Bureau of Political-Military Affairs
Directorate of Defense Trade Controls
Office of Defense Trade Controls Compliance

International Traffic in Arms Regulations (ITAR)
Compliance Program Guidelines

The guidelines contained in this document are intended to provide an overview of an effective compliance program and an introduction to defense trade controls, including information on the laws and regulations the U.S. Department of State, Bureau of Political-Military Affairs, Directorate of Defense Trade Controls (DDTC), administers. These defense trade controls are contained in the Arms Export Control Act (AECA) (22 U.S.C. § 2751 *et seq*.) as amended, and the International Traffic in Arms Regulations (ITAR), Title 22 of the Code of Federal Regulations in parts 120-130, both of which are authoritative on defense trade controls. The guidelines contained in this document are not intended to serve as a basis for any registration or licensing decisions on the part of the public or DDTC. To the extent there is any discrepancy between these guidelines and either the AECA or the ITAR, the AECA and ITAR will prevail.

INTRODUCTION

This document contains information on the elements of an effective ITAR Compliance Program (ICP) and how to design and implement an ICP for organizations that manufacture, export, broker, or temporarily import defense articles and defense services described on the United States Munitions List (USML).

The purpose of an ICP is to establish robust policies and procedures to ensure that organizations and their staff who engage in ITAR-controlled activities do so in compliance with the ITAR, Title 22 of the Code of Federal Regulations in parts 120-130, issued pursuant to the Arms Export Control Act (AECA) (22 U.S.C. § 2751 *et seq*.), as amended. Operating an effective ICP helps organizations integrate ITAR requirements into their business and research processes and helps mitigate the risk of violating the regulations.

The elements in this document provide a foundation for an ICP's basic structure and function and are not intended to be exhaustive. The scope of ITAR activity in which different organizations engage varies substantially, and so ICPs should be tailored to address each organization's ITAR-controlled activities, risk factors, and size. Although this document describes elements of a compliance program it believes organizations should have and includes recommendations regarding what they should do, organizations for which those elements and recommendations are not relevant are not expected to include them in their ICP.

The elements in this document are specifically focused on assisting organizations developing a program to comply with the ITAR. Many organizations engage in activities that fall under the jurisdiction of multiple U.S. trade laws and regulations. Therefore, organizations should ensure their ICP functions effectively within the context of a holistic export trade compliance program.

DDTC has identified the elements below as critical for an effective ICP:

- Element 1: Management Commitment
- Element 2: DDTC Registration, Jurisdiction and Classification, Authorizations, and Other ITAR Activities
- Element 3: Recordkeeping
- Element 4: Reporting and Addressing Violations
- Element 5: Training
- Element 6: Risk Assessment

- Element 7: Audits and Compliance Monitoring
- Element 8: Export Compliance Manual and Templates

ELEMENT 1: MANAGEMENT COMMITMENT

A. Developing and Generating Support for a Culture of Compliance

Management commitment is one of the most important factors in creating a deep-rooted culture of ITAR compliance within organizations. While robust management commitment alone is insufficient to ensure compliance with all relevant U.S. export control laws and regulations, it is essential for fostering a proactive compliance posture.

Management includes not only senior management, but also managers at all levels within the organization, and the most important stance management can take to engender a culture of compliance is to lead by example. Through their words and actions, management should encourage compliance and should discourage the prioritization of business or other interests over compliance. Employees should have a high level of assurance that ITAR compliance is management's greatest priority in all export-related decisions. Management should communicate to employees that they are encouraged to raise questions or concerns about compliance and potential risk areas and employees will not experience retribution or retaliation if they do so. Employees should understand that ITAR compliance is everyone's responsibility within the organization.

To help generate support and buy-in among employees, management should incorporate compliance into employee performance plans and evaluations. Employees should be expected to think about and recommend ways to improve compliance and raise concerns when they see a possible problem, and their performance plans and evaluations should account for those expectations. Additionally, management should recognize and reward employees who speak up, even if the problem reported resulted in no specific confirmed violation, but perhaps lead to improving the organization's compliance procedures.

In addition, management should communicate to employees that export control violations will not be tolerated and may result in disciplinary action against the employee, regardless of the employee's position, title, or performance. Management should adopt clear disciplinary procedures and consequences for addressing compliance misconduct, should enforce them consistently across the organization, and should ensure that they are proportionate to the misconduct and appropriate to deter future misconduct.

information technology resources, and other resources to fulfill their responsibilities and implement an effective ICP. In assessing whether such resources are adequate, management should take account of the organization's size, scope of operations, and overall risk profile.

Export Compliance Management Commitment Statement

Another critical way to demonstrate strong management support for ITAR compliance is to have the Chief Executive Officer, President, or other senior executives personally sign an Export Compliance Management Commitment Statement that is communicated to employees through all appropriate channels, including in the opening pages of an ITAR Compliance Manual, on the corporate website, and through periodic email reminders to all employees. The organization should review and disseminate this statement at least annually for all employees and, as appropriate, all contractors to read and sign. The statement should:

- Underscore the organization's commitment to export compliance and providing sufficient resources to ensure compliance.
- Reference the role and function of the U.S. export control system and its importance in protecting the foreign policy and national security of the United States.
- Affirm that no export shall be made under any circumstances that violates or potentially violates the ITAR.
- Emphasize the importance of employees understanding the ITAR and its impact on their job functions. Employees should also understand specific risks of non-compliance regarding an organization's activities, technologies, and export destinations.
- Communicate the importance of routine export compliance monitoring and auditing.
- Stress the importance of and/or the requirement to report known or suspected violations to the organization's export compliance department anonymously or via an organization's compliance hotline.
- Reiterate that reporting known or suspected ITAR violations in good faith will not adversely affect employees.
- Reiterate that reporting known or suspected export violations will be used to measure job performance.
- Include the name and contact information of the personnel responsible for responding to ITAR compliance inquiries.

C. Organizing the Compliance Function Appropriately

Management is responsible for deciding where to locate compliance personnel within an organization's structure. This includes establishing organizational charts and developing descriptions of the organization's trade and export compliance functions and determining the extent to which the ICP is centralized. The organizational structure should clearly identify the following areas of authority:

- Who in management is responsible for overseeing the ICP?
- Who within the ICP is the point of contact regarding export compliance questions?
- Who within the ICP and/or business functions is responsible for investigating and identifying the root causes of ITAR violations?
- Who within the ICP and/or business functions is responsible for overseeing and implementing corrective actions?
- Who within the ICP is responsible for drafting, finalizing, and submitting export-related documents to DDTC?
- Who within the ICP is responsible for sending other communications regarding export compliance matters to DDTC, if necessary?
- Who is responsible for legal interpretation and guidance on internal export compliance matters?

Empowered Officials (EOs) typically handle at least some of the responsibilities listed above. As set forth in ITAR § 120.67, some of the primary attributes and responsibilities of an EO include, but are not limited to:

- Direct employment by an organization in a position having authority for policy or management within the organization.
- Written legal empowerment to sign license applications and other requests for approval on behalf of the organization.
- Understanding 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.
- Independent authority to:
    - Inquire into any aspect of a proposed export, temporary import, or brokering activity by the organization;
    - Verify the legality of the transaction and the accuracy of the information to be submitted to DDTC; and
    - Refuse to sign any license application or other request for approval

without prejudice or adverse recourse.

Management is responsible through training and hiring practices for ensuring that compliance personnel possess the requisite technical knowledge, expertise, and experience to effectively implement the ICP. Management should also ensure that compliance personnel, including the EO, are delegated sufficient authority and autonomy to implement the ICP, consistent with their responsibilities. Management should hold routine and periodic meetings with the EO to ensure that employees are following ITAR policies and procedures.

