

ITAR COMPLIANCE RISK MATRIX

Version	Date	Description of Changes
1.0	09/08/2023	Final

ITAR COMPLIANCE RISK MATRIX

The International Traffic in Arms Regulations (ITAR) Compliance Assessment Risk Matrix is a tool for organizations that manufacture, export, broker, or temporarily import defense articles and defense services described on the United States Munitions List (USML) to assist organizations in assessing their level of ITAR compliance risk. ITAR risk assessments in the defense trade controls context are evaluations of the potential compliance risks that are specific to each organization and that, if left unaddressed, may lead to ITAR violations. ITAR risk assessments therefore allow organizations to ascertain and analyze the likelihood that ITAR violations may occur, the most common reasons ITAR violations may occur, and the types of ITAR violations that are most likely to occur or may result in harm to U.S. national security. After conducting an ITAR risk assessment to understand the full spectrum of ITAR compliance risks, organizations should use that data to create an effective and tailored ITAR compliance program and allocate resources as appropriate to prioritize and mitigate those risks.

A basic approach to ITAR compliance involves three areas:

1. Identify any ITAR-controlled activities or defense articles, including technical data.
2. Recognize the threats and vulnerabilities relevant to those ITAR-controlled activities or defense articles, including technical data.
3. Formulate a risk-based ITAR compliance plan that mitigates the organization's vulnerabilities. See the Directorate of Defense Trade Controls (DDTC's) Compliance Program Guidelines for an overview of an effective ITAR compliance program.

This matrix is organized into:

1. Enterprise Risks – These risks should be understood as areas applicable to the entire organization, not the size or structure of the organization.
2. Organizational Function Risks – These risks should be understood as areas that are typically most applicable to the function or group within the identified responsibilities. If your organization does not have a function or group performing these tasks specifically, you should still consider these risks and where they exist in your organization.
3. ITAR Compliance Program Element Risks.

Note: The ITAR Compliance Assessment Risk Matrix is meant to be a tool for organizations to use to review and assess their ITAR compliance risks and gain a general understanding of their overall level of ITAR compliance risk. It is not intended to be comprehensive, nor is it intended to be exhaustive, and not all risks apply to all organizations. ITAR compliance risks are specific to each organization's operations and functions. This information is not

intended to serve as a basis for any actions or decisions on the part of the public or the DDTC. To the extent there is any discrepancy between this information and either the Arms Export Control Act, as amended (AECA) or the ITAR, the AECA and ITAR will prevail. See ITAR Compliance Risk Assessment Matrix, Supplement 1, ITAR Risk Matrix for Universities for information tailored to universities, research institutes, and laboratories.

1. ENTERPRISE RISKS

ITAR compliance risks vary widely. The size and structure of each organization and the scope of its business are major factors that inform ITAR compliance risk.

