PROGRAM MATERIALS
Program #36109
June 30, 2026

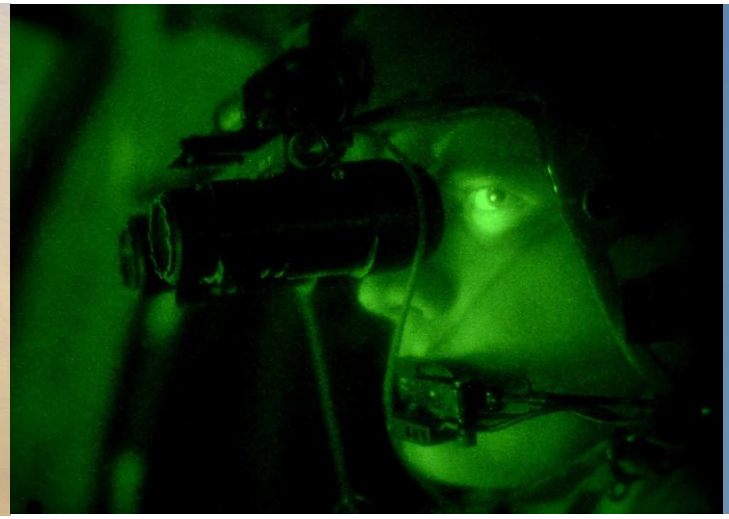
Export Controls Compliance

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

Watson & Associates, LLC
Attorneys | Consultants

Exports Controls Compliance


June 30, 2026

By Wojciech Z. Kornacki, Esq.

Lecturer

Not Legal Advice / For Educational Purposes Only

Watson & Associates, LLC
Attorneys | Consultants

Agenda

Learn About the International Traffic in Arms Regulations (ITAR)

Understand your compliance obligations and the latest enforcement actions

Analyze your compliance risks and best mitigation mechanisms

What are my reporting obligations if violations occur

Watson & Associates, LLC
Attorneys | Consultants

Sources

The Arms Export Control Act (AECA), 22 U.S.C. § 2778

ITAR (22 CFR parts 120-130)

Executive Order 13637, *Administration of Reformed Export Controls* (2013)

Executive Order 14268, *Reforming Foreign Defense Sales To Improve Speed and Accountability* (2025)

91 FR 35926 (proposed rule)

https://www.pmddtc.state.gov/

Watson & Associates, LLC
Attorneys | Consultants

ITAR

ITAR Part 120 - Purpose and Definitions
The ACEA authorized POTUS to control the export and import of defense articles and services

The Office of Defense Trade Controls Licensing and the Director, Office of Defense Trade Controls Licensing

§ 120.2 Designation of defense articles and defense services. – United States Munitions List

§ 120.3 Policy on designating or determining defense articles and services on the U.S. Munitions List.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.31 Defense article.
(a) Defense article means any item or technical data designated in § 121.1 of this subchapter and includes:
(1) Technical data recorded or stored in any physical form, models, mockups or other items that reveal technical data directly relating to items designated in § 121.1 of this subchapter; and
(2) Forgings, castings, and other unfinished products, such as extrusions and machined bodies, that have reached a stage in manufacturing where they are clearly identifiable by mechanical properties, material composition, geometry, or function as defense articles.(b) It does not include basic marketing information on function or purpose or general system descriptions.
(c) The policy described in § 120.3 is applicable to designations of additional items.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.50 Export.

(a) Export, except as set forth in § 120.54 or § 126.16 or § 126.17 of this subchapter, means:

(1) An actual shipment or transmission out of the United States, including the sending or taking of a defense article out of the United States in any manner;

(2) Releasing or otherwise transferring technical data to a foreign person in the United States (a deemed export);

(3) Transferring registration, control, or ownership of any aircraft, vessel, or satellite subject to this subchapter by a U.S. person to a foreign person;

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.50 Export. (continued)
(4) Releasing or otherwise transferring a defense article to an embassy or to any of its agencies or subdivisions, such as a diplomatic mission or consulate, in the United States;
(5) Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad; or
(6) The release of previously encrypted technical data as described in § 120.56(a)(3) and (4).
(b) Any release in the United States of technical data to a foreign person is deemed to be an export to all countries in which the foreign person has held or holds citizenship or holds permanent residency.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.51 Reexport.(a) Reexport, except as set forth in § 120.54 or § 126.16 or § 126.17 of this subchapter, means:
(1) An actual shipment or transmission of a defense article from one foreign country to another foreign country, including the sending or taking of a defense article to or from such countries in any manner;
(2) Releasing or otherwise transferring technical data to a foreign person who is a citizen or permanent resident of a country other than the foreign country where the release or transfer takes place (a deemed reexport); or
(3) Transferring registration, control, or ownership of any aircraft, vessel, or satellite subject to this subchapter between foreign persons.(b) Any release outside the United States of technical data to a foreign person is deemed to be a reexport to all countries in which the foreign person has held or holds citizenship or holds permanent residency.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.32 Defense service.
(a) Defense service means:
(1) The furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing, or use of defense articles;
(2) The furnishing to foreign persons of any technical data controlled under this subchapter, whether in the United States or abroad; or
(3) Military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.33 Technical data.