Business" for instructions on how to submit a Form DS-4076 electronically via DECCS. Please note that a supporting letter from the original equipment manufacturer (OEM) is generally required for CJ applications by persons other than the OEM.

DDTC Jurisdiction and Classification Suggestions

Organizations routinely disclose to DDTC ITAR violations resulting from improper jurisdiction and classification. To reduce the risk of these types of ITAR violations from occurring, DDTC recommends that organizations take the following actions:

- If any doubt exists regarding the proper jurisdiction or classification, err on the side of caution, and submit a CJ request to DDTC.
- Understand the form and fit of the articles, as well as the function and performance capability of the articles.
- Document the design and development process for new products and monitor and document modifications to existing products.
- Designate employees with the necessary technical expertise, e.g., engineers or program managers, and export controls personnel to perform jurisdiction and classification review functions.
- Establish formal written policies and procedures for reviewing and documenting jurisdiction and classification decisions.
- Develop a system of tracking and marking jurisdiction and classification determinations at the time – or as soon as possible after – commodities are manufactured.
- DDTC routinely updates USML categories, so organizations should consistently monitor these updates and adjust their internal jurisdiction and classification determinations accordingly.
- If a CJ request is pending, DDTC recommends treating the commodity as defense article or a defense service until DDTC issues the CJ determination.
- Keep records of all jurisdiction and classification decisions in a central location that can easily be accessed, reviewed, referred to, and updated.

C. Authorizations

DDTC authorization via a license or other approval is required prior to engaging in any ITAR-controlled export (see ITAR § 120.50), reexport (see ITAR § 120.51), retransfer (see ITAR § 120.52), temporary import (see ITAR 120.53), or brokering activities (see ITAR 129.2).

license is valid, e.g., change in freight forwarder, potential U.S. or foreign subcontractors involved in the transaction, or changes in the end use or end user.
- Reviewing for restrictions on parties to the transaction, including by screening through the Consolidated Screening List.
- Creating, submitting, tracking and disposition of licenses and other authorizations.
- Successfully implementing agreements (e.g., internal controls, technology control plans, identifying foreign person status, and employment status of meeting attendees).
- Communicating with all foreign parties to determine who will be involved in the transaction and their roles, e.g., recipients of services, providers, subcontractors.
- Working with foreign parties to understand if there will be dual or third-country national employees working on the proposed activities and how the foreign party will screen those individuals.
- Ensuring foreign parties have compliance safeguards in place to protect any technical data transferred under the agreements from unauthorized access.
- Protecting against unauthorized release of technical data to foreign entities and foreign employees.
- Recordkeeping and tracking the use of licenses and other approvals.
- Assessing all conditions that must be satisfied to qualify for use of any license exemption.
- Reviewing and approving use of license exemptions by appropriate compliance personnel.

DDTC Reexports, Retransfers, and General Correspondence Requests Suggestions

To reduce the risk of ITAR violations related to the reexport or retransfer of defense articles from occurring, DDTC recommends that organizations take the following actions:

- Establish policies and procedures for reviewing and obtaining authorization for reexports and retransfers.
- Establish policies and procedures for tracking and keeping records regarding export authorizations for reexports or retransfers.
- Ensure understanding of the difference between requesting an initial

See ITAR § 130.10 for a full list of the required information to be submitted in a report to DDTC.

DDTC Political Contributions, Fees, and Commissions Suggestions

To reduce the risk of ITAR part 130-related violations, DDTC recommends that organizations take the following actions:

- Understand whether you or your vendors are involved in paying political contributions, fees, or commissions.
- Understand what information needs to be asked of and received from your vendors.
- Establish policies and procedures for accurate and accessible recordkeeping of such political contributions, fees, or commissions.

G. Cybersecurity and Encryption

Although the ITAR does not explicitly require organizations to implement specific cyber security or encryption measures for the storage or transmission of technical data, cyber intrusion events, and the theft of technical data may result in unauthorized exports. Other U.S. Government agencies and programs, however, have specific cyber security requirements. DDTC expects organizations to take steps to protect their technical data from cyber intrusions and theft and consider carefully what cyber security solutions work most effectively for them.

Having specific policies, procedures, and tools for the encryption of technical data is a critical part of cyber security. Organizations should consider both how to encrypt the storage and transmission of technical data externally, including via cloud and other remote storage, and how to appropriately encrypt technical data on portable devices.

For further information on activities that are not exports, reexports, retransfers, or temporary imports related to the sending, taking, or storing of technical data, see ITAR § 120.54.

DDTC Cybersecurity and Encryption Suggestions

To reduce the risk of ITAR violations and improve cyber security measures, DDTC recommends that organizations take the following actions:

- Establish policies and procedures for recurring training on travel with

ELEMENT 3: RECORDKEEPING

A. ITAR Recordkeeping Requirements

The ITAR requires all registrants to maintain records regarding the manufacture, acquisition, and disposition of defense articles, including technical data; the provision of defense services; brokering activities; and information on political contributions, fees, and commissions furnished or obtained, pursuant to ITAR part 130. The ITAR requires that such records are:

- Reproducible in paper format, if digital;
- Legible and readable;
- Unaltered once recorded or, if altered, with any alterations properly recorded, including who made them and when;
- Readily accessible if digital images; and
- Maintained for a period of five years from the expiration of the license or other approval, to include exports using an exemption, or from the date of the transaction.

The following records must be maintained:

- License or other approval;
- License exemption;
- Technical data exports;
- Oral, visual, or electronic exports;
- Certain information related to special comprehensive export authorizations;
- Related to the Defense Trade Cooperation Treaty between the United States and Australia;
- Related to the Defense Trade Cooperation Treaty between the United States and the United Kingdom;
- Related to exemptions involving employees who are dual and third-country nationals;
- Related to voluntary disclosures;
- Brokering recordkeeping requirements; and
- Related to political contributions, fees, and commissions.

B. Establishing Recordkeeping Roles and Responsibilities

For each transaction or activity type, organizations should determine which records must be maintained pursuant to the ITAR's recordkeeping requirements and develop a list of those records. Based on the list, organizations should develop written policies and procedures to ensure that these records are maintained properly. Such written policies and procedures should clearly articulate who within the organization is responsible for the various recordkeeping responsibilities. They should also include, but are not limited to, the following:

- Establishing policies and procedures for recordkeeping and for timely destruction of records, or their maintenance past required dates where relevant to ongoing matters, including, e.g., disclosures to DDTC.
- Determining how and where records will be maintained.
- Determining how and when records will be inspected for completeness, accuracy, and quality.
- Developing and maintaining processes for managing records by identifying classes of records and logs of record creators and keepers. If appropriate, maintain a detailed log or index of records of more sensitive records.
- Establishing record-retention requirements for emails, contracts with freight forwarders, brokers, and distributors, and other records.
- Creating recordkeeping redundancies, such as backup IT servers, where appropriate.
- Ensuring that recordkeeping methods do not allow for unrecorded alterations.

Organizations should clearly allocate responsibilities for recordkeeping among personnel in business units, records management, information technology, system administration, and other offices within the organization. Organizations should also identify personnel designated with recordkeeping responsibilities and ensure that oversight of such personnel exists to confirm they are adequately performing their recordkeeping responsibilities. Finally, organizations should develop ongoing training and awareness programs to ensure personnel involved in the recordkeeping process can effectively comply with ITAR recordkeeping requirements.