Enterprise Risk	LOW RISK	MEDIUM RISK	HIGH RISK
Organization Size, Exposure, and Changes/Growth	<ul style="list-style-type: none"> • Small-sized organization with: • Few or no international sales, transactions with foreign persons, and/or only incidental contact with ITAR-controlled items. • Limited reliance on ITAR-controlled software and technical data. • Only manufacturing activity, no exports. • Routinely performs compliance resource reviews to address and adapt to changes/increases in ITAR footprint. • Allocates funding to support additional resources or personnel as needed in response to changes/growth. 	<ul style="list-style-type: none"> • Medium-sized organization with: • Minimal U.S. Munitions List (USML) category specialization. • Some international presence. • Some international sales, transactions with foreign persons, and/or sales primarily intended to supply the U.S. government outside of the U.S. • Some dependence on ITAR-controlled technical data and software systems. • Performs compliance resource reviews as needed in response to changes/increases in ITAR footprint. • Allocates some funding to support additional resources or personnel as needed in response to changes/growth and is a lengthy process. 	<ul style="list-style-type: none"> • Large-sized organization with: • Diverse product line. • Extensive international presence. • Broad base of domestic and foreign customers. • Does not perform compliance resource reviews in order to adapt to changes/increases in ITAR footprint. • Does not allocate funding to support additional resources or personnel in response to changes/growth as needed.
Ownership Structure	<ul style="list-style-type: none"> • Exclusively U.S. person ownership. 	<ul style="list-style-type: none"> • Non-U.S. person ownership. • Non-U.S. person owners exclusively from non-ITAR §126.1 countries. 	<ul style="list-style-type: none"> • Predominantly or exclusively non-U.S. person ownership. • Individuals or entities from ITAR § 126.1 countries on Board or as Executives. • Owned and/or controlled by a foreign company.
Organization Location and Structure	<ul style="list-style-type: none"> • No or few subsidiaries or affiliates. • All subsidiaries or affiliates based in the United States. 	<ul style="list-style-type: none"> • Few or more subsidiary/affiliates. • Subsidiaries/affiliates outside the United States. 	<ul style="list-style-type: none"> • Multitiered, complex structure, to include multiple or complex, holding companies. • Subsidiaries/affiliates in ITAR § 126.1 countries.

Enterprise Risk	LOW RISK	MEDIUM RISK	HIGH RISK
Mergers, Acquisitions, & Divestitures (MAD)	<ul style="list-style-type: none"> • No or limited history of participation in mergers, acquisitions, and/or divestitures associated with defense articles or defense services. 	<ul style="list-style-type: none"> • Possibility of merger, acquisition, or divestiture. • ITAR violations discovered during MAD due diligence activity. • Some target entities involve ITAR-controlled activity. 	<ul style="list-style-type: none"> • Regularly engages in merger, acquisition, and/or divestiture activities. • Target entities involved in ITAR-controlled activity. • No ITAR compliance due diligence activity is conducted prior to MAD. • If applicable, does not file with the Committee on Foreign Investment in the United States. • Does not provide 60-day and/or 5-day notice to DDTC.
Lines of Business	<ul style="list-style-type: none"> • Transacts in a limited number of ITAR-controlled products or services. • Products and services are not ITAR-controlled. 	<ul style="list-style-type: none"> • Multiple lines of ITAR-controlled products or services offered. • Furnishes defense services to non-U.S. Government customers. • Some sales involve Significant Military Equipment and/or classified defense articles. • Engages in brokering activities. • Mix of commercial and ITAR-controlled products. • Occasionally provide defense services. 	<ul style="list-style-type: none"> • Business mostly or exclusively focused on non-U.S. business/markets. • Extensive international logistics operations. • Sales involve Significant Military Equipment and/or classified defense articles. • Engages regularly in brokering activities. • Mostly/exclusively ITAR-controlled products • Regularly furnishes defense services.
International Business	<ul style="list-style-type: none"> • No international activity or interactions with foreign customers. • May conduct limited amount of overseas support to U.S. Government. • Solely domestic manufacturing of defense articles with no export activity. • No use of Foreign Service Centers. • No foreign subsidiaries/affiliates/vendors that manufacture, develop, repair, and/or service ITAR-controlled products outside the United States. 	<ul style="list-style-type: none"> • Some foreign customers, suppliers, vendors, sales representatives, distributors, resellers, consultants, and/or brokers. • Some manufacturing of ITAR-controlled defense articles abroad. • Has some export licenses and authorizations to procure defense articles from abroad. • Use of Foreign Service Centers that have limited ITAR knowledge. • Limited overseas subsidiaries / affiliates / vendors that manufacture, develop, repair, and/or service ITAR-controlled products outside the United States. • Minimal Technical Assistance Agreements (TAAs), Manufacturing License Agreements 	<ul style="list-style-type: none"> • More than half of revenue comes from international business with a majority of customer base being foreign persons. • Has a global structure for manufacturing and/or development of defense articles. • Extensive manufacturing facilities and/or warehouse or distribution centers abroad. • Manufactures and procures non-ITAR controlled items from ITAR § 126.1 countries. • Heavy reliance on Foreign Service Centers but Foreign Service Centers lack ITAR expertise and procedures.