(a) Technical data means for purposes of this subchapter:

(1) Information, other than software as defined in § 120.40(g), which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions, or documentation;

(2) Classified information relating to defense articles and defense services on the U.S. Munitions List and 600-series items controlled by the Commerce Control List;

(3) Information covered by an invention secrecy order; or

(4) Software (see § 120.40(g)) directly related to defense articles.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.39 Foreign defense article or defense service.
Foreign defense article or defense service means any article or service described on the U.S. Munitions List of non-U.S. origin. Unless otherwise provided in this subchapter, the terms defense article and defense service refer to both U.S. and foreign origin defense articles and defense services described on the U.S. Munitions List. A defense article or defense service is determined exclusively in accordance with the Arms Export Control Act and this subchapter, regardless of any designation (either affirming or contrary) that may be attributed to the same article or service by any foreign government or international organization.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.52 Retransfer.
except as set forth in § 120.54 or § 126.16 or § 126.17 of this subchapter, means:
(1) A change in end-use or end-user, or a temporary transfer to a third party, of a defense article within the same foreign country; or
(1) (2) A release of technical data to a foreign person who is a citizen or permanent resident of the country where the release or transfer takes place.(b) [Reserved]

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.53 Temporary import.
Temporary import, except as set forth in § 120.54, means bringing into the United States from a foreign country any defense article that is:
(1) To be returned to the country from which it was shipped or taken; or
(2) Any defense article that is in transit to another foreign destination.
(b) Temporary import includes withdrawal of a defense article from a customs bonded warehouse or foreign trade zone for the purpose of returning it to the country of origin or country from which it was shipped or for shipment to another foreign destination.
(c) Permanent imports are regulated by the Attorney General under the direction of the Department of Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives (see 27 CFR parts 447, 478, 479, and 555).

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.54 Activities that are not exports, reexports, retransfers, or temporary imports.(a) The following activities are not exports, reexports, retransfers, or temporary imports:
(1) Launching a spacecraft, launch vehicle, payload, or other item into space;
(2) Transmitting or otherwise transferring technical data to a U.S. person in the United States from a person in the United States;
(3) Transmitting or otherwise transferring within the same foreign country technical data between or among only U.S. persons, so long as the transmission or transfer does not result in a release to a foreign person or transfer to a person prohibited from receiving the technical data;
(4) Shipping, moving, or transferring defense articles between or among the United States as defined in § 120.60;(5) Sending, taking, or storing technical data that is:(i) Unclassified;(ii) Secured using end-to-end encryption; …

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.34 Public domain.(a) Public domain means information which is published and which is generally accessible or available to the public:
(1) Through sales at newsstands and bookstores;
(2) Through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information;
(3) Through second class mailing privileges granted by the U.S. Government;
(4) At libraries open to the public or from which the public can obtain documents;
(5) Through patents available at any patent office;
(6) Through unlimited distribution at a conference, meeting, seminar, trade show, or exhibition, generally accessible to the public, in the United States;
(7) Through public release (i.e., unlimited distribution) in any form (e.g., not necessarily in published form) after approval by the cognizant U.S. Government department or agency (see also § 125.4(b)(13) of this subchapter); or
(8) Through fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.56 Release.

(a) ***Release.*** Technical data is released through:

(1) Visual or other inspection by foreign persons of a defense article that reveals technical data to a foreign person;

(2) Oral or written exchanges with foreign persons of technical data in the United States or abroad;

(3) The use of access information to cause or enable a foreign person, including yourself, to access, view, or possess unencrypted technical data; or

(4) The use of access information to cause technical data outside of the United States to be in unencrypted form.

(b) ***Provision of access information.*** Authorization for a release of technical data to a foreign person is required to provide access information to that foreign person, if that access information can cause or enable access, viewing, or possession of the unencrypted technical data.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.57 Authorization types.

License
Other Approval
Exemption
Manufacturing License Agreement
Technical Assistance Agreement
Distribution Agreement

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.58 Subject to the Export Administration Regulations (EAR).
Items subject to the EAR are those items listed on the Commerce Control List in part 774 of the Export Administration Regulations (EAR) and all other items that meet the definition of that term in accordance with § 734.3 of the EAR. The EAR is found at 15 CFR parts 730 through 774.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.60 United States.

United States, when used in the geographical sense, includes the several states, the Commonwealth of Puerto Rico, the insular possessions of the United States, the District of Columbia, the Commonwealth of the Northern Mariana Islands, any territory or possession of the United States, and any territory or possession over which the United States exercises any powers of administration, legislation, and jurisdiction.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.61 Person.
Person means a natural person as well as a corporation, business association, partnership, society, trust, or any other entity, organization or group, including governmental entities. If a provision in this subchapter does not refer exclusively to a foreign person or U.S. person, then it refers to both.

§ 120.62 U.S. person.
U.S. person means a person who is a lawful permanent resident as defined by 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any corporation, business association, partnership, society, trust, or any other entity, organization, or group that is incorporated to do business in the United States. It also includes any governmental (Federal, state, or local) entity. It does not include any foreign person as defined in § 120.63.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.63 Foreign person.
Foreign person means any natural person who is not a lawful permanent resident as defined by 8 U.S.C. 1101(a)(20) or who is not a protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any foreign corporation, business association, partnership, trust, society, or any other entity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments, and any agency or subdivision of foreign governments (e.g., diplomatic missions).

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.67 Empowered official.
(a) Empowered official means a U.S. person who:
(1) Is directly employed by the applicant or a subsidiary in a position having authority for policy or management within the applicant organization; and
(2) Is legally empowered in writing by the applicant to sign license applications or other requests for approval on behalf of the applicant; and
(3) Understands the provisions and requirements of the various export control statutes and regulations, and the criminal liability, civil liability, and administrative penalties for violating the Arms Export Control Act and the International Traffic in Arms Regulations in this subchapter; and

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.67 Empowered official (continued).
(4) Has the independent authority to:(i) Inquire into any aspect of a proposed export, temporary import, or brokering activity by the applicant;(ii) Verify the legality of the transaction and the accuracy of the information to be submitted; and(iii) Refuse to sign any license application or other request for approval without prejudice or other adverse recourse.(b) For the purposes of a broker who is a foreign person, the empowered official may be a foreign person who otherwise meets the criteria for an empowered official in paragraph (a) of this section.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.68 Party to the export.

Party to the export means:(1) The chief executive officer, president, vice-presidents, other senior officers and officials (e.g., comptroller, treasurer, general counsel), and any member of the board of directors of the applicant;(2) The freight forwarders or designated exporting agent of the applicant; and(3) Any consignee or end-user of any item to be exported.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.66 Affiliate.