Organizations should ensure that every employee involved in ITAR-controlled activities is trained on how to:

- Identify and preserve relevant records;
- Share and retrieve relevant records;
- Properly dispose of hard drives, thumb drives, and other portable media devices on which records are stored; and
- Maintain a backup system for preserving relevant records.

Organizations should ensure that all required records are captured and correctly filed to allow for efficient search and retrieval by conducting periodic audits on the recordkeeping system. Management should also communicate the importance of recordkeeping to all employees and ensure that sufficient resources exist to allow employees to perform their recordkeeping duties.

C. **Recordkeeping and Technology Control Plans**

Organizations that possess technical data and either employ foreign persons or conduct frequent meetings with foreign persons should consider creating and maintaining a Technology Control Plan (TCP). A TCP sets out an organization's policies and procedures for protecting technical data and includes the following elements:

- Management commitment;
- Personnel-screening procedures;
- A physical security plan;
- An information security plan; and
- Training and awareness programs.

A TCP can help reduce the risk of inadvertent ITAR violations through telephone, facsimile, electronic mail, social media, or in-person exchanges, particularly during informal technical exchanges with foreign persons. Organizations can implement a TCP in several ways, including for an organization, a location, or a defined project. Organizations should incorporate TCP requirements into their ICP and ensure impacted employees are aware of specific TCP requirements.

TCPs should also address how organizations will keep records regarding foreign-person visitors at their facilities. For example, organizations could document all foreign person visits and any special conditions attached to the visits. Such records should indicate:

- The visitor's name and nationality or nationalities;
- The name and affiliation of the organization represented;
- The date of the visit;
- Persons, physical areas, and room numbers visited;
- Purpose of the visit with specific emphasis on products or services discussed; and
- A summary of the visit, including any issues or circumstances of note.

In addition to documenting these interactions with foreign persons, TCPs should address how organizations will collect and store human resources records for foreign person employees involved in ITAR-controlled activities.

Instituting these recordkeeping practices through a TCP may also have the additional benefit of increasing awareness among employees that certain types of interactions with foreign persons create risk areas for potential ITAR violations, thereby minimizing the risk of an inadvertent violation.

D. Recordkeeping and Voluntary Disclosures

Establishing and implementing robust recordkeeping policies and procedures are foundational to establishing a strong ICP. In the event an ITAR violation occurs, thorough documentation is essential for submitting a voluntary disclosure to DDTC that meets the requirements in ITAR part 127. Without strong recordkeeping policies and procedures, organizations may find it difficult to provide all information and documentation described in ITAR part 127 for voluntary disclosures and to respond to any questions that DDTC may have regarding the violation. A failure to maintain or produce relevant records in certain circumstances constitutes an ITAR violation.

DDTC Recordkeeping Suggestions

DDTC recommends that organizations identify and implement best practices for recordkeeping including, but not limited to, the following:

- In the event records include copies of exported technical data, ensuring the records are properly secured, including through encryption for digital records, to prevent unauthorized access.
- Before employees depart an organization, ensuring any records subject to ITAR recordkeeping requirements they possess are identified and

preserved.

- Evaluating the physical storage site and control procedures for disposal of records to minimize the risk of losing records or failing to properly secure technical data.
- Implementing a backup system for electronic storage and implementing measures that will assist in the recovery of information and other electronic communications on computer systems if the primary computer system fails.
- Maintaining thorough records of non-disclosure agreements and screenings involving dual and third-country national employees, as appropriate.
- Maintaining copies of relevant records that exist on a third-party organization's IT systems, such as copies of shipping records from freight forwarders, disclosures submitted by outside counsel, or licensing information.
- Acquiring or developing a central IT storage system or database for relevant records.
- For offsite record storage and destruction, reviewing the contractual terms to ensure that ITAR-controlled technical data is protected.
- Periodically reevaluating the efficacy of recordkeeping policies and procedures.
- Retaining records of any disclosures and any supporting documentation.
- Developing and implementing a system to document all communications with DDTC officials, including through outside counsel, involving ITAR-related matters, which may help ensure continuity and consistency in an organization's export compliance functions.

- Incorporate ITAR compliance into employee performance plans and evaluations.
- Implement reporting procedures for organizations to voluntarily disclose ITAR violations to DDTC and also to mandatorily disclose ITAR violations involving proscribed destinations pursuant to ITAR § 126.1(e)(2).

B. Establish Policies and Procedures for Investigating ITAR Violations and Implementing Corrective Actions

Organizations should draft, periodically update, and make available to employees policies and procedures for investigating and addressing potential ITAR violations that are reported or otherwise detected. These policies and procedures should cover, among other things, how the organization will:

- Determine when to investigate suspected violations.
- Document the information reported, detected, or otherwise obtained as part of the investigation.
- Analyze the root causes of any ITAR violations.
- Draft a report describing the outcome of the investigation and the recommended corrective actions, including any recommended disciplinary measures.
- Present the report to and brief management.
- Document management's response to the report and whether management approved the recommended corrective actions.
- Implement the corrective actions and document the implementation of the corrective actions, including who implemented them and how.
- Monitor the corrective actions to ensure they remain fully implemented and are working properly over time.
- Report back to management after the approved corrective actions are implemented.

Organizations should use personnel qualified to conduct timely and properly scoped investigations of ITAR violations and should ensure that such personnel have adequate resources and funding. Organizations should ensure that investigations are independent, objective, thorough, and properly documented. Organizations should consult in-house and outside ITAR experts, where appropriate, during or after an investigation. Management's response to such investigations should reflect the critical importance of ITAR compliance, including

by recognizing and rewarding employees who report suspected ITAR violations. Organizations should also continuously update their compliance programs to incorporate changes to the ITAR and lessons learned from past violations.

C. Establish Policies and Procedures for Properly Submitting Voluntary Disclosures to DDTC

Organizations should develop written policies and procedures for disclosing ITAR violations to DDTC. Organization should ensure that these policies and procedures are fully consistent with all requirements set forth in ITAR § 127.12 for voluntary disclosures.

DDTC strongly encourages organizations to disclose suspected ITAR violations promptly. DDTC may consider a voluntary disclosure pursuant to ITAR § 127.12 as a mitigating factor in determining the administrative penalties, if any, that should be imposed. However, for a disclosure to be considered "voluntary" for purposes of ITAR § 127.12, it must be made prior to the time the U.S. Government becomes aware of either the same or substantially similar information from another source and initiates an investigation or inquiry of its own. Accordingly, an organization that wishes to obtain the significant mitigation credit for voluntary disclosures should disclose any violations as quickly as possible to DDTC. Failure to voluntarily disclose a violation may result in circumstances detrimental to U.S. national security and foreign policy interests and will be an adverse factor in determining the appropriate disposition of the matter. DDTC reviews and closes most voluntary disclosures without any administrative action.

Organizations should submit an initial notification to DDTC pursuant to ITAR § 127.12. If they have not yet identified all the required information under ITAR § 127.12, then they may subsequently provide a full disclosure within 60 days. Organizations that request extensions for the submission of a full disclosure are encouraged to do so as far in advance of the 60-day deadline as possible. If organizations confirm that no ITAR violation occurred after submitting an initial notification, then they may request a withdrawal of their notification.

Organizations should ensure that voluntary disclosure submissions contain all the required information, provide appropriate documentation, and enclose the certification required in ITAR § 127.12(e). Consistent with these requirements, voluntary disclosures should demonstrate that the organization conducted a thorough root cause analysis to determine why ITAR violations occurred, including by identifying whether the violations are systemic.

In the event the organization's policies and procedures should have prevented a violation, the disclosure should identify the business units that had ownership of the specific policies and procedures at issue and explain how those units have been held accountable. Voluntary disclosures should also demonstrate that the organization developed and has either implemented or has plans to implement corrective actions that address the root causes and prevent the recurrence of similar violations.