Enterprise Risk	LOW RISK	MEDIUM RISK	HIGH RISK
		(MLAs), Distribution Agreements, or Warehouse Agreements.	
Markets	<ul style="list-style-type: none"> No foreign customers. 	<ul style="list-style-type: none"> The organization transacts with a few foreign customers (no ITAR § 126.1 countries). 	<ul style="list-style-type: none"> Large foreign customer base including customers from ITAR § 126.1 countries.
Use of Third-Party Agents, Representatives, and Consultants	<ul style="list-style-type: none"> No use of third-party agents, representatives, and/or consultants in support of ITAR-controlled activities. Regular use of third-party agents with regular submission of Part 130 reports. 	<ul style="list-style-type: none"> Limited use of third-party agents, representatives, and consultants in countries identified as high risk of diversion and/or co-located in geographic regions with § 126.1 countries. Third-party agents, representatives, or consultants who inconsistently follow regulations. 	<ul style="list-style-type: none"> Regular use of third-party agents, representatives, or consultants with little experience or background in ITAR-related business. Use of third-party agents, representatives, or consultants from § 126.1 countries (when required authorizations are in place).
International Travel, Conferences, Trade Shows	<ul style="list-style-type: none"> Employees have limited international travel. Employees do not attend, receive, distribute, nor present at international conferences and/or trade shows. 	<ul style="list-style-type: none"> Employees frequently travel to overseas destinations where they participate in demonstrations, speaking engagements, and trade shows. 	<ul style="list-style-type: none"> Employees travel to ITAR § 126.1 countries to speak at academic conferences, or to visit sites in countries where it is known that persons from ITAR § 126.1 countries may be present.
Exports	<ul style="list-style-type: none"> Limited, distribution or export of ITAR-controlled defense articles or defense services. Limited manufacturing of defense articles and no exports. Limited ITAR-controlled activities with foreign persons. Extensive and organized record keeping. 	<ul style="list-style-type: none"> Few exports of defense articles and furnishing of defense services. Mix of ITAR-controlled and non-ITAR-controlled products shipped overseas. Employees occasionally hand carry defense articles or technical data overseas. Routinely hand carry defense articles overseas. Spotty recordkeeping and records kept in multiple locations that are hard to produce when needed. 	<ul style="list-style-type: none"> High volume of export of defense articles and furnishing of defense services. Routinely hand carry defense articles or technical data overseas. Lack of record keeping and reporting. Reliance on third parties for classification of defense articles on the USML and to assist with ITAR compliance.
Foreign-Person Employment	<ul style="list-style-type: none"> Has processes in place to identify foreign person employees and protect against unauthorized access to or release of defense articles, including technical data, and defense services to foreign person employees. 	<ul style="list-style-type: none"> Has limited processes and safeguards in place to identify or protect against unauthorized access to or release of defense articles, including technical data, and defense services to foreign person employees. 	<ul style="list-style-type: none"> Has significant number of foreign person employees in the United States and/or working for the U.S. entity overseas. No or weak processes in place to protect against unauthorized access to or release of defense articles, including technical data, and defense