(a) Affiliate (of a registrant) means a person that directly, or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with, such registrant.(b) For purposes of this section, “control” means having the authority or ability to establish or direct the general policies or day-to-day operations of the firm. Control is rebuttably presumed to exist where there is ownership of 25 percent or more of the outstanding voting securities if no other person controls an equal or larger percentage.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

Not A Defense Article / Not A Defense Service

A specific article or service is not a defense article or defense service for purposes of this subchapter if it:

(1) Is determined to be under the jurisdiction of another department or agency of the U.S. Government (see § 120.5) pursuant to a commodity jurisdiction determination (see § 120.4) unless superseded by changes to the USML or by a subsequent commodity jurisdiction determination; or

(2) Meets one of the criteria of § 120.41(b) when the article is used in or with a defense article and specially designed is used as a control criteria.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.4 Commodity jurisdiction.

(a) The commodity jurisdiction procedure is used with the U.S. Government if doubt exists as to whether an article or service is covered by the U.S. Munitions List (USML). It may also be used for consideration of a redesignation of an article or service currently covered by the USML. The Department must provide notice to Congress at least 30 days before any item is removed from the USML.

(b) The procedure for submitting a Commodity Jurisdiction Determination Request to the Directorate of Defense Trade Controls is set forth in § 120.12.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.5 Relation to regulations of other agencies.

The Department of Commerce and the Export Administration Regulations —

(1) Export of items subject to the Export Administration Regulations by authority of the Department of Commerce
(2) Export of items subject to the EAR by authority of the Department of State.

Nuclear related controls; Department of Energy and the Nuclear Regulatory Commission.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.6 U.S. criminal statutes.
Arms Export Control Act, 22 U.S.C. 2778
Export Administration Act, 50 U.S.C. 4610
18 U.S.C. Section 175, 371, 545, 554, 793, 794, 798, 1001, 1831, 1832, 2332d, 2339A, 2339B, 2339C, or 2339D,
Trading with the Enemy Act, 50 U.S.C. 4315
International Emergency Economic Powers Act, 50 U.S.C. 1705
Securities Exchange Act
Foreign Corrupt Practices Act
Atomic Energy Act
National Security Act
Intelligence Report and Terrorism Prevention Act

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.7 Relations to other provisions of law.

(a) The provisions in this subchapter are in addition to, and are not in lieu of, any other provisions of law or regulations. The sale of firearms in the United States, for example, remains subject to the provisions of the Gun Control Act of 1968 and regulations administered by the Department of Justice. The performance of defense services on behalf of foreign governments by retired military personnel continues to require consent pursuant to part 3a of this title. Persons who intend to export defense articles or furnish defense services should not assume that satisfying the requirements of this subchapter relieves one of other requirements of law.

(b) All determinations, authorizations, licenses, approvals of contracts and agreements, and other action issued, authorized, undertaken, or entered into by the Department of State pursuant to section 414 of the Mutual Security Act of 1954, as amended, or under the previous provisions of this subchapter, continue in full force and effect until or unless modified, revoked, or superseded by the Department of State.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.10 Introduction to the U.S. Munitions List.

(a) The U.S. Munitions List. (Articles, Services, and Technical Data)

(b) Composition of U.S. Munitions List categories. describing end-items, major systems and equipment; parts, components, accessories, and attachments; and technical data and defense services directly related to the defense articles of that USML category.

(c) Significant Military Equipment paragraphs in the USML. All items described within a USML paragraph or subordinate paragraph that is preceded by an asterisk (*) are designated Significant Military Equipment (SME).

(d) Missile Technology Control Regime (MTCR) designation. Annotation with the parenthetical (MT) at the end of a USML entry indicates those defense articles that are on the MTCR Annex.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.12 Commodity jurisdiction determination requests.

(a) Upon electronic submission of a Commodity Jurisdiction Determination Form (Form DS-4076), the Directorate of Defense Trade Controls (DDTC) shall provide a determination of whether a particular article or service is covered by the U.S. Munitions List in part 121 of this subchapter.

The determination, consistent with §§ 120.2, 120.3, and 120.4, entails consultation among the Departments of State, Defense, Commerce, and other U.S. Government agencies and industry in appropriate cases. State, Defense, and Commerce will resolve commodity jurisdiction determination disputes in accordance with established procedures. State shall notify Defense and Commerce, and other U.S. Government agencies as appropriate, of the initiation and conclusion of each case.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.13 Registration.

(a) Any person who engages in the United States in the business of manufacturing or exporting or temporarily importing defense articles, or furnishing defense services, is required to register with the Directorate of Defense Trade Controls as set forth in part 122 of this subchapter. For the purpose of this subchapter, engaging in such a business requires only one occasion of manufacturing or exporting or temporarily importing a defense article or furnishing a defense service.

A manufacturer who does not engage in exporting must nevertheless register.(b) Any U.S. person; foreign person located in the United States; or foreign person located outside the United States that is owned or controlled by a U.S. person, who engages in brokering activities is required to register with the Directorate of Defense Trade Controls as set forth in part 129 of this subchapter.(c) The registration requirements as set forth in parts 122 and 129 of this subchapter include limited exemptions.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.14 Licenses and related authorizations.
(a) Export, reexport, retransfer, or temporary import, of defense articles. The approval of the Directorate of Defense Trade Controls (DDTC) must be requested and obtained before the export, reexport, retransfer, or temporary import of a defense article, unless an exemption under the provisions of this subchapter is applicable.
(b) Furnishing defense services. The approval of DDTC must be requested and obtained before a defense service may be furnished, unless an exemption under the provisions of this subchapter is applicable.
(c) Brokering activities. The approval of DDTC must be requested and obtained before engaging in the business of brokering activities for the defense articles described in § 129.4(a) of this subchapter by a person who is required to register as a broker under part 129 of this subchapter, unless an exemption under the provisions of part 129 is applicable.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.15 Exemptions.

…

Any person engaging in any export, reexport, transfer, or retransfer of a defense article or defense service pursuant to an exemption must maintain records of each such export, reexport, transfer, or retransfer. The records shall, to the extent applicable to the transaction and consistent with the requirements of § 123.22 of this subchapter, include the following information …

f) To claim an exemption for the export of technical data under the provisions of this subchapter (e.g., §§ 125.4 and 125.5 of this subchapter), the exporter must certify that the proposed export is covered by a relevant section of this subchapter, to include the paragraph and applicable subordinate paragraph. …

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.16 Eligibility for approvals.

