

## **IMPLEMENTATION CONSIDERATIONS:**

### **Dual/Third National Rule**

Before using the exemptions in §126.18 of the International Traffic in Arms Regulations (ITAR) (22 C.F.R. Parts 120-130) regarding dual and third country national employees some consideration should be given to the following matters to prevent diversion of ITAR-controlled defense articles, including technical data, to unauthorized end-users and end-uses:

- a) ITAR compliance program** with implementing policies and procedures.
- b) Empowered and experienced** individuals responsible for implementation and oversight of the plan.
- c) Record-keeping.** The company should have processes and procedures in place to ensure that all records are maintained as required for no less than five years.
- d) Employee training and education** in the ITAR and the compliance program.
- e) Specialized training** of key personnel (e.g., human resources).
- f) Employee screening** to determine general bona fides and identify any diversion risk of ITAR-controlled defense articles, including technical data. The individual's history of trustworthiness, reliability, and adherence to company rules/policies is relevant, in addition to answers to questions regarding substantive contacts. Use of publicly available information and government-sponsored controls list is encouraged. See sample questionnaire below.
- g) Non-Disclosure Agreement (NDA)** with the employee as a condition of continued employment. The NDA is for individuals with access to ITAR-controlled technical data related to defense articles on the U.S. Munitions List. The employee agrees that such controlled technical data will not be further disclosed, exported or transferred in any manner not authorized or approved by the U.S. Government. The NDA will also contain an acknowledgement that the individual does not work for or on behalf of any

country subject to §126.1 of the ITAR and that the individual will report promptly any approach or inquiry from any such country or its representatives. See sample NDA

The following terms provide further information when considering utilizing the exemptions in §126.18:

**1) Substantive contacts.** Contacts contemplated are relationships with individuals that pose a risk of diversion of ITAR-controlled defense articles, including technical data. The most fundamental requirement is full disclosure of all substantive contacts. Contacts with individuals from countries listed in §126.1 of the ITAR (e.g., Iran, North Korea, People’s Republic of China) are of concern, but so too can be contacts with individuals from other countries with a pattern of diverting defense articles. Mere contact with an individual is not necessarily a disqualifier, but rather the nature and substance of the contact must be evaluated to determine the risk of diversion. Licensed foreign parties (companies, organizations and governments) should assess contacts in detail, especially those described below:

- a) Contacts with Government or Military Officials, Agents, or Proxies.** These may range from contact with local customs officials at a port of entry to active collaboration with foreign agents for purposes of circumventing export control laws and regulations.
- b) Business contacts.** These can be associations between two businesses or between an individual and a business. Consider the nature of the contact. Did it begin recently or has it been sustained? Is the business a legitimate enterprise, a “paper” company or a front company? Can it be confirmed independently? Is there any evidence the business in question attempts to acquire sensitive technologies from other sources for itself or for purposes of diversion?
- c) Family contacts.** What is the nature of the family relationship? What other activity (e.g., government, business or other employment, association or organization) is the second family member engaged in that would pose a risk of diversion?

- d) Non-family contacts.** These contacts include friendships and other associations. The most offensive would be with individuals acquiring and selling defense articles for profit or monetary gain, individuals who work for or with front companies, individuals assisting terrorist organizations, individuals working for criminal organizations, or others with the intent of circumventing export controls.
- e) Continuing connections to a third country.** Citizenship, particularly one that cannot be renounced, is not necessarily a disqualifier. An affinity, loyalty, or allegiance to interests of a third country or its government may cause an individual to breach rules or release proprietary or controlled articles or technology without authorization. The totality of continuing connections to the country should be considered. These connections include, among other things, carrying a passport of that country, casting ballots for elections in that country, currently or previously holding an official position within that country, and prior employment with the government of that country. For instance, an active or prior contractual relationship or employment with the government of an ITAR §126.1(a) country would generally disqualify an employee from access to ITAR-controlled defense articles and technical data.
- f) Frequent Travel.** It may be an indicator of relationships with nationals of that country which pose a risk of diversion. Travel may be innocuous or a cover for diversionary activities.
- g) Maintaining a residence in a third country.** Maintaining a residence is not necessarily a disqualifier, but the circumstances of ownership and the potential for a broader connection to the country should be considered.

**2) Bona fide, full-time regular employee.** Employees qualify if they have a full-time employment relationship with the company and the company is legally responsible for the employee's actions (*respondeat superior*). See §120.39 of the ITAR for the definition of a regular employee.

Enclosures:

- 1) Sample Questionnaire

## 2) Sample Non-Disclosure Agreement (NDA)

## **Sample Questionnaire**

- a) How often and where do you travel outside (country of employment) for purposes other than employment with this company?
- b) Do you hold/use a passport from another country?
- c) Do you maintain a residence in another country?
- d) Do you have business contacts, business partners, business contracts, brokers, or any other relationship with a business in another country or other countries subject to U.S. or U.N. embargo?
- e) Do you have contact with family members that work for or with the government of another country? If so, what is their relationship with the government?
- f) Do you have contacts with any other individuals or groups involved in acquiring controlled defense articles, including technical data, illegally or otherwise circumventing export control laws? Please explain the nature of that contact.
- g) Do you hold any office, position, appointment, or any other relationship with the government of another country?
- h) Do you receive a salary, compensation, or any payment from any source (e.g., government, business, other organization or individual) in another country?
- i) Do you have contacts with agents from another country or another country's government?
- j) Have you ever served in or provided information to the government of another country (e.g., military, foreign ministry, intelligence agency or law enforcement)?
- k) Is there any aspect of your overall relationship to another country that would cause you to violate company rules or release ITAR-controlled defense articles, including technical data, without authorization?
- l) Have you ever been approached or asked, directly or indirectly, to provide any ITAR-controlled defense article, including technical data, without authorization?

- m) Have you ever sold or been provided any ITAR-controlled defense articles, including technical data, of the company or any former employer without authority?
- n) Have you fully and completely disclosed all contacts with foreign persons, groups, associations, businesses and governments?
- o) Have you provided fully and truthfully all your contact information to the company, including any addresses, cellular telephone numbers, electronic mail addresses and social networking addresses?
- p) Will you report promptly to the company security officer inquiries or efforts by others in any manner to acquire export controlled defense articles, including technical data, without a license or other authorization?
- q) Have you answered all questions above fully, honestly and faithfully?

**Sample Non-Disclosure Agreement (NDA)**

I, \_\_\_\_\_, acknowledge and understand that any technical data related to defense articles on the U.S. Munitions List and proprietary data that I will have access to or which is disclosed to me by (employer's name) are subject to control under United States law (the International Traffic in Arms Regulations (the "ITAR").

I hereby certify that such controlled technical data will not be further disclosed, exported, or transferred in any manner not authorized under the ITAR, except with the prior written approval of the U.S. Department of State and [employer's name]. I certify that I will report promptly to [employer's name] and its security and export control officers any inquiry or request to provide controlled technical or proprietary data to any third person without authority.

I further certify that I have never acted for, represented, or provided information to and do not currently act for, represent, or provide information to any country or person acting on its behalf that is subject to Section 126.1 of the ITAR, including but not limited to Iran, Syria, North Korea, Sudan, China, Burma, Cuba, or Libya, or any entity that is owned or controlled by such country. Furthermore, I certify that I understand and will comply with the notification requirements of Section 126.1(e) of the ITAR or any other law.

I make this certification voluntarily and understand and agree that it may be provided to the government of [employer's location] and the United States which have an interest in ensuring that controlled defense articles and technical data are not provided or transferred to persons without authority.

---

Signature & Printed Name & Address