Enterprise Risk	LOW RISK	MEDIUM RISK	HIGH RISK
			services to foreign entities and foreign employees. <ul style="list-style-type: none"> • Potential foreign person employees need for access to technical data with there being no export license or other authorization in place. • Foreign person employees from ITAR § 126.1 countries.
Classified Work	<ul style="list-style-type: none"> • No ITAR-controlled activities involving classified defense articles, classified technical data, or classified information. 	<ul style="list-style-type: none"> • Business involves ITAR-controlled activities involving limited classified contracts. • Business involves limited export of classified defense articles, technical data, or information. • Limited number of employees with the required security clearance level involved in the classified work involving ITAR-controlled activities. 	<ul style="list-style-type: none"> • Significant portfolio of classified work that involves regular export of classified defense articles or classified information outside the United States or abroad. • Lack of employees with the required security clearance level in the United States and/or abroad involved in the classified work involving ITAR-controlled activities. • Lacks policies and procedures on handling and exporting classified defense articles, technical data, and defense services.
Foreign Person Visitors	<ul style="list-style-type: none"> • Limited or no foreign person visits/tours in its facilities. • Processes in place to protect against unauthorized access to or release of defense articles, including technical data, and defense services to foreign visitors. • No ITAR-related work or defense articles out in plain view at facilities. • Export licenses are routinely and consistently obtained for foreign visitors. 	<ul style="list-style-type: none"> • Foreign visitors occasionally participate in meetings or tours in its facilities. • Limited process in place to protect against unauthorized access to or release of defense articles, including technical data, and defense services to foreign visitors. 	<ul style="list-style-type: none"> • Large number of foreign visitors or tours of facilities. • No processes in place to protect against unauthorized access to or release of defense articles, including technical data, and defense services to potential foreign visitors. • ITAR-related work and/or defense articles in plain view at facilities. • Houses/stores defense articles in facilities in non-secured areas.
Screening	<ul style="list-style-type: none"> • Regularly screens all outside parties. • Screens all new employees at time of hire. 	<ul style="list-style-type: none"> • Screen most outside parties. • Screens only foreign person hires. 	<ul style="list-style-type: none"> • No party screening. • No new hire screening.

2. ORGANIZATIONAL FUNCTION RISKS

All functions within an organization should be evaluated to determine the level of ITAR compliance risk associated with that function.

Organizational Function	LOW RISK	MEDIUM RISK	HIGH RISK
Senior Management / Program Management	<ul style="list-style-type: none"> • Actively promotes a culture of ITAR compliance. • Promulgates ITAR compliance policies and procedures throughout the enterprise. • Directs development of internal ITAR procedures. • Periodically assesses and addresses ITAR compliance resources. • Directs and conducts consistent training on U.S. export control laws and regulations throughout the enterprise. 	<ul style="list-style-type: none"> • Has an ITAR compliance program but lacks sufficient internal ITAR procedures for each business function. • Periodically conducts ITAR training. 	<ul style="list-style-type: none"> • Does not actively promote a culture of ITAR compliance. • Lacks enterprise-wide ITAR compliance policies and procedures. • ITAR processes are not incorporated into business functions.
Export Control Resources and Personnel	<ul style="list-style-type: none"> • Has in-house ITAR expertise. • ITAR processes are fully integrated into all business functions. • Export control personnel understand their functions and ITAR requirements. • All personnel involved in exports are fully trained and guidance on U.S. export control laws and regulations. • Has a sufficient number of export control personnel. • Export control provides training on U.S. export control laws and regulations to key functional areas. • Keeps up with export control regulatory changes. 	<ul style="list-style-type: none"> • May need additional export control personnel. • Has some internal ITAR expertise. • Export control personnel receive some training on U.S. export control laws and regulations. 	<ul style="list-style-type: none"> • Insufficient number of export control resources. • Does not have sufficient in-house expertise on U.S. export control laws and regulations. • No training on U.S. export control laws and regulations is conducted.
Information Technology (IT)	<ul style="list-style-type: none"> • Technical data is not backed up to servers in foreign locations, unless compliant with the provisions of ITAR 120.54(a)(5) • Use of virtual private network (VPN), ITAR-controlled information transferred 	<ul style="list-style-type: none"> • Data stored in standard cloud or accessible by limited numbers of authorized foreign persons. 	<ul style="list-style-type: none"> • Much technical data stored outside the United States is not compliant with the provisions of ITAR 120.54(a)(5) • Authorized data accessible by larger numbers of foreign persons.