D. Communicate Potential Consequences of ITAR Violations to Employees

Management should ensure that all employees understand their legal obligations under the AECA and ITAR, as well as consequences for violating those obligations. Management should make available educational materials and post visual reminders to all relevant employees that underscore the following:

- ITAR controls ensure that commercial exports of defense articles and defense services advance U.S. national security and foreign policy objectives. Criminal and civil penalties for violating the ITAR are severe because such violations may harm U.S. national security and foreign policy.
- Criminal convictions for willful ITAR violations can result in a maximum criminal penalty of $1,000,000 per violation, imprisonment of up to 20 years per violation, or both.
- Organizations and/or individuals criminally convicted of ITAR violations will also be subject to statutory debarment that renders them ineligible to participate directly or indirectly in defense trade for a specified period.
- Civil penalties for ITAR violations can result in a fine of more than $1,200,000 per violation, and that amount increases annually to adjust for inflation. DDTC imposes civil penalties based on strict liability unless otherwise specified in the text of the ITAR. This means that organizations and/or individuals may be held civilly liable for ITAR violations even if they did not know or have reason to know that they were violating the ITAR.
- Any ITAR violation, regardless of intent, may trigger administrative debarment if the violation provides DDTC with a reasonable basis to believe that the violator cannot be relied upon to comply with the ITAR in the future.
- Administrative settlements typically include the execution of a Consent

Agreement under which the respondent is required to institute enhanced compliance measures for a period of two to four years. Instituting these enhanced compliance measures is typically time and resource intensive for most organizations.

- Administrative settlements are posted publicly on DDTC's website, which may result in both negative publicity and reputational damage for the respondent.

Management should also ensure that employees understand other potential consequences, including possible disciplinary actions, for ITAR violations within an organization.

ELEMENT 5: ITAR TRAINING

A. ITAR Training Programs

ITAR Training Programs Basics

ITAR training programs should be tailored, dynamic, up-to-date, and adequately resourced. They should also clearly identify the job-specific export control responsibilities for all employees. Programs should allot sufficient time for employees to complete their training, and they should offer training on a recurring basis, at a minimum annually. Organizations should maintain accurate training records to verify that employees have completed all relevant compliance-related training sessions. In addition to offering formal ITAR training sessions on a recurring basis, organizations should make available ITAR training resources that employees may consult at any time.

Tailoring ITAR Training Programs

Organizations should ensure that ITAR training programs are tailored to address their specific compliance risks. Some of the risks that organizations should consider when designing an ITAR training program include the following and discussed in detail in Element 6 of this document:

- The nature and scope of their defense articles and defense services being provided;
- The parent, subsidiaries, affiliates, suppliers, customers, clients, business partners and other relevant parties with which they interact, directly or indirectly;
- The geographic regions in which they operate; and
- The duties and responsibilities of the employees and other personnel being trained.

Implementing Dynamic and Up-to-Date ITAR Training Programs

ITAR training programs should be dynamic and reviewed periodically for updates and revisions based on changes in the organization's commodities and their end uses and end users, as well as any changes to the ITAR or guidance from DDTC. Organizations should monitor the *Federal Register* and DDTC's website routinely for ITAR-related updates that should be integrated into recurring training sessions. Organizations should also establish a mechanism to disseminate ITAR-related

updates to personnel in a timely manner in between training sessions, such as through organization-wide email updates.

Organizations should also stay informed of export compliance best practices and monitor relevant publications that may describe export compliance enhancements and lessons learned from export control violations by other organizations. For instance, upon learning of an ITAR violation or "close call" within one's own organization, or identifying vulnerabilities in the organization's ICP, or obtaining a negative testing result or audit finding, organizations should use such incidents to provide specific training to relevant personnel within the organization, in addition to taking corrective action.

Hiring Knowledgeable and Experienced Trainers

An effective ITAR training program requires knowledgeable, experienced trainers. Organizations should ensure their trainers are subject matter experts on the ITAR who keep well-informed regarding the latest changes to the ITAR, guidance from DDTC, and industry best practices. Internal trainers should pursue their own continuing education to ensure that they remain subject matter experts in the field.

B. Tiered Training Based on Each Employee's Functions

Organizations should adopt a tiered ITAR training program based on the responsibilities of each employee and other personnel within the organization. Organizations should tailor their ITAR programs as specifically as possible to help employees and other personnel understand their specific export control responsibilities in light of the organization's risk profile. Organizations should provide their employees and other personnel with different levels and types of ITAR training depending on the knowledge and skills needed to perform their job functions and the compliance risks that arise in each position. For example, training programs could be divided into four tiers, directed at four categories of positions within the organization, as reflected in the pyramid diagram above and described below. Smaller organizations may adopt this tiered approach or

provide comprehensive ITAR training to all personnel.

Tier 1: General ITAR Training for All Personnel

For the first and bottom tier – all personnel – training should cover the basics of export controls and should be comprehensible for a broad audience with little or no background in export controls or the ITAR. Generally, this level of training is provided to all personnel within organizations. Organizations should provide the training to all new hires and contractors during the onboarding process and then reinforce that training through periodic education and awareness activities to those with little or no exposure to exports.

Tier 1 training should provide all personnel within the organization a basic understanding of the ITAR and a clear understanding of everyone's shared export compliance responsibilities within the organization. Tier 1 training should, at a minimum, cover the following topics:

- Basic ITAR overview, including:
    - Regulated activities;
    - Key ITAR definitions, including export, foreign person, technical data, defense service, and defense article, and provide real world examples specific to the organization's business;
    - Licenses or other approvals; and
    - How ITAR violations occur.
- Overview of the organization's ICP
- Recordkeeping procedures
- Red flags specific to the organization's business
- Screening requirements
- Practical advice and case studies to address real-life scenarios
- Company-specific risk profile and high-risk compliance areas
- Reporting ITAR violations
- Potential consequences of violating the ITAR:
    - Strict liability for civil violations;
    - Civil and/or criminal monetary penalties;
    - Imprisonment for criminal violations; and
    - Debarment
- Enhancing ITAR-compliance processes
- Organization charts and contact information for key export compliance personnel, Empowered Officials, and other relevant personnel.

Tier 2: Senior Management

For the second tier – senior management – training should be more detailed and include more than just the basics of export controls. Senior management must have a thorough understanding of export controls to properly comprehend the compliance risks associated with the organization's activities and risk profile. Organizations with a Board of Directors or a Board of Trustees should conduct the same type of top-level briefing for them as well.

Tier 2 training should provide senior management with an intermediate level of understanding of the ITAR and a clear understanding of the critical role senior management plays in ITAR compliance within the organization. In addition to topics covered in Tier 1, Tier 2 training should, at minimum, include an intermediate ITAR overview and the following topics:

- Detailed description of the organization's ICP;
- The importance of communicating management commitment to complying with U.S. export controls;
- Allocating appropriate resources and hiring adequate staff to ensure ITAR compliance;
- Creating and maintaining a culture of ITAR compliance within the organization; and
- A detailed description of the potential consequences of violating the ITAR.

Tier 3: Positions with Export Functions

The specific personnel that fall in the third tier – positions with export functions – will vary from one organization to another, depending on the organization's activities. For most companies, it will likely include program management, technical, and/or engineering personnel with access to ITAR-controlled defense articles, shipping and receiving, supply chain, business development, human resources, and IT.

