceability and audit trail of application and data access requests should be maintained
• Password controls for access and application security restricted to specific “drives” within a business entity (i.e. minimum set of access privileges necessary to execute their job)
• Desktops/Laptops: End of lease, destruction, repair—need to include procedures on handling the above that may contain export controlled data
• Smart Cards or internally developed access cards mirrored off the DoD Common Access Card (CAC) can improve reliability and capabilities
• Digital signatures on documentation, emails, and information transferred over the internet.
• FTTP sites for storage and transfer of data to outside vendors, customers and overseas subsidiaries, including level of encryption for transmitting emails with ITAR technical data
Limiting Access of Foreign Nationals and Overseas Subsidiaries

• Focus# 1: Creation of “smart identifiers” within an employee profile (must include HR, IT, and hiring manager)

• Focus# 2: Data segregation both for documentation and engineering drawings; test manufacturing floor (locked document control centers, floor layout and/or production area)

• Focus# 3: Escort requirements, color coded badges, marked production floors with “color tape”; SOP for all receptionists and plant managers

• Focus# 4: IT Networks and servers: 2-factor authentication (password and key), safe-recipient listings, stand-alone servers, restricted access to networks containing export controlled data

• Focus# 5: Create a “hosting foreign national visitors” form: release of data, visual and written; location of meeting rooms (avoid deep within the facility); need-to-know only access to information to perform their tasks

• Focus# 6: Visitor request – FN: should include the primary host name, location, country(s) represented, reason for visit, personal info (name, DOB, passport no., citizenship), what type of technical data will be discussed, tour of facility and/or system/hardware demo, approval signatures from both host and local export manager as well as security/facilities badge issuance approvals

• Look at the Defense Security Service (DSS) agency branch of the DOD: a wealth of information on controlling FN’s employed or assigned to a facility
• EasyLobby ®Secure Visitor Management badge: provides enterprise-class scalability including pertinent visitor data and printing capabilities

• Quest® Software & hardware:
  - File Access: ability to report historical information as to who accessed controlled data and files, including business critical files such as drawings, artwork, CAD data, including changes
  - Ability to collect data from multiple systems to identify where export controlled data is stored
  - 2-factor authentication tool to ensure person is who they say they are (token code or mobile device)
  - Active Roles Server: grant access to employees assigned to export controlled projects certain user rights specific only to their needs

• Titus® Software:
  - Classification sector: enforces classification at point of creation
  - Label marker: raises security awareness through visual markings (“internal only”)
  - Metadata generator: enhances archiving, data loss prevention (key in an enforcement action!) and organizational firewall protection (remember your Help-Desk issue)
  - Policy and security enabling: encrypt and protect emails
• Virtual data rooms: can provide a single-source secure way to control access to critical documents, including access controls, real-time audit reports, automatic water-markings, etc.

• Information labeling:
  • Accountability on the user, i.e. protective labeling in subject line such as “ITAR or export controlled”.
  • Pop-up warnings to prevent from sending to inappropriate recipient or large distribution list
  • Automating labeling and marking of export controlled data using metadata (i.e. placement on a computer network where the data was created)
  • e-Discovery: ability to find and retrieve critical emails by reading classification labels (i.e. “ITAR 2015”)
• After all of the above, your program should disclose the following:
  • ITAR data at rest or “in-use” on systems
  • ITAR data in back-end systems (storage, backups, databases and data rooms)
  • Monitoring capabilities in the transmission of sensitive data on a real-time basis (i.e. track movement of ITAR data across the network, both internally and as it exfiltrates the network)
  • Encryption controls (Cloud Computing)
Primary Objective of TCPs (cont’d)

- Access Controls for FN’s and visitors (historical auditing capabilities)
- Data requirements: File access & Active Directory
- Collecting data from multiple systems (i.e. emails, ECNs, CAD data, drawings, artwork, activity logs)
- Authentication of who is accessing controlled technology, including on the manufacturing floor (i.e. work-travelers)
End Result of a Solid TCP

- Establishes a well-designed enterprise Information Security Program (InfoSec)
- Ability to collect & correlate disparate IT data from numerous systems and devices
- Pass internal and external government audits
- Real-time data collection and analysis, including tamper proof logs
- Alert notifications for suspicious activity involving databases and systems that store ITAR information
End Result of a Solid TCP (cont’d)

• Architecture of IT systems will support a robust Technology Control Plan, including “man in the middle” attacks, server authentication (digital certificates), encryption, cloud computing
• Vulnerability and Penetration testing protocols, including operating systems security assessments
• Long-term access of event logs and repositories, in the event of non-compliance
Product engineers, test and reliability labs, and prototype departments are “key critical” for ITAR training and could be your “first line of defense”, along with sales engineers.