Organizational Function	LOW RISK	MEDIUM RISK	HIGH RISK
	<p>through encrypted file transfer protocols only, routine password changes required.</p> <ul style="list-style-type: none"> Automates export control functions. Does not transfer electronic technical data (e.g., email, file transfers) to foreign partners/vendors/subsidiaries. Technical data stored separately from non-ITAR-controlled data, with access controls in place. Processes and procedures in place to request, review, approve/deny access to technical data or systems/networks. Controls and processes/procedures built into and across all business units (i.e., Human Resources, IT, Trade Compliance). Has a fully implemented trade/compliance management software suite. 	<ul style="list-style-type: none"> VPN use, ITAR-controlled information transferred through encrypted email, routine password changes required. Has automated some export control functions. Few transfers of electronic technical data (e.g., email, file transfers) to foreign partners/vendors/subsidiaries. Technical data resides on systems located in the United States but sometimes accessed by employees and partners/vendors/subsidiaries outside of the United States with authorization. Technical data co-mingled with non-ITAR-controlled data, but access controls are in place. Does not routinely verify that only authorized technical data is stored in travel laptops. Has some trade/compliance automation tools. 	<ul style="list-style-type: none"> Does not use VPN, ITAR-controlled information transferred through unencrypted email. High transactional volume relying on manual processes in conducting various ITAR-controlled activities, including tracking authorizations and exports. Regular transfers of electronic technical data (e.g., email, file transfers) to foreign partners/vendors/subsidiaries. Technical data is regularly accessed by employees and partners/vendors/subsidiaries outside of the United States. No separation of technical data from non-ITAR data and no access controls in place. No processes and procedures in place to request, review, approve/deny access to technical data or systems/networks. Does not adequately track access to ITAR-controlled technical data. All physical locations/directories of technical data are not identified and documented. Has no trade or ITAR compliance automation tools. Routinely outsources IT management and is not familiar with the physical location of servers.
Manufacturing	<ul style="list-style-type: none"> Drawings or manufacturing instruction are labeled with appropriate markings. No exposure to any non-U.S. persons. 	<ul style="list-style-type: none"> Classification of items prior to export. Some non-U.S. person exposure with appropriate export controls in place. 	<ul style="list-style-type: none"> Outsourcing manufacturing to foreign sources. Limited ITAR-controlled technology transfer controls in place. Lack of classification knowledge of defense articles. No ITAR controls/checks in place for non-U.S. persons.
Business Development / Sales / Marketing	<ul style="list-style-type: none"> Minimal exports, imports, or sales of defense articles internationally. 	<ul style="list-style-type: none"> Exports, imports, or sells some defense articles domestically and internationally. 	<ul style="list-style-type: none"> Exports, imports, or sells defense articles internationally.