A U.S. person may receive a license or other approval pursuant to this subchapter. A foreign person may not receive such a license or other approval, except as follows:

(1) A foreign governmental entity in the U.S. may receive a license or other approval;

(2) A foreign person may receive a reexport or retransfer approval; or

(3) A foreign person may receive an approval for brokering activities. …

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.17 End-use monitoring.

Pursuant to section 40A of the Arms Export Control Act (22 U.S.C. 2785) and related delegations of authority, the Department of State is required to establish a monitoring program in order to improve accountability with respect to defense articles and defense services, sold, leased, or exported under Department of State licenses or other approvals under section 38 of the Arms Export Control Act and this subchapter.(b) All exports of defense articles, technical data, services, and brokering activities made pursuant to this subchapter are subject to end-use monitoring by the Department of State through the Blue Lantern program.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.18 Denial, revocation, suspension, or amendment of licenses and other approvals.

(a) Policy. Licenses or approvals shall be denied or revoked whenever required by any statute of the United States. Any application for an export license or other approval under this subchapter may be disapproved, and any license or other approval or exemption granted under this subchapter may be revoked, suspended, or amended without prior notice whenever:(1) The Department of State deems such action to be in furtherance of world peace, the national security or the foreign policy of the United States, or is otherwise advisable; or …

Watson & Associates, LLC
Attorneys | Consultants

ITAR

Notification. The Directorate of Defense Trade Controls will notify applicants or licensees or other appropriate U.S. persons of actions taken pursuant to paragraph (a) of this section. The reasons for the action will be stated as specifically as security and foreign policy considerations permit.(c)

Reconsideration. If a written request for reconsideration of an adverse decision is made within 30 days after a person has been informed of the decision, the U.S. person will be accorded an opportunity to present additional information. The case will then be reviewed by the Directorate of Defense Trade Controls.(d) Reconsideration of certain applications. Applications for licenses or other requests for approval denied for repeated failure to provide information or documentation expressly required will normally not be reconsidered during the 30 day period following denial. They will be reconsidered after this period only after a final decision is made on whether the applicant will be subject to an administrative penalty imposed pursuant to this subchapter.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.19 Violations and penalties.

(a) Part 127 of this subchapter specifies conduct that constitutes a violation of the Arms Export Control Act (AECA) and/or the International Traffic in Arms Regulations in this subchapter and the sanctions that may be imposed for such violations.

(b) The Department strongly encourages the disclosure of information to the Directorate of Defense Trade Controls by persons that believe they may have violated any export control provision of the AECA, or any regulation in this subchapter, order, license, or other authorization issued under the authority of the AECA.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.20 Administrative procedures.

…
The Secretary of State is also authorized to revoke, suspend, or amend licenses or other written approvals whenever such action is deemed to be advisable. The administration of the AECA is a foreign affairs function encompassed within the meaning of the military and foreign affairs exclusion of the Administrative Procedure Act and is thereby expressly exempt from various provisions of that Act. Because the exercising of the foreign affairs function, including the decisions required to implement the AECA, is highly discretionary, it is excluded from review under the Administrative Procedure Act.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.21 Disclosure of information.

(a) Freedom of information. Subchapter R of this title contains regulations on the availability to the public of information and records of the Department of State. The provisions of subchapter R apply to such disclosures by the Directorate of Defense Trade Controls.(b) Determinations required by law. Section 38(e) of the Arms Export Control Act (AECA) (22 U.S.C. 2778(e)) provides that information obtained for the purpose of consideration of, or concerning, license applications shall be withheld from public disclosure unless the release of such information is determined by the Secretary of State to be in the national interest. …

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.22 Advisory opinions and related authorizations.

(a) Preliminary authorization determinations. A person may request information from the Directorate of Defense Trade Controls (DDTC) as to whether it would likely grant a license or other approval for a particular defense article or defense service to a particular country.

(c) Interpretations of the International Traffic in Arms Regulations in this subchapter. Any person may request an interpretation of the requirements set forth in this subchapter in the form of an advisory opinion. A request for an advisory opinion must be made in writing.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 120.23 Organizations and arrangements.

(a) North Atlantic Treaty Organization.
(b) Major non-NATO ally.
(c) Wassenaar Arrangement (dual use)
(d) Missile Technology Control Regime —
(e) Defense Trade Cooperation Treaty between the United States and Australia
(f) Australia Implementing Arrangement
(g) Defense Trade Cooperation Treaty between the United States and the United Kingdom.
(h) United Kingdom Implementing Arrangement.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 127.6 Seizure and forfeiture in attempts at illegal exports.

(a) An attempt to export from the United States any defense articles in violation of the provisions of this subchapter constitutes an offense punishable under section 401 of title 22 of the United States Code. Whenever it is known or there is probable cause to believe that any defense article is intended to be or is being or has been exported or removed from the United States in violation of law, such article and any vessel, vehicle or aircraft involved in such attempt is subject to seizure, forfeiture and disposition as provided in section 401 of title 22 of the United States Code.

(b) Similarly, an attempt to violate any of the conditions under which a temporary export or temporary import license was issued pursuant to this subchapter or to violate the requirements of § 123.2 of this subchapter also constitutes an offense punishable under section 401 of title 22 of the United States Code, and such article, together with any vessel, vehicle or aircraft involved in any such attempt is subject to seizure, forfeiture, and disposition as provided in section 401 of title 22 of the United States Code.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

§ 127.7 Debarment.
Administrative debarment & Statutory debarment.

Appeals. Any person who is ineligible pursuant to paragraph (b) of this section may appeal to the Under Secretary of State for Arms Control and International Security for reconsideration of the ineligibility determination.