Individuals assigning part-numbers and respective ECCNs & USML classifications ensures tagging and identifying controlled finished goods and components.

Training should be specific to the individuals’ and departments’ roles. Example: product development review, engineering work order for fiber optic cable (5A001.c.1 vs. 5A991.b vs. Cat. XI(c))

Process documentation: ECNs, 1st article inspection and conformance reports, artwork/drawings, and software & test results may all contain export controlled information.

Must know when prohibited from distribution to unauthorized individuals, restricting the treatment of data/technology, and imposing restrictions on dissemination of such information.
Training On ITAR Compliance: Your Company’s Best ROI (cont’d)

- Tailor specific to job duties concentrating on the following:
  - HR: Foreign national perspective, job description requirements for hiring manager, conjunctive with H1B and other applications
  - IT: Ensure identifiers for all FN’s, including help-desks; access to servers, SAP, CAD rooms, should be limited based on job responsibilities. Software deployment administrator and email administrators
  - Engineering: oversight on any managers who have FNs in their presence or as direct reports
  - Shipping departments: your last “gatekeeper” from keeping a violation from occurring
  - Procurement: are they aware if supplier is selling you an ITAR controlled item
  - Travel only laptops or at a minimum, cognizant of maintaining control of personal laptops containing export controlled data. Alternative: requirement to “remove” off-line all emails and export controlled data
  - Signed TCP acknowledgement to bind all personnel
At a minimum, your TCP and ITAR compliance program will need to include:

- Flow charts of departments effected by the TCP
- Physical security and facilities department
- Hiring managers responsible for Foreign National employees
- HR procedures, including informing departments of FN presence when deemed necessary (careful of labor law issues!)
- Legal
- IT including support staff, after-hours help desks, and security administrators
- Compliance department
- Internal Audit (minimum yearly review of all processes and procedures)
- …con’t
In addition to the above, it should also include:

- R & D and/or New Product Introduction
- Written and documented procedures/policies, preferably incorporated into current business and/or ISO procedures to allow for self-policing
- Local, ancillary and disparate solutions need to be addressed
- Effective, enterprise wide TCP to track, report, manage and comply with the EAR
- Classification policy for ECCNs & USML (i.e. Decision Trees)
- Create “filters” by business unit, plant, facility
- Best to approach development of a TCP by starting with what your “end purpose” is and building backwards, including identifying business units, facilities, departments, and/or floors that need to have both electronic measures in place and physical measures in place—than you can “VCE” the concept to other facilities and divisions
Creating a Checklist and Audit Template

- Critical to develop a checklist of what your ITAR program should look like, based on your current business practices and anticipation of future needs. This can be done by:
  - Conducting department interviews
  - Testing current systems (don’t forget the legal department/patent filings)
  - Transactional testing of current controls
  - SOP reviews
  - General observations of current practices
Past experience has taught me the following categories should be addressed:

- Procedural controls
- Corporate/Business
- Regulatory environment
- Email/Documentation
- Recordkeeping
- Technology Transfers
- IT/IS Systems
- Qualified ITAR Products
- Test Data Results
- HR/Employee controls (including training)
- Security

The end result when reviewing, auditing and addressing each of the above areas should be a comprehensive program covering, at a minimum, the areas above.
From both a systems standpoint and a documentation position, at the conclusion of any checklist/audit findings and/or architecting your ITAR compliance program, you should have, at a minimum:

- General ITAR controls across all business units and departments (i.e. competencies, procedural, corporate and regulatory)
- Specific controls applicable to any and all departments affected by ITAR projects
- Computer Systems required to support and meet ITAR regulations, both today and in the future
In-Depth Review Areas