Organizational Function	LOW RISK	MEDIUM RISK	HIGH RISK
	<ul style="list-style-type: none"> • Classifies all defense articles prior to marketing. • Does not use third-party agents or advisers. • Business development personnel trained in export controls. 	<ul style="list-style-type: none"> • Uses some third-party agents under strict controls. 	<ul style="list-style-type: none"> • Uses sales third-party agents frequently and with few ITAR compliance controls. • Business development personnel not trained in export controls.
Procurement / Supply Chain / Purchasing	<ul style="list-style-type: none"> • Does not purchase defense articles. • Obtains or performs export jurisdiction/classifications for all items in its bill of materials. • Checks vendors/suppliers for DDTC registration status and performs party screening. • Exclusive use of U.S. suppliers with U.S. locations. • Small number of suppliers. • Fully vet suppliers and obtain export jurisdiction/classification. • Suppliers are familiar with the ITAR and have robust ITAR compliance programs. 	<ul style="list-style-type: none"> • Obtains export jurisdiction/classification for some items on bill of materials. • Random checks on vendors/suppliers. • Moderate number of suppliers outside the United States. • Use of vendors or suppliers that have a mix of U.S. and non-U.S. locations. 	<ul style="list-style-type: none"> • Does not obtain export jurisdiction/classification for anything in its bill of materials. • Does not vet vendors/suppliers. • Does not screen customers and other parties to the transaction. • Heavy reliance on suppliers outside the United States. • Use of vendors or suppliers that are unfamiliar with the ITAR. • Suppliers in ITAR § 126.1 countries. • Complex supply chain with multiple vendors and suppliers in multiple countries involved in producing a product or service. • Inconsistent records concerning vendors and suppliers, including lack of updated approved suppliers and vendors.
Shipping and Logistics	<ul style="list-style-type: none"> • Only ships domestically. • Handles export controls and documentation in-house • Export approval checks in place 	<ul style="list-style-type: none"> • Ships limited number of ITAR-regulated products. • Ships/provides defense articles and defense services overseas on occasion. • Relies heavily on freight forwarders to handle export controls and documentation. 	<ul style="list-style-type: none"> • Has a mix of ITAR-regulated and non-ITAR-regulated products. • Ships ITAR-regulated products to multiple countries. • Relies entirely on freight forwarders to handle export controls and documentation.
Human Resources	<ul style="list-style-type: none"> • Strong processes in place to (1) determine whether a potential employee is a foreign person, (2) assess whether the position requires access to ITAR-controlled defense articles, including technical data, and defense services, and (3) ensure the required export authorizations or 	<ul style="list-style-type: none"> • Limited processes in place to (1) determine whether a potential employee is a foreign person, (2) assess whether a position requires access to ITAR-controlled articles, technical data and (3) ensure the required export authorizations or technology control plans are in place to prevent unauthorized exports. 	<ul style="list-style-type: none"> • No processes in place to (1) determine whether a potential employee is a foreign person, (2) assess whether a position requires access to ITAR-controlled technical data and (3) ensure the required export authorizations or technology control plans are in place to prevent unauthorized exports.

Organizational Function	LOW RISK	MEDIUM RISK	HIGH RISK
	<p>technology control plans are in place to prevent unauthorized exports.</p> <ul style="list-style-type: none"> • Thorough understanding of how the ITAR defines a U.S. person. • Consistent process exists for vetting citizenship status of all new hires. • Clear understanding of export licensing requirements of employees at non-U.S. locations. 	<ul style="list-style-type: none"> • General understanding of how the ITAR defines U.S. person. • Inconsistent process for vetting citizenship status of new hires. • Weak ITAR compliance processes and lack of coordination with export controls in obtaining licenses for foreign persons. 	<ul style="list-style-type: none"> • Limited understanding of how the ITAR defines U.S. person. • No process exists for vetting the citizenship status of new hires, or use of outside staffing agencies to verify citizenship status of new hires. • Lacks proper vetting of nationality of employees at non-U.S. locations.
Engineering/Research & Development/Technical Expertise	<ul style="list-style-type: none"> • Engineering/technical work conducted in the United States with only U.S. persons. • Strong engineering/technical expertise involved in export jurisdiction and USML classification determination process. • Export jurisdiction and USML classification determination process in place through lifecycle of development. • Research and development (R&D) conducted in the United States only with only U.S. persons. 	<ul style="list-style-type: none"> • Limited amount of development of new technologies or products. • Occasional development of new technologies or products outsourced to foreign persons. • Export jurisdiction and USML classification determination process in place for end-item post-development. • R&D conducted primarily in the United States developed by foreign persons. 	<ul style="list-style-type: none"> • Develops new technologies or products often. • Outsources R&D. • No export jurisdiction and USML classification determination process in place. • R&D at all levels with U.S. and foreign persons collaborating.
Physical Security	<ul style="list-style-type: none"> • Facilities have a process in place for visitor access, including screening, export analysis, badging, and IT access. • Processes are in place to prevent visitor access to areas containing ITAR-controlled inventory, including sensitive technology or data. • Real-time electronic tracking systems for ITAR-controlled inventory with check-in/check-out process. • Training in place for physical security personnel to understand where export control compliance issues may arise. 	<ul style="list-style-type: none"> • Facilities have some processes in place for visitor access, including screening, export analysis, badging, and IT access. • ITAR-controlled inventory separated, but areas not secured from access by visitors and non-authorized personnel. • Tracking system in place for check-in/check-out of ITAR-controlled inventory, but not electronic and/or in real-time. 	<ul style="list-style-type: none"> • Facilities lack processes in place for visitor access, including screening, export analysis, badging, and IT access. • No processes in place to prevent visitor access to areas containing ITAR-controlled inventory, including sensitive technology or data, or inventory stored offsite. • Unsecured facility, room, and/or cage. • ITAR-controlled inventory not segregated in storage facility. • Manual check-in/check-out process for visitors. • No tracking system in place for check in/check out of ITAR-controlled inventory. • No training in place for physical security personnel on export control compliance issues.