For universities, it will likely include administrative staff, researchers, faculty and/or principal investigators involved in activities, including, e.g., contracts and grants, product development, and research labs, as well visiting foreign students and scholars participating in controlled research. Organizations should provide more detailed and targeted ITAR training to such personnel, at a minimum, on an annual

basis.

Tier 3 training should provide relevant employees with export functions with an advanced- level understanding of the ITAR and their significant export compliance responsibilities within the organization. In addition to topics covered in Tiers 1 and 2, as appropriate, Tier 3 training should, at minimum, cover the following additional topics:

- How to handle technical data, including marking procedures;
- Deemed exports;
- Jurisdiction and classification;
- Pertinent USML Categories;
- Export authorization approval process;
- License conditions and exceptions;
- Exemptions applicable to business;
- Agreement and license types;
- Non-Disclosure Agreements;
- Recordkeeping; and
- Targeted training to individual roles.

Tier 4: Export Compliance Team

The final and top tier of the training program comprises the export compliance team, including the EO, export compliance manager, compliance supporting staff, and legal counsel advising on export compliance issues. Training for this group should be thorough and detailed and include not only the organization's ICP but training on all export control regulations that could impact the organization's exporting activities.

Compliance managers and their team also need to receive training on potential future needs for their organization, including mergers, acquisitions, or divestitures, development of a new product line, expansion into a new region of the globe, or new developments in U.S. foreign policy.

Tier 4 training should provide the export compliance team with an expert-level understanding of the ITAR and their export compliance responsibilities within the organization. In addition to topics covered in Tiers 1, 2,
and 3, as appropriate, Tier 4 training should, at minimum, cover the following additional topics:

- Establishing and maintaining ITAR policies and procedures, including the ICP.
- Obtaining and tracking the use of the organization's licenses and other approvals.
- Establishing TCPs.
- Other detailed training in specific areas of export regulations relevant to the organization, such as:
    - Export document preparation,
    - Country-specific diversion risks,
    - Recordkeeping requirements, and
    - Self-assessments and internal audits.
- Attending DDTC seminars and other outside training programs as appropriate.

Employee Accountability

Organizations should include ITAR training as a requirement in performance plans and reviews and ensure that employees and other personnel complete their ITAR training on time. Organizations should also hold employees and other personnel accountable for both completing their ITAR training in a timely manner and for completing refresher training to retain their knowledge from their initial training. Further, at the end of each ITAR training session, organizations should test employees on the materials and issue a certificate of completion when they successfully complete the test.

an organization begins exporting to a new geographic area or opens a new foreign office, the organization should update its risk assessment accordingly. Updating the risk assessment is also important following mergers, acquisitions, and divestitures, particularly if the company merges or acquires foreign persons. In addition, organizations should update their risk assessment if they discover new or evolving ITAR compliance risks through audit findings, ITAR violations or "close calls," employee feedback, or any other sources.

Organizations may internally design, update, and conduct the ITAR risk assessment, or they may retain outside ITAR experts to do so. Organizations should ensure that their original risk assessments and any updates, as well as any changes to ICPs because of their risk assessments, are fully documented and preserved. DDTC recommends examining the Sample Audit Checklists in Element 7 to help assess and determine possible risk factors.

Frequency of ITAR Risk Assessments

Organization should periodically review risk assessments to determine whether its risks are properly addressed. Periodic risk assessments will depend on specific circumstances and how quickly risks change. There is no one-size-fits-all approach for updating risk assessments, but organizations should ensure that the frequency is adequate to accurately account for the potential ITAR compliance risks at any given time. For example, the organization may decide to conduct a company-wide risk assessment every year or perform targeted risk assessments focused on certain risk areas on an ad-hoc basis throughout the year.

Prioritizing and Mitigating ITAR Compliance Risks

After performing their ITAR risk assessments, organizations should analyze and prioritize those risks based on all relevant factors, including the likelihood that such risks would result in ITAR violations. Organizations should then integrate their risk-based analysis and prioritization into their ICPs and allocate resources as appropriate to mitigate those risks.

B. Addressing Common ITAR Risk Areas

This section identifies some common risk areas for purposes of conducting ITAR risk assessments and developing and updating ICPs. As described above, ITAR compliance risks may vary across organizations. Organizations have frequently identified risks in the following areas:

result from organizations not adequately securing their inventory of defense articles and not tracking them appropriately once exported.

See DDTC's website for the DDTC ITAR Risk Matrix, and supplementing University-specific Risk Matrix, that outline important areas of focus.

ELEMENT 7: AUDITS & COMPLIANCE MONITORING

A. Audits

Comprehensive, independent, and objective audits, performed regularly, assist organizations in determining the effectiveness of their ICP. Such audits allow organizations to identify deficiencies in their ICP and remediate them.

Audit Personnel

Organizations should assemble an internal team or, as appropriate, hire external third parties to conduct periodic ITAR compliance audits. If the organization already has an auditing team, it should incorporate ITAR policies and procedures with corporate audits. Auditors, whether internal or external, should determine the appropriate type and scope of the audit. Organizations should ensure their auditors have sufficient:

- Qualifications, technical knowledge, strong ITAR expertise, and sufficient resources to conduct the audit;
- Authority to ensure employees comply with audit-related requests for information;
- Independence from the audited activities; and
- Autonomy and independence from management, including direct access to any relevant employees, the board of directors, and/or the board's audit committee.

Audit Methodology

Audits should consist of:

- Interviews with relevant functional area personnel, as well as the compliance team and senior management, as appropriate;
- Document collection and review;
- Access to IT systems; and
- Site visits, as appropriate.

Auditors should maintain a detailed log to track the progress of documents requested and obtained, interviews requested and completed, and sites visited. The auditors should coordinate all interviews with the organization's compliance

department, as appropriate. The audit team should review all documents provided by the relevant business units in the development of checklists to be used when conducting the interviews and site visits. See Section C below for examples of such checklists.

Types of Audits

Different types of audits serve different purposes, and organizations should develop, as appropriate, an audit strategy, utilizing the different types of audits listed below, that is right for their circumstances.

- Functional-Level Audits: functional-level audits look at distinct areas of compliance programs, e.g., recordkeeping or shipping procedures. This audit type can help identify risk areas at an early stage and provide an opportunity to correct any deficiencies. Functional-level audits should be conducted more frequently than program-level audits because they are smaller in scale.
- Program-Level Audits: at the program-level, organizations should conduct internal audits as periodically as appropriate. Program-level audits should include both a review of all export policies and procedures and an assessment of whether each business unit implemented such policies and procedures.
- External Audits: external audits can provide an unbiased, third-party evaluation of an organization's overall compliance program and practices. Organizations should consider the use of an outside auditor periodically, as appropriate.

Audits in the Context of Mergers, Acquisitions, and Divestitures

Audits may be appropriate when mergers, acquisitions, and divestitures (MAD) occur. Pursuant to ITAR part 122, DDTC registrants must notify DDTC within specific timeframes regarding certain changes in registration, including ownership and legal organizational structure. Many of these notice requirements arise during the pre- and post-closing processes of MAD transactions.

Acquiring organizations should conduct due diligence reviews of target organizations that engage in ITAR-controlled activities. Due diligence reviews should assess the effectiveness of the target organization's ITAR compliance program and identify potential past ITAR violations. In the event such ITAR violations have not already been reported to DDTC, the target organization or the acquiring organization are strongly encouraged to submit a voluntary disclosure prior to or immediately after closing, as appropriate.

The acquiring organization should conduct an audit after closing the merger, acquisition, or divestiture. The appropriate scope of any post-closing audit will vary depending upon the circumstances. If the acquiring organization uncovers numerous unresolved compliance issues in its pre- closing due diligence, an in-depth audit may be appropriate. If, on the other hand, the target organization had a robust compliance program and provided documentation of regular audits and remedial actions, the acquiring organization may choose to perform a functional audit instead.