§ 127.10 Civil penalty.
For each violation of 22 U.S.C. 2778, an amount not to exceed the greater of $1,271,078 or the amount that is twice the value of the transaction that is the basis of the violation with respect to which the penalty is imposed;
(ii) For each violation of 22 U.S.C. 2779a, an amount not to exceed $1,055.721, or five times the amount of the prohibited incentive payment, whichever is greater; and
(iii) For each violation of 22 U.S.C. 2780, an amount not to exceed $1,256,607.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

Penalties

Civil Penalties

Pursuant **ITAR § 127.10:**

- $1 million+ per violation
- **Debarment**
- Generally settled through a negotiated Consent Agreement

Criminal Penalties

Pursuant to **AECA** section 38(c)22 U.S.C. 2778(c)):

- Up to $1 million, 20 years' imprisonment, or both, per violation
- **Debarment**

Watson & Associates, LLC
Attorneys | Consultants

ITAR

Debarment Examples:

Between approximately January 2016 and November 2019, Respondent and company provided the UAE government with various cyber services, including CNE services and related support activities.

The systems developed, maintained, deployed, and operated by Respondent and others allowed the company to gain unauthorized access to, and to thereby acquire data from, computers, electronic devices, and servers around the world…

Respondent re-exported and retransferred defense articles in violation of Department authorizations and falsified export controls documents. When notified of ineligibility to engage in defense trade, Respondent created a new company and engaged in funnel transactions

Watson & Associates, LLC
Attorneys | Consultants

ITAR

Debarment Examples (continued):

During the period covered by the violation set forth herein, Respondent was engaged in the provision of defense services and was not registered with DDTC

Respondent created false export control documents – purporting to be authorized by the Department. Respondent's misconduct caused the company to export defense articles, including technical data, and provide defense services without authorization and in violation of AECA and ITAR

Respondent misrepresented/misclassified defense articles to avoid obtaining proper authorizations. Respondent was aware that the defense articles were used to develop defense programs in Vietnam

Watson & Associates, LLC
Attorneys | Consultants

ITAR

127.12 Voluntary disclosures.

…

(i) Whether the transaction would have been authorized, and under what conditions, had a proper license request been made;
(ii) Why the violation occurred;
(iii) The degree of cooperation with the ensuing investigation;
(iv) Whether the person has instituted or improved an internal compliance program to reduce the likelihood of future violation;
(v) Whether the person making the disclosure did so with the full knowledge and authorization of the person's senior management.
(If not, then the Directorate will not deem the disclosure voluntary as covered in this section.)

Watson & Associates, LLC
Attorneys | Consultants

ITAR

127.12 Voluntary disclosures (continued).

…

Factors to be addressed in the voluntary disclosure include, for example,

-whether the violation was intentional or inadvertent;

-the degree to which the person responsible for the violation was familiar with the laws and regulations, and whether the person was the subject of prior administrative or criminal action under the AECA;

-whether the violations are systemic;

and the details of compliance measures, processes and programs, including training, that were in place to prevent such violations, if any.

In addition to immediately providing written notification, persons are strongly urged to conduct a thorough review of all export-related transactions where a possible violation is suspected.

Watson & Associates, LLC
Attorneys | Consultants

ITAR

Most Common Violations

Export without authorization

Unauthorized access to technical data

Failure to comply with license provisos

Failure to maintain required records

Failure to register or maintain registration

Misuse of ITAR exemptions

Exporting to prohibited places

Watson & Associates, LLC
Attorneys | Consultants

ITAR

Best Compliance Practices

Due Diligence / Compliance Program / Order of Review Tool
https://www.trade.gov/consolidated-screening-list

Develop Detailed and Clearly Defined Compliance Policies & Conduct Training

Request a Commodity Jurisdiction

Request an advisory opinion

Transaction Records Managements

Mandatory Reporting

Additional Courses:

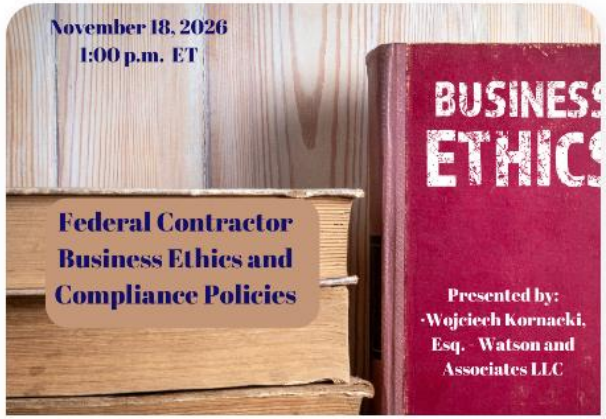
2026-07-20

2026-07-30

2026-08-27

2026-09-28

2026-10-29



2026-11-18

2026-12-10

Not Legal Advice / For Educational Purposes Only

Thank you!

Wojciech Kornacki
Government Contract and Compliance Counsel,
Of Counsel
kornackiw@theodorewatson.com I 202.640-3023

CRITICAL THINKING, CLEAR DIRECTION, DECISIVE RESULTS

Not Legal Advice / For Educational Purposes Only

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

VERSION TRACKER

Version	Date	Description of Changes
1.0	12/05/2022	Final
1.1	09/19/2023	Edits to pages 24, 44, and 59

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.

TABLE OF CONTENTS:
ELEMENTS OF AN EFFECTIVE ITAR COMPLIANCE PROGRAM (ICP)

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.

B. Demonstrating Management Commitment Through Policies and Procedures

Management is ultimately responsible for ensuring its organization's compliance with the ITAR. Management can demonstrate its commitment to ITAR compliance by:

- Creating and maintaining an ICP;
- Providing sufficient resources, including time, funding, personnel, and training, to implement and maintain an ICP commensurate with the organization's risk; and
- Creating and maintaining an Export Compliance Management Commitment Statement.

ITAR Compliance Program

A critical aspect of management's effort to demonstrate its commitment to compliance with the ITAR is creating and maintaining an ICP. An effective ICP should be:

- In writing and clearly state the organizations ITAR compliance policies and procedures;
- Specifically tailored to an organization's ITAR-controlled activities and its areas of risk;
- Regularly reviewed and updated by various business departments responsible for complying with the ITAR; and
- Fully supported by management.