3. COMPLIANCE PROGRAM ELEMENT RISKS

Organizations should assess each element of an effective compliance program found in DDTC’s Compliance Program Guidelines to identify potential gaps or vulnerabilities.

Compliance Program Element	LOW RISK	MEDIUM RISK	HIGH RISK
Management Commitment to ITAR Compliance	<ul style="list-style-type: none"> • An export compliance management commitment statement widely communicated to employees. • Senior management involved in and briefed on ITAR compliance matters. • Culture of ITAR compliance in day-to-day operations is highlighted within the organization. • Sufficient resources and budget supporting trade compliance (i.e., personnel, funds, IT). • Organization of the ITAR compliance function appropriate for operations. • Management promotes consistent and documented training on U.S. export control laws and regulations. 	<ul style="list-style-type: none"> • Management commitment statement not widely communicated to employees. • Senior management generally aware of ITAR compliance matters. • ITAR compliance staff and resources insufficient for operations. 	<ul style="list-style-type: none"> • No management commitment statement. • Senior management unaware of ITAR compliance matters or their importance. • Budget insufficient to support trade compliance (i.e., personnel or IT resources), as needed. • No organization culture of ITAR compliance. • ITAR compliance processes are decentralized and there are no clear reporting lines.
DDTC Registration, Export Jurisdiction & USML Classification, Authorizations, & Other ITAR Activities	<ul style="list-style-type: none"> • DDTC registration not required because the organization does not manufacture, export, broker, or temporarily import defense articles and defense services. • Procedures in place to determine export jurisdiction, if needed. • Strong cyber security and encryption measures implemented. Reviewed regularly by third party export control experts. • Have procedures to closely monitor and manage export authorizations. Have a process in place to monitor, track and manage export authorizations. Dedicated resources to export authorization management. 	<ul style="list-style-type: none"> • Automated IT systems or processes in place. • Small number or occasional number of exports require formal authorization or use of an exemption. • DDTC registration submitted in a timely manner and monitored to report material changes properly. • Self-classify products only and rely on internal ITAR expertise. • Export jurisdiction and USML classification procedures are implemented only at the end of the export cycle. • Limited policies and procedures on export jurisdiction and USML classification. 	<ul style="list-style-type: none"> • No process for monitoring and managing export authorizations. • Only manual tracking [of export authorizations] performed. • No checks in place. • Regular export of defense articles and defense services, including technical data, requiring a license authorization or other authorization. • DDTC registration not monitored to report material changes. • No policies or procedures in place to evaluate export jurisdiction and USML classification or to submit Commodity Jurisdiction requests when appropriate. • No restricted party screening conducted.