Acquiring organizations should ensure that any continuing ITAR violations by the acquired organization identified through the post-acquisition audit are stopped and remediated. Organizations should follow the relevant procedures in ITAR § 127.12 to investigate and voluntarily disclose the violations to DDTC.

Sharing Audit Findings and Following Up

After the auditors complete their interviews, document collection and review, and site visits, they should write a draft audit report. The draft audit report should include an executive summary, findings and recommendations, and appendices that explain the methodology, including the interviews conducted, documents reviewed, and sites visited. Prior to finalizing the audit report, the auditors should share their findings and recommendations with the relevant business units to correct any inaccuracies. After making any final modifications, auditors should brief senior management on the audit findings and recommendations.
Organizations should ensure the final audit report is provided to all relevant business units, as well as senior management. Organizations should maintain audit reports for at least five years.

If an audit report includes recommendations for revisions to procedures or corrective actions, organizations should include specific timetables and an implementation plan for management to approve. Organizations should continue to track the progress of corrective actions until they are completed. Once corrective actions are completed, organizations should prepare an additional report to management, and compliance personnel should confirm that each corrective action has been fully implemented.

Each vulnerability or violation identified in an audit is an opportunity for organizations to improve their ICP. Organizations should incorporate these lessons learned into training programs and their ICP in order to share them across business

units and functions. Organizations should also actively plan to remediate deficiencies in their ICPs that audit findings identify.

B. Compliance Monitoring

In addition to conducting periodic audits, organizations should regularly review their ICPs and amend their ITAR compliance policies and procedures as appropriate in response to:

- Any changes to the ITAR or DDTC guidance;
- Export compliance best practices and lessons learned from export control violations by other organizations;
- Lessons learned from any ITAR violations or "close calls" within the organization;
- Vulnerabilities identified in the organization's ICP, or negative testing results or audit findings; and/or
- Changes to an organization's ITAR risk factors, including where such risk factors have changed because of a merger, acquisition, and/or divestiture, or where there are changes to the organization's product line, services, or customers.

C. Sample Audit Checklists

The following are sample checklists that auditors should further develop before conducting an audit. Auditors should use these sample checklists to formulate document requests and interview questions for employees within the relevant functional areas of organizations. These sample checklists are not intended to be exhaustive, and they may not all be applicable to every organization. Auditors should customize checklists based on relevant factors, including an organization's specific activities and risk profile.

Management

- Has senior management issued a formal statement clearly communicating your organization's commitment to compliance with U.S. export control laws and regulations?
    - Does this statement include contact information for the person and Empowered Official primarily responsible for your organization's export compliance?

    - Is this statement easily accessible online or in print?
    - Has this statement been distributed to all employees whose work is impacted by export regulations?
    - Are employees whose work is impacted by export regulations required to sign an acknowledgment that they understand the organization's obligation to comply with U.S. export laws and its commitment to compliance?
    - Does your management assess ITAR compliance resource needs at least on an annual basis?
    - Has senior management communicated its commitment to compliance directly to those in leadership/authority positions, particularly business leads over the areas of the organization where export-controlled work is performed?
- Has your organization drafted, implemented, and disseminated written policies and procedures regarding export trade compliance?
    - Are these policies and procedures widely disseminated and readily accessible throughout your organization?
    - Does your organization ensure that the policies and procedures are followed?
    - Does your organization make available to all employees an organizational chart that clearly identifies personnel with authority over export control matters?
- How does the trade compliance office support your organization's different divisions in general and management in particular?
    - How many trade compliance personnel do you have on staff?
    - Do you believe the trade compliance function is adequately staffed to support your organization?
    - To whom does the trade compliance function report?
    - Do trade compliance personnel participate in staff meetings?
    - Are trade compliance staff integrated into business development decisions?

Trade Compliance

- Does the trade compliance function have sufficient support from management?
- Is trade compliance your primary area of responsibility? Do you have any other responsibilities within your organization?
    - Who is your backup when you are out of the office? Is that person

properly trained, and do they have the authority to act on your behalf?

- Does your organization provide tailored training for different functional areas, e.g., program management, business development, contracts, procurement, etc.?
    - How often and what type of training do trade control personnel receive annually?
    - Who is responsible for export control training?
- Does the trade compliance office routinely conduct risk assessments for the organization?
    - Have you determined areas of your organization that currently perform or are likely to perform ITAR-related activities?
    - Have you identified and implemented measures to address risk areas? If so, have you conducted an inventory of these areas to confirm whether they currently contain or are likely to receive or develop any defense articles, defense services or technical data?
- How does your organization classify its commodities?
- Does your organization maintain a product/technology matrix with USML categories? If so, how and by whom is the matrix maintained and updated?
- What processes are in place for reporting potential ITAR violations?
    - Does a "hotline" within the organization exist where employees can report potential violations, including anonymously?
    - Does management support investigations into potential violations? Is there support from management to hold personnel responsible for violations?
    - Who is responsible for investigating potential violations? If outside counsel is involved, is the Empowered Official also involved in the review and findings?
    - What process is used to ensure corrective actions, if any, are put in place and verified? Who is responsible for this action?
    - Does the Empowered Official have the authority and backing from management to stop any actions that may lead to a violation?
- Do you have a system/process in place to assess, review, and identify areas where a license, exemption, or other approval will be required?
    - What is the volume of licensing activity in each business unit?
    - Who determines whether a license is needed from DDTC?
    - Who is responsible for submitting export license requests to the DDTC?

    - How is party screening performed and who is responsible for this process?
    - What are the procedures for responding to negative/positive screening responses?
    - When a license or other approval is received, explain the process for implementing the authorization within your organization's divisions, e.g., how do you ensure that licenses are properly decremented and that temporary exports are returned? Who is responsible for meeting any conditions of approvals?
    - Explain how you track licenses, agreements, and other approvals to ensure you properly close them out, seek a replacement, or request an extension for an authorization.
    - How do you track the release of technical data via telephone, fax, email, hand carry or other means? How do you document these releases to authorized foreign person employees?
    - How often does the organization's trade compliance office perform audits on licenses and other authorizations? What percentage (random, 5-10%, 50%, or 100%) is used when conducting such audits? Where are the results of the audits stored?
    - Do policies and procedures exist regarding the recordkeeping and reporting requirements under the ITAR and are those policies and procedures readily available to employees?
    - Who ensures that employees are complying with ITAR recordkeeping and reporting requirements, as well as whether personnel are complying with our organization's policies and procedures?
- Does your organization verify that suppliers are able to properly handle ITAR-controlled defense articles and defense services, including technical data?
    - Do your suppliers employ foreign persons?
    - Do your suppliers always provide an export classification of the parts being procured? If not, the organization may want to obtain the proper classification of suppliers' parts.
    - Do you have a supplier due diligence process?
    - If you provide ITAR-controlled technical data to suppliers, do you consistently identify defense articles, including technical data, as such? Do you include markings on the technical data itself and on packing materials, emails, etc.? Do you ensure that suppliers understand their obligations under the ITAR not to export,

reexport, or retransfer that technical data without first obtaining DDTC approval?
    - Do your terms and conditions include trade controls related requirements such as compliance with the ITAR?
- Are trade compliance personnel invited to business development meetings so that they can properly anticipate and prepare for business pursuits that may require authorizations from DDTC in the future?
- Are engineering or business development personnel aware that a license is needed to export technical data or provide defense services to foreign customers?
    - If not, what level of training is provided to business development personnel prior to meeting with a foreign customer.
- Are trade compliance personnel aware of meetings with foreign customers concerning ITAR-controlled programs?
    - What is the process for approving any international travel? Are trade compliance personnel aware of all such travel?
    - Is export compliance training provided prior to any international travel?
    - Does your organization have a mobile device (laptop and hand-held devices) policy? Are employees trained on the appropriate use of such devices when traveling abroad?
    - What policy is in place to address hand-carry of defense articles outside of the U.S.? Who is responsible for overseeing this process and what measures are in place to control this type of export?