When developing an ICP, management should identify areas that could potentially pose a risk of ITAR violations and the lines of authority, e.g., direct, indirect, and unofficial, in those areas that can assist in preventing ITAR violations. After an ICP is established, management should remain actively engaged in improving the compliance program, e.g., by attending periodic ICP resource and planning meetings at which employees can discuss any ITAR compliance deficiencies they have identified or propose changes to enhance the ICP.

Sufficient Compliance Resources

Management should provide compliance personnel with adequate resources, including the appropriate training, funding, human capital, organizational support,

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.

ELEMENT 2: DDTC REGISTRATION, JURISDICTION & CLASSIFICATION, AUTHORIZATIONS, & OTHER ITAR ACTIVITIES

A. Registration

The ICP should include information on registration requirements in the ITAR.

Who Needs to Register?

The organization's ICP should explain who is required to register with DDTC. The ITAR sets forth the general requirements to register for manufacturers, exporters, and temporary importers in ITAR part 122 and for brokers in ITAR part 129, while also imposing registration requirements in certain unique circumstances. See, e.g., ITAR §§ 126.16(k) and 126.17(k) regarding requirements for intermediate consignees under the Australia and UK treaties, respectively.

The ITAR requires that, subject to certain exemptions, any person who engages in the United States in the business of manufacturing or exporting or temporarily importing defense articles, including technical data, or furnishing defense services, must register with DDTC. Manufacturers who do not engage in exporting must nevertheless register.

The ITAR also requires that, subject to certain exemptions, persons engaged in brokering activities with respect to the manufacture, export, import, or transfer of any foreign defense article or defense service must register with DDTC. The brokering registration requirement applies to any U.S. person, any foreign person located in the United States, and any foreign person located outside of the United States and owned or controlled by a U.S. person. A manufacturing registration does not satisfy brokering registration requirements and vice versa, and persons engaged in both manufacturing and brokering activities must register as both a manufacturer and broker.

The purpose of registration is primarily to provide the U.S. Government with visibility into who is involved in ITAR-controlled activities. **Registration does not confer any export, temporary import, or brokering rights or privileges. Registration also does not constitute a certification of ITAR compliance or indicate the effectiveness of an ICP.**

Registration is generally a precondition to the issuance of any license or other approval, including the use of certain license exemptions. Additional DDTC registration information and FAQs can be found on DDTC's website.

Types of Registration

There are three types of registration: manufacturer, exporter, and broker. Organizations can apply as a manufacturer, exporter, and/or broker in one registration application. They will receive a code that corresponds with their registration type and a completion letter from the DDTC under their account after payment (currently via Defense Export Control and Compliance System (DECCS)).

Submitting Registration Applications and Renewals

A prospective registrant must electronically submit a Statement of Registration (Department of State form DS-2032) to the Office of Defense Trade Controls Compliance (DTCC) by following the submission guidelines available on the DDTC website and referring to the requirements set forth in ITAR § 122.2. Registrations are valid for 12 months and must be renewed annually. The expiration date is included in the registration letter issued by DDTC. Registration renewal submissions should be submitted through DECCS up to a maximum of 60 days but no less than 30 days in advance of the renewal expiration.

Registration Changes and Notifications

Registrants are required to notify DDTC within a specified time period, e.g., five or 60 days, when certain changes in their organization occur. Changes that require notification to DDTC include, but are not limited to, when:

- Certain persons related to the organization have been indicted or otherwise charged with or convicted of violating certain criminal statutes.
- Organizations change certain information in the Statement of Registration, such as name, address, ownership, or persons listed on registration.
- Organizations intend to sell or transfer ownership or control to a foreign person.
- Organizations are part of acquisitions or mergers.

Additional notification requirements are found in ITAR § 122.4.

DDTC Registration Suggestions

Organizations often submit voluntarily disclosures pursuant to ITAR § 127.12 regarding their failure to notify DDTC of registration changes required under the ITAR. To reduce the risk of these types of ITAR violations from occurring, DDTC recommends that organizations take the following actions:

- Understand which activities require an organization to register with DDTC and determine whether the organization is required to do so.
- Assign a senior officer to oversee the registration process and to sign the required notifications.
- Establish and implement policies and procedures to ensure the complete and timely submission of registration renewals and required notifications for material changes. For example, create policies and procedures to ensure that export compliance personnel are informed in advance of changes in senior officers and mergers and acquisitions to ensure timely updates to the registration statement.
- Protect registration codes, which are specific to the registrant and should not be made available publicly.

B. Jurisdiction and Classification

To determine whether organizations or individuals need to register or obtain a DDTC license or other approval, they must determine the appropriate jurisdiction and classification of the commodities they manufacture, export, temporarily import, or broker. Jurisdiction refers to the set of regulations to which a commodity is subject, e.g., the ITAR or the Export Administration Regulations (EAR), whereas classification refers to the specific entry on the respective control list under which the commodity is described, e.g., USML Category VIII(a)(2), or Commerce Control List Export Control Classification Number ECCN 9A610.a).

Commodity Jurisdiction Requests

Manufacturers, exporters, and temporary importers may self-classify their items and services. However, if after reviewing the Order of Review described in ITAR § 120.11, doubt remains regarding the jurisdiction and/or classification of an item or service, organizations may submit a Commodity Jurisdiction (CJ) determination request to DDTC as described in ITAR § 120.12 for an authoritative determination.

To submit a CJ request, navigate to DDTC's website and under "Conduct

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(b)).

Licenses, Agreements, and Other Approvals

As defined in the ITAR, a "license" is a document bearing the word "license" that is issued by DDTC that permits the export, reexport, retransfer, temporary import, or brokering of a specific defense article or defense service controlled under the ITAR.

An "other approval" is a document, other than a license, issued by DDTC that approves an ITAR-controlled activity or the use of an exemption to the license requirements in the ITAR. License exemptions are therefore considered a form of DDTC authorization. Additional information about obtaining a license or other approval from DDTC can be found on DDTC's website. Licenses are submitted and tracked in DECCS.