Compliance Program Element	LOW RISK	MEDIUM RISK	HIGH RISK
	<ul style="list-style-type: none"> Export jurisdiction and USML classification procedures implemented and followed at all stages, including research & development, manufacturing, and exporting. No brokering activities. No political contributions, fees, and commissions. 	<ul style="list-style-type: none"> Regularly screen for restricted parties and entities. Cyber security and encryption measures implemented. Periodically monitor export authorizations. 	<ul style="list-style-type: none"> Brokering activities. No reporting of political contributions, fees, and commissions. Cyber security measures are weak.
Recordkeeping	<ul style="list-style-type: none"> Accurate and complete records are maintained in a central location and monitored. Processes and procedures exist for maintaining records. 	<ul style="list-style-type: none"> Maintain most of the required records. Records are stored in various locations. Processes and procedures exist for maintaining records but not consistently followed 	<ul style="list-style-type: none"> Records incomplete and difficult to locate and obtain. No processes and procedures exist for maintaining records.
Detecting, Reporting, & Disclosing ITAR Violations	<ul style="list-style-type: none"> Management actively encourages employees to raise ITAR compliance concerns. Policies and procedures in place for timely submitting disclosures of potential ITAR violations, including use of voluntary disclosures, and investigating and implementing corrective actions. Employees raise ITAR compliance issues without fear of retaliation. 	<ul style="list-style-type: none"> Employees are not encouraged to raise ITAR compliance concerns. Policies and procedures in place for notification of potential ITAR violations, including use of voluntary disclosures, but are not routinely followed. 	<ul style="list-style-type: none"> Employees do not raise ITAR compliance concerns out of fear of retaliation. ITAR violations are not readily detected. History of ITAR violations that have not been disclosed to the relevant regulatory agency. Management does not support submission of voluntary disclosures. No consequences exist for committing ITAR violations.
Training	<ul style="list-style-type: none"> All employees, including new hires, and contractors are required to complete awareness training on U.S. export control laws and regulations on a regular basis. Job-specific training provided to functional personnel and new hires on relevant ITAR compliance topics. Records of ITAR compliance trainings are regularly maintained. 	<ul style="list-style-type: none"> Annual general awareness training on U.S. export control laws and regulations is provided to all employees only once without refresher training. Training is not tailored nor provided to functional personnel and new hires. Records of ITAR compliance training is spotty. 	<ul style="list-style-type: none"> Limited training on U.S. export control laws and regulations. Training primarily provided to trade compliance personnel and not on a regular basis. Management does not provide ITAR compliance training to employees. Records of ITAR compliance training not maintained.
Risk Assessment	<ul style="list-style-type: none"> Risk assessment for potential ITAR violations performed regularly. Risks for ITAR violations evaluated regularly for improvements. 	<ul style="list-style-type: none"> Risk assessment for potential ITAR violations performed once. 	<ul style="list-style-type: none"> Risk assessment for potential ITAR violations never performed. Unaware of high-risk areas.

Compliance Program Element	LOW RISK	MEDIUM RISK	HIGH RISK
Audits & Compliance Monitoring	<ul style="list-style-type: none"> Regular audits conducted to ensure integrity of compliance programs. Follow through on findings and corrective actions. 	<ul style="list-style-type: none"> Ad hoc audits conducted on compliance programs. Findings and corrective actions are identified but incomplete with little follow-through. 	<ul style="list-style-type: none"> Limited or no audits conducted on compliance programs. No follow through on findings and corrective actions.
ITAR Compliance Manual	<ul style="list-style-type: none"> Comprehensive ITAR compliance manual exists, is published, and used for training regularly. Written policies and procedures on ITAR compliance and updated as applicable. Updates are communicated organization wide as changes occur. 	<ul style="list-style-type: none"> ITAR compliance manual exists but is not easily accessible. Written policies and procedures on ITAR compliance exist but are not updated very often. Some policies and procedures on ITAR compliance are followed. General awareness of policies and procedures on ITAR compliance exists. 	<ul style="list-style-type: none"> No ITAR compliance manual exists. Policies and procedures for ITAR compliance exist but are not implemented. No policies and procedures for ITAR compliance exist. No training provided.