Program Management / Principal Investigators

- What training have you received regarding export compliance, and how often is it repeated?
    - Do you know whom to contact if you have any questions regarding export compliance?
- What procedures exist for approving international travel?
- What procedures exist for safeguarding technical data or other proprietary information on mobile devices while traveling internationally?
- What procedures exist for approving what information may be shared during meetings with foreign nationals, regardless of the location, domestic or internally?

- How do you comply with the terms of any export license or other approvals? Who is ultimately responsible for managing authorizations?
- How do you coordinate with the shipping and receiving department regarding exports and temporary imports of ITAR-controlled defense articles?
- What is the process for repair and return of parts? How is this coordinated with the various functional areas of the business unit and customers?
- Does your organization have a system to capture and track all exports, including technical data under licenses or other approvals?
    - How is this coordinated with the trade compliance team?
- What is the process for determining when a license is required? If doubts exist, who do you contact?
- Is the trade compliance office available to assist and provide you and your office with timely and sound advice?
- What is the process for hosting foreign persons to your facility.

Human Resources

- What is your organization's process for hiring a foreign person?
    - When an internal request is made to hire a foreign person, does human resources (HR) verify whether that person will have access to controlled data or any manufacturing processes?
    - Does HR screen potential applicants before they hired? How do they screen?
    - Once a potential foreign person hire is screened, does HR share the results with the office over trade compliance before extending an employment offer?
    - Is proof of the U.S.-person status verified at the time of hiring?
    - How are foreign person employees identified within your organization (special badge, IT, etc.)?
    - Are foreign person employees required to sign non-disclosure agreements?
    - Does your organization hire from third-party vendors, e.g., a temp agency? If so, how are nationalities of the persons hired confirmed?
    - Does your organization hire contractors that employ foreign persons? If so, how is that process conducted and coordinated?
- If foreign persons are hired, how does HR coordinate the hiring with the

trade compliance office? When is the process started?

- Does the trade compliance office include HR in the export compliance training module, and, if so, how is HR's role characterized?
- Is there a process in place between HR and the trade compliance office and/or program management for obtaining a license or other authorization and, if needed, any renewals necessary for the continued employment of a foreign person employee?
- If a foreign person is relocated to another location/program within your organization, how is HR/trade compliance office notified? What are the procedures for handling the transfer process?

- If a foreign person employee is terminated, does HR coordinate with trade compliance office, and, if so, in what manner?

Business Development / Sales

- In general, how does Business Development (BD) handle potential opportunities outside the United States, and how does BD coordinate with the trade compliance office?
  - Does BD receive tailored export control training? Who is BD's POC within the trade compliance office?
  - For international proposals, how would you assess BD's knowledge and training regarding whether export authorization is necessary?
  - At what point is the trade compliance office consulted and brought into the process when dealing in international opportunities or proposals?
  - Is the trade compliance office consulted in the early stages of internal opportunities?
  - What procedures exist to screen potential business opportunities (parties)? How do you coordinate screening with the trade compliance office? If you obtain a negative result, who makes the final call?
  - Does your organization use any international consultants? If so, how is this coordinated and controlled?
  - What processes exist for determining whether any BD activity requires reporting of fees or commissions pursuant to ITAR part 130, and who is responsible for filing those reports?
- What is the process for attending a general trade show? How does BD

coordinate with the trade compliance office for trade shows?
    - Does BD think of the trade compliance office as a partner in planning for participation in trade shows?
    - Does export compliance provide accurate and timely guidance to BD in advance of trade shows?
    - If controlled technical data or a mockup or model are used at a trade show, how does BD coordinate the licensing requirements with the trade compliance office?
    - Who is responsible for protecting and securing defense articles at trade shows?
    - Is there a process for determining what is considered public domain information that may be used at trade shows? Who and how is that determination made? Is such material appropriately marked?
    - Is BD aware of and does it understand how to obtain authorization to designate controlled data into the public domain?
- If operating under a license, how is the license is implemented and how are its conditions of approval met?
- What is the policy for BD personnel traveling overseas with mobile devices? Please explain how this is coordinated with IT and the trade compliance office.
- Does your organization permit hand-carry exports to occur? If so, please explain the procedures.
- How are meetings with foreign persons recorded? What is the procedure for conducting such meetings?
- How does your organization handle a visit by a foreign person?
    - Does your organization have an established procedure to conduct a plant tour?
    - Does trade compliance review and approve foreign person visitors in advance, e.g., are your foreign person visitors screened against restricted/denied party lists before they visit?
    - Are foreign person visitors always escorted by a U.S. person employee of your organization?
    - While visiting your organization, do visitors always wear badges that clearly indicate they are non-U.S. Persons?

Engineering / Product Development / Technical Roles

- How are products or technologies developed? Is it a global or multi-

party process? Are the parties you work with screened prior to collaboration? If so, who conducts the screening and where are the records kept? If not, why not?

- What are the procedures used to develop and distribute product or technology export classifications?
- Are relevant employees trained on processes of jurisdiction and classification, including the order of review?
- What are the procedures for controlling visitors to access facilities, especially foreign nationals if involved in the process? Visitor access to company computer systems?
- Are there formal procedures for the release of sensitive data to third parties? Is there a mechanism in place to notify and bind recipients of such data to follow company policy and export control laws?
- Who is responsible for assessing a commodity's end use or application?
- With whom in the company is end-use or application specific evaluations/determinations shared? Does that include trade compliance personnel for purposes of export classification? Where in the development process is export compliance consulted?
- Where is product or technology development information stored? In hard copy, on site? In hard copy, with the third parties? Electronically – e.g., File Transfer Protocol? Cloud-band? Closed system (i.e., non-networked electronic library)? Other?

Commodity Jurisdiction Process/Classification of Products

- Is there a process for determining what data is considered general marketing or public domain information versus technical data that requires a license or the use of an exemption? What is the process for reviewing whether the data is in the public domain? Do you clearly identify on the information itself the ITAR-controlled status of the information?
- Have you developed a standard operating procedure for classification and designated trained individuals to conduct classification?
- Is a classification review conducted by the Empowered Official in the compliance office?
- Are procedures in place for ensuring that no technical data is exported to potential foreign customers or suppliers prior to a review by the trade compliance office to determine the proper jurisdiction and classification and any licensing requirements? If so, is there a process for ensuring that

all functional areas (i.e., sales, marketing, business development, procurement, and program management, etc.) are aware and properly trained to those requirements?

- If the company purchases or obtains controlled products or technology, does it:
    - Determine the proper jurisdiction of the article from the original equipment manufacturer?
    - If required, implement a technology control plan for the products or technology obtained?
    - Maintain records of export activities concerning the product(s)?