Agreements approved by the Office of Defense Trade Controls Licensing (DTCL) may authorize U.S. persons to furnish defense services and export technical data to foreign persons, manufacture defense articles abroad, or establish distribution points abroad for defense articles of U.S. origin for subsequent distribution to foreign persons or entities. Agreements are submitted and tracked in DECCS. There are three different types of agreements that cover these activities:

- Manufacturing Licensing Agreements (MLA): agreements whereby a U.S. person grants a foreign person an authorization to manufacture defense articles abroad and that involve or contemplate either the export of technical data or defense articles or the performance of a defense service; or the use by the foreign person of technical data or defense articles previously exported by the U.S. person.
- Technical Assistance Agreements (TAA): agreements for the performance of a defense service(s) or the disclosure of technical data, as opposed to an agreement granting a right or license to manufacture defense articles.
- Distribution Agreements: agreements to establish a warehouse or distribution point abroad for defense articles exported from the United States for subsequent distribution to entities in an approved sales territory.

Additional information on agreements can be found on DDTC's website and under ITAR part 124. Guidance for preparing agreements can be found on DDTC's website in the Agreement Guidance section, and further detail is provided in the DDTC's Guidelines for Preparing Agreements.

Reexports, Retransfers, and General Correspondence Requests

Prior written DDTC approval must be obtained before reselling, transferring, reexporting, retransferring, transshipping, or disposing of a defense article to any end user, end use, or destination other than as stated on the export license or in the Electronic Export Information filing for any exemption previously claimed. This requirement applies in all circumstances, except where the transaction is in accordance with the provisions of an exemption that explicitly authorizes the resale, transfer, reexport, retransfer, or disposition of a defense article without such approval.

U.S. and foreign persons may submit a written request for approval of a reexport or retransfer of defense articles or technical data to DTCL through DECCS. This request is typically referred to as a General Correspondence (GC) request. Foreign persons may also submit GC requests regarding reexports, retransfers, or changes in end use to DTCL, and they do not need to be registered with DDTC in order to do so.

Additional information about approvals for reexports or retransfers can be found in ITAR part 123.

DDTC Licenses, Agreements, and Exemptions Suggestions

To reduce the risk of ITAR violations related to obtaining and using licenses, agreements, and exemptions, DDTC recommends that organizations establish policies and procedures for the following:

- Incorporating licensing and other authorization considerations in all appropriate organization processes.
- Anticipating, to the extent possible, the need for licenses in advance of proposed export activities.
- Ensuring that business development, sales, and marketing personnel understand timelines for obtaining licenses.
- Ensuring ample time to draft, submit, and receive approval for agreements.
- Ensuring all parties understand appropriate terms, conditions, and provisos of the agreement, and conducting periodic audits of export activities under the agreement.
- Performing as much fact finding as practicable ahead of submitting license applications and anticipating changes that may occur while a

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

export authorization and a subsequent reexport or retransfer approval.

- Gather all relevant information about the transaction prior to requesting written approval to ensure the request is not returned without action by DDTC due to lack of information.
- Educate foreign recipients of U.S. defense articles about end use and other ITAR requirements. For example, foreign recipients should understand that destruction is considered a change in end use, and they must request approval from DDTC in advance of destruction or demilitarization.

D. Restricted Party Screening

An organization should screen all parties involved in a transaction prior to engaging in any ITAR-controlled activity with such parties. This includes screening such parties through the Consolidated Screening List (CSL) or restricted party screening tools containing CSL information. The CSL is a list that U.S. government agencies, including the Departments of State, Commerce, and the Treasury, maintains restrictions on certain exports, reexports, or transfers of items. U.S. government agencies routinely update their lists, which are consolidated in the CSL, and DDTC encourages routine screening against the CSL to avoid prohibited transactions. Information on screening and the CSL can be found on the International Trade Administration's website.

Proscribed Countries

It is the policy of the U.S. Government to deny licenses for exports and imports of defense articles and defense services destined for or originating in certain countries listed in ITAR § 126.1, subject to certain exceptions. DDTC considers unauthorized transactions with proscribed countries to be serious violations of the ITAR. More information on the types of prohibited exports, imports, and sales to or from specific countries can be found in ITAR § 126.1.

DDTC Restricted Party Screening and Proscribed Countries Suggestions

To ensure effective screening and reduction of the risk of ITAR violations involving restricted parties and proscribed countries, DDTC recommends that organizations take the following actions:

- Establish policies and procedures for implementing screening within the organization's operations. For example, consider establishing procedures

for screening prior to each of the following activities: entering substantive business discussions, signing contracts or other agreements, submitting license applications, and exporting.
- Establishing policies and procedures for resolving positive hits and reviewing questionable transactions.
- Determine the frequency of routine screening and rescreening of customers, suppliers, or other entities engaged in on-going transactions. Frequency may differ depending on risk related to jurisdiction, industry, entity, etc.
- Maintain detailed screening record results.
- Dedicate adequate resources for screening.
- Monitor updates to U.S. Government lists.
- Ensure that all relevant employees understand which destinations are proscribed under ITAR § 126.1 and the potential consequences of exporting without authorization to one of those destinations.

E. Brokering

ITAR § 129.1(a) states that, "persons engaged in the business of brokering activities shall register and pay a registration fee and that no person may engage in the business of brokering activities without a license."

A broker, as defined in ITAR § 129.2(a), is any person who engaged in brokering activities who is also U.S. person wherever located, any foreign person located in the United States, or any foreign person located outside the United States that is owned or controlled by a U.S. person.

Brokering activities, as defined by ITAR § 129.2(b), mean any action on behalf of another to facilitate the manufacture, export, permanent import, transfer, reexport, or retransfer of a U.S. or foreign defense article or defense service, regardless of its origin. Such activities include, but are not limited to:

- Financing, insuring, transporting, or freight forwarding defense articles and defense services.
- Soliciting, promoting, negotiating, contracting for, arranging, or otherwise assisting in the purchase, sale, transfer, loan, or lease of a defense article or defense service.