- Typical risks have been found in:
  - Classifications (ECCN vs. USML), including technical data
  - Customer Screening: End-Use/User
  - Hand carries: both of product & laptops
  - Records Management: inability to tie all data and records to one order/license
  - Technology Transfers: 3rd party vendors
  - Licensing/regulatory reporting: tracking values and quantities
• Failure to advise DDTC on all notifications of initial exports under TAAs (22 CFR 123.22)
• Misuse of ITAR exemptions
• Shipping & Receiving Controls: confirming quantities under a license, DSP61 on imports, etc.
## ITAR Compliance Program Guidelines

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Yes/No or N/A</th>
<th>Internal SOP reference number/QMS/ISO#</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0 Recordkeeping</td>
<td>- Description of record systems concerning U.S. origin products&lt;br&gt;- Procedures for maintaining records relating to U.S. origin products</td>
<td>Yes</td>
<td>See Sec. 1.2 of ITAR Compliance Manual</td>
</tr>
<tr>
<td>5.0 Internal Monitoring</td>
<td>- Perform audits periodically to ensure integrity of compliance program</td>
<td>Yes</td>
<td>See Sec. 3.8 of ITAR Compliance Manual</td>
</tr>
</tbody>
</table>
Free TCP References:

NISPOM 10-509: great source of materials for building your TCP
  • Defense Security Service: Technology Control Plan available on their site
  • Defense Security Cooperation Agency: “SAMM” manual/policy
  • DoD 5105.38-M
  • BIS’s website: Export Management & Compliance Program
  • Defense Technology Security Administration: Technology Transfer Control Plan Development Guidelines available on their site
  • Security and Policy Review Handbook: Published by Aerospace Industries Association
  • The Aberdeen Group: excellent source of “White Papers”
  • DoD Standard 5220.22-M: Software and Data files security program
  • National Institute of Standards and Technology: excellent source for computer systems technology controls
  • DISAM: http://www.disam.dsca.mil/: Excellent source and links for TCPs
Areas of Concern

• R&D, New Product Introduction: Important to let this department understand that the “original design intent” is a critical step in the determination of whether or not a product may be subject to the ITAR. Otherwise known as the “genesis” of a product, this concept is critical at the point of development and design, which can directly affect whether a product is subject to the ITAR regulations.

• Documenting the above is critical and should include the technology that is being used (both design and manufacturing), BOMS, patent drawings, data, engineering drawings, product specifications, and competitors’ offerings, to show that the product is subject to the Export Administration Regulations, as opposed to the ITAR.

• Do not confuse end-user or end-use, with whether an item is subject to the ITAR. Neither is exclusively used to determine jurisdiction and DDTC has stated that an item may be used 100% by the military, for a military end-use, and yet, not be subject to the ITAR.
**Factors for Determining Predominant Civil Applications:**

- Nature, Function and Capability of civil applications vs. military applications
- Performance Equivalent standards (Form, Fit, Function definitions: see 120.4(d)(2))
- Number, Variety and Predominance of civil applications vs. military
- Nature of controls imposed by other Nations and foreign policy (i.e. Wassenaar Arrangement, a multilateral convention for dual-use and arms export controls)
- Level of technology is readily available outside the U.S.
- Product does not perform or support a core military function, i.e. intelligence gathering, surveillance; instead, it’s a secondary function
- Foreign performance equivalents are available in civil applications and outside the U.S. (i.e. foreign availability of like systems or products is a strong indication the item should not be controlled)
Individuals within department generating technical information should be given clear guidelines on how to label such information as being subject to the ITAR. The following statement should be programmed, whenever possible, when a drawing is generated that is known to be controlled by the ITAR:

**For ITAR technical drawings only:**
- **WARNING** - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.), International Traffic in Arms Regulations, ITAR 22 C.F.R. 120-130. Violations of these export laws are subject to severe criminal penalties.

- The more visible the markings, the more likely the recipient of the information will be on notice that they have an obligation to treat the information as export controlled. The same should be done if ITAR controlled data is made available via a FTTP site or cloud based data room.
• Your goal is to ensure that any ITAR controlled products are clearly marked as such, to avoid inadvertent exports without an export license, including putting your domestic customer and/or freight forwarder on notice.