Shipping

- Explain in general the process for handling international shipment of goods. How is this coordinated with trade compliance?
- Does shipping coordinate sufficiently with the trade compliance office?
- Does shipping and receiving receive adequate support and tailored training from the trade compliance office?
- Who is responsible for obtaining, contracting, and coordinating with your freight forwarders or customs brokers?
- How is domestic shipping handled?
- Who in shipping is empowered to authorize a shipment? Who is their backup, and are they sufficiently trained?
- Do written procedures exist for handling incoming shipments from international customers?
- Does your organization have procedures in place to provide freight forwarders with direction on how to export and temporarily import your goods, including obtaining assurances that shipments of ITAR-controlled defense articles will not transit ITAR § 126.1 countries?
- What procedures exist for placing a destination control statement on the necessary paperwork and shipping documents, and who is responsible for this placement?
- What is the procedure for maintaining shipping records? Where are they located and for how long are they kept?
- Who is responsible for maintaining empowered attorneys for the freight forwarders and brokers?

Information Technology

- Are all IT personnel sufficiently trained regarding export controls? Is tailored training provided? If so, how, by whom, and how often?
- To what extent and how does IT coordinate with trade compliance regarding storage and access to export-controlled data?
- What are the procedures and criteria for granting access to the system for employees and contractors? Are they different?
- What limitations and/or restrictions are placed on others who are not full-time employees of your organization?
- What types of controls are used to prevent unauthorized external access?
- Is there a mechanism in place for tracking what and by whom documents were accessed, copied, shared, or emailed outside the business?
- What is the policy for remote access of the server by employees and or contractors, including at both domestic and international locations?
- Explain in detail your organization's process for transmitting any technical data overseas.
- Does a process exist to label technical data before it is sent out outside of your organization?
- When transmitting unclassified technical data using end-to-end encryption, are all the requirements of ITAR § 120.54 met?
- Is there a system in place to mark or identify electronically technical data, e.g., do documents containing such data have an export legend citing the regulatory authority?
- How are cyber-attacks identified and what is the organization's investigation and mitigation strategy?
- Is the trade compliance office informed of cyber-attacks? What government agencies does the organization notify of any cyber-attack?
- Is there a mechanism to check-in and check-out to track the use of technical data?
- Does your organization have procedures for issuing and using mobile devices? Does it cover international travel?
    - Do employees receive or can they access ITAR-controlled technical data on mobile devices?
    - For international travel, does your organization issue and ensure that employees travel with clean or sanitized mobile devices? Please explain.
- What type of server system does your organization use, e.g., are the servers in-house or leased?

    - Is there a protocol in place to retain and backup all emails and documents on the server? If so, explain how long the documents and emails are retained.
    - If necessary, can emails from former employees be retrieved or reconstructed?
    - Where is your server located? If located overseas, do you ensure that ITAR-controlled technical data is not stored or backed up to the foreign server, unless compliant with the provisions of ITAR § 120.54(a)(5) regarding storage of unclassified technical data secured using end-to-end encryption?
    - What procedures exist for limiting foreign access to the server by foreign customers or partners? Does your organization ever allow such access?
    - Are your cloud software systems FedRAMP certified?
- What is your organization's process regarding access to IT servers when an employee is terminated from your organization? What measures are taken to ensure the former employee can no longer access your organization's server and information?

Physical Security

- Do you have a process for visitor access?
- How do you process foreign national visitors? For example, screening, export analysis, badging, IT access, etc.
- How do you prevent visitor access to areas containing sensitive technology or data?
- Do you train physical security personnel to understand where export control compliance issues arise? Who conducted the training? How often?
- Are export control requirements incorporated in all access procedures?
- Are there any specific technology control plans in place that govern physical or visual access to controlled products or technical data?
- Who manages technology control plans? How often are they reviewed and updated?

ELEMENT 8: ITAR COMPLIANCE MANUAL

A. Objectives of the ITAR Compliance Manual

Organizations should develop an ITAR Compliance Manual (ICM) and make it available to all employees. The primary objective of the ICM is to provide all employees with a written, authoritative source that sets forth the organization's policies and procedures for ITAR compliance and that defines clear and consistent responsibilities and expectations for employees with respect to ITAR compliance. ICMs are also useful for helping organizations preserve institutional memory and share best practices regarding ITAR compliance.

B. Drafting an Effective ITAR Compliance Manual

The export compliance team should take the lead in drafting the ICM. After the export compliance team has developed a draft manual, organizations should consider selecting various employees who work in different business units outside of export compliance to review and provide feedback on the draft. This ensures that the manual incorporates suggestions and clarifications from the organization's various business units. This also helps to get their support and buy-in for the ICM. Organizations should obtain final approval for the ICM from senior leadership before finalizing the document.

An effective ICM should be well organized, easy to understand, and should:

- Explain why export compliance is important to the organization, including the promulgation of an Export Compliance Management Commitment Statement.
- Provide summaries of applicable export laws and regulations.
- What is the role and function of the ITAR Compliance Program?
- Identify the roles and responsibilities of relevant export compliance personnel and other functional personnel who are responsible for ensuring the organization's compliance with the ITAR.
- Explain how employees should coordinate both within the compliance function and outwardly with other parts of the organization to ensure ITAR compliance.
- Capture the day-to-day operations and ITAR compliance risks relevant to the organization, including through diagrams or other visual aids.
- Describe in detail the organization's compliance policies and procedures.

The ICM should either include or reference the organization's policies and procedures, which should cover:

- Preventing, detecting, and reporting AECA and ITAR violations;
- Identifying, classifying, and marking defense articles, defense services, and technical data, to include the evaluation of authorized limits of software version;
- Incorporating AECA and ITAR compliance into management business plans at the senior executive level and various business functions to ensure effective compliance;
- Obtaining, managing, and complying with the scope of ITAR authorizations;
- Maintaining appropriate records; and
- Meeting and maintaining adequate AECA and ITAR compliance staffing levels at all divisions and facilities.

- Include templates, checklists, and/or forms that are applicable to ITAR compliance within the organization.
- The organization's ITAR compliance training plan for its employees.

C. Publication and Access

Organizations should make their ICMs readily available to all employees, such as by posting the ICMs on internal websites and emailing the ICMs periodically. ICMs should clearly identify an appropriate point of contact for any questions and export control concerns. Organizations should also incorporate their ICMs into their export compliance training programs and encourage employees to use the ICMs as a reference.

D. Updating the ITAR Compliance Manual

Organizations should periodically review their ICMs for updates, revisions, and improvements based on these factors:

- Any changes to the ITAR or DDTC guidance.
- Best practices and lessons learned from ITAR violations or "close calls" within the organization or other organizations.
- Vulnerabilities identified in the organization's ITAR Compliance Program, or negative ad-hoc testing results or audit findings.
- Key risk aeras and changes to an organization's ITAR risk factors, including where such risk factors have changed because of a merger,

acquisition, and/or divestiture, or where there are changes to the organization's product line, services, or customers.

Compliance personnel should have the ability to make suggestions or changes to internal ITAR-compliance processes and procedures. ICMs should be updated on a regular basis, at least annually.

LIST OF ABBREVIATIONS

Abbreviation	Definition
AECA	Arms Export Control Act
BD	Business Development
CCL	Commerce Control List
CJ	Commodity Jurisdiction
CSL	Consolidated Screening List
DDTC	Directorate of Defense Trade Controls
DECCS	Defense Export Control and Compliance System
DTCC	Office of Defense Trade Controls Compliance
DTCL	Office of Defense Trade Controls Licensing
DTCP	Office of Defense Trade Controls Policy
ECCN	Export Control Classification Number
EO	Empowered Official
GC	General Correspondence
HR	Human Resources
ICM	ITAR Compliance Manual
ICP	ITAR Compliance Program
ITAR	International Traffic in Arms Regulations
MLA	Manufacturing License Agreement
OEM	Original Equipment Manufacturer
TAA	Technical Assistance Agreement
TCP	Technology Control Plan
USML	United States Munitions List