• The following statement, whenever possible, should be printed on order confirmations, packing slips and/or commercial invoices accompanying the physical shipment, whether domestically or internationally:

• **For Domestic ITAR Product Shipments Only:** If you are shipping products subject to the ITAR, you should place the following statement on all documents and airway bills:
  
  • **WARNING** - This shipment is subject to the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.), International Traffic in Arms Regulations, ITAR 22 C.F.R. 120-130. Violations of these export laws are subject to severe civil and/or criminal penalties. Dept. of State approval required prior to exporting.
Examples of Technical Data

• Your sales, engineering, and R&D departments should be trained to identify when technical data is controlled. Some examples to use are:
  • is not found in the public domain, either in whole or in part
  • was generated by independent R&D for military application
  • was generated under a Dept. of Defense, or similar agency contract/project (i.e. DARPA funding)
  • is a genuine engineering scale drawing, not a “cartoon”
  • provides understanding of sensitive capabilities (i.e. nuclear applications)
  • provides meaningful insight in the areas of design or manufacturing of defense articles
  • contains answers to questions involving “how to” and “why” as it applies to a defense article
  • is extracted unabridged from technical documents directly relating to defense articles/project
  • Otherwise “appears” as though it might be technical data

• **For ITAR purposes only:** For technical data to be *excluded* from the ITAR, one would have to answer in the *affirmative*, that the information exists in the public domain.
Misc. Issues

• Additional Preventive Measures to take into consideration when dealing with ITAR projects or projects associated with EAR export controlled items (ECR Act):
  • Product Development and Marketing: new international and domestic military or defense projects and proposals should be reviewed by the Empowered Official (“EO”)
  • Contracts associated with ITAR projects and purchase orders should be reviewed by the EO in order to identify any ITAR clauses
  • When in doubt with a 3rd party supplier/vendor, ask whether their product is ITAR or export controlled under the EAR, and always obtain this in writing or confirm it in a follow-up email.
  • MIL-Standard products are not ITAR controlled, unless modified
• United Technology Corporation “lessons learned”: multimillion dollar settlement with DDTC was primarily due to the following errors: lack of internal processes/procedures and technical data/documents/information being **potentially accessible** by Foreign Nationals and violations as follows:
  
  • Unauthorized exports and re-exports, resulting from the failure to properly establish jurisdiction over BOTH defense articles and technical data. **Meaning**: they treated certain products and technology as ‘commercial’ when in fact it was ITAR
  
  • Unauthorized exports, resulting from the failure to exercise internal controls over technical data. **Meaning**: always follow a Technology Control Plan which addresses ITAR technical data and information
  
  • Failure to properly manage DDTC authorized agreements (i.e. export licenses, TAAs, MLAs). **Meaning**: attention to the provisos and license conditions is critical
Most often used definitions on ITAR Export Controls:

- 120.4: Commodity Jurisdiction
- 120.9: Defense Service
- 120.10: Technical Data
- 120.11: Public Domain
- 120.15 & 120.16: U.S. & Foreign Persons, including Defense Article
- 120.17: Export: Hardware, Technical Data, Services, and Significant Military Equipment (SME)
- 120.19: Reexport & Retransfer
- 120.41: Definition of Specially Designed and whether it’s an article of the USML or CCL. In addition, you should reference the EAR, under section 772.1
Quick Reference Guide

- Recordkeeping and Reporting Requirements can be found in:
  - 122.5: Maintenance of Records
  - 123.22(b)(3)(iii): Filing of Export Information
  - 123.26: Recordkeeping requirement for exemptions
  - 125.6: Certification requirements for exemptions

- Principal U.S. government Exemptions can be found in:
  - 126.4; 125.4(b)(1), (b)(3), and (b)(11)
Quick Reference Guide

• 22 CFR 120.9: Defense Services pertaining to defense articles, including the furnishing of assistance and/or training to foreign persons in the areas of:

  • Design, Development
  • Engineering, Modification, Destruction
  • Technical Data
  • Manufacture, Production, and Assembly
  • Operation, Processing
  • Testing, Repair, and Maintenance
  • Demilitarization (moving an item from USML to Commercial)
  • Use of a military item, including technology and support equipment
  • Technical Data
Thank you!

If you have any questions and/or are looking for membership please contact us at:

Global Trade & Supply Chain Institute (GTSCI™): www.gtsci.org

Email: Info@gtsci.org

Contact number: 630.234.3800

Toll Free Number: 855.534.3614