Authorization Requirements

ITAR § 129.4 provides a list of defense articles and defense services for which a broker must obtain written approval from DDTC prior to engaging in brokering activities. A broker may request DDTC approval for brokering activities by submitting a completed Form DS-4294 in DECCS. The organization must describe in the request the who, what, where, when, and why of the transaction. A full list of required information can be found in ITAR § 129.6.

Brokers can find exemptions to brokering requirements in ITAR § 129.5. Exempt activities include:

- Certain brokering activities undertaken for an agency of the U.S. Government, as described in ITAR § 129.5(a).
- Certain brokering activities involving foreign defense articles or defense services arranged wholly within and destined exclusively for the North Atlantic Treaty Organization (NATO), NATO countries, Australia, Israel, Japan, New Zealand, or the Republic of Korea, as described in ITAR § 129.5(b).

These brokering exemptions do not apply if the transaction involves ITAR § 126.1 countries or parties debarred pursuant to ITAR § 127.7, as set forth in ITAR § 129.7.

Annual Brokering Activities Report Requirement

Any person who engages in brokering activities is required to provide to DDTC on an annual basis a report of their brokering activities in the previous 12 months. Reports must be submitted along with the broker's annual renewal submission or, if not renewing, within 30 days after expiration of registration. The information required for these reports can be found in ITAR § 129.10.

DDTC Brokering Suggestions

To reduce the risk of brokering-related ITAR violations, DDTC recommends that brokers take the following actions:

- Establish policies and procedures for obtaining prior authorization for brokering activities, reporting brokering activities, and maintaining records regarding brokering activities.
- Understand which activities constitute brokering activities under the

ITAR and identify whether and to what extent the broker is engaged in such activities.
- Review and understand the available exemptions to the brokering authorization requirements.
- Submit annual brokering reports to DDTC on time.

F. Political Contributions, Fees, and Commissions

Applicants and suppliers or vendors need to report to DDTC certain political contributions, fees, or commissions relating to sales of defense articles or defense services valued at $500,000 or more that are being sold commercially to or for the use of the armed forces of a foreign country or international organization. More information can be found in ITAR part 130.

A reportable fee or commission is any loan, gift, donation, or other payment of $1,000 or more made, or offered or agreed to be made directly or indirectly, whether in cash or in kind, and whether pursuant to a written contract, that is:

- To or at the direction of any person, irrespective of nationality, whether employed by or affiliated with an applicant, a supplier, or a vendor; and
- For the solicitation or promotion or otherwise to secure the conclusion of a sale of defense articles or defense services to or for the use of the armed forces of a foreign country or international organization.

The phrase fee or commission does not include:

- A political contribution or a payment excluded by ITAR § 130.6 from the definition of political contribution;
- A normal salary (excluding contingent compensation) established at an annual rate and paid to a regular employee of an applicant, supplier, or vendor;
- General advertising or promotional expenses not directed to any sale or purchaser; or
- Payments made, or offered or agreed to be made, solely for the purchase by an applicant, supplier, or vendor of specific goods or technical, operational, or advisory services, when such payments are not disproportionate in amount with the value of the specific goods or services furnished. See ITAR § 130.5(b).

Political contribution means any loan, gift, donation, or other payment of $1,000 or

more made, or offered or agreed to be made, directly or indirectly, whether in cash or in kind, which is:

- To or for the benefit of, or at the direction of, any foreign candidate, committee, political party, political faction, or government or governmental subdivision, or any individual elected, appointed or otherwise designated as an employee or officer thereof; and
- For the solicitation or promotion or otherwise to secure the conclusion of a sale of defense articles or defense services to or for the use of the armed forces of a foreign country or international organization. Taxes, customs duties, license fees, and other charges required to be paid by applicable law or regulation are not regarded as political contributions. See ITAR § 130.6.

Reporting

To determine whether a report needs to be provided to DDTC under ITAR part 130, applicants (as defined in ITAR § 130.2) and suppliers (as defined in ITAR § 130.7) must conduct their due diligence with respect to their vendors (as defined in ITAR § 130.8). Applicants and suppliers should request the information listed in ITAR § 130.10, which includes any political contributions, fees, or commissions paid or offered or agreed to be paid with respect to the sale. See ITAR § 130.12 and ITAR § 130.13 for more on the information to be furnished by applicants, suppliers, and their vendors.

Each applicant or supplier must inform DDTC as to whether the applicant, suppliers, or their vendors have paid, or offered or agreed to pay:

- Political contributions in an aggregate amount of $5,000 or more.
- Fees or commissions in an aggregate amount of $100,000 or more. If so, the applicant must furnish to DDTC the information specified in ITAR § 130.10.
- Any payments or offers or agreements to make payments of political contributions or fees or commissions that the applicant or supplier learns of after submission of the license application and any value changes to previously submitted reports must be submitted as a supplement report and must include a detailed statement of the reasons why the applicant or supplier did not furnish the information at the time of the application. See ITAR § 130.11 for information regarding supplementary reports.

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

mobile devices for new and existing employees.

- Ensure foreign person employees do not receive unauthorized access to technical data.
- Ensure technical data is not backed up to servers in foreign locations, unless it meets the criteria set out in ITAR § 120.54(a)(5) regarding storage of unclassified technical data secured using end-to-end encryption.
- Coordinate with IT to implement intrusion detection systems.
- Educate employees about phishing, malware, and other cyber threats.
- Review electronic storage options, such as cloud storage services, and understand how service providers protect ITAR-controlled technical data.
- Establish security policies for file sharing and collaboration tools.
- Establish measures for encryption of data on mobile devices, such as laptops and cell phones.
- Establish policies and procedures for the review and approval of employee travel with mobile devices.
- Ensure that IT logs and controls access to company networks that contain ITAR-controlled technical data by authorized personnel.

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.

ELEMENT 4: DETECTING, REPORTING, & DISCLOSING VIOLATIONS

A. Detect and Report Suspected ITAR Violations Early

Organizations should develop and disseminate policies and procedures that provide clear guidance to all employees regarding the detecting and reporting of suspected ITAR violations. Because ITAR violations can cause serious harm to U.S. national security and foreign policy, they can result in the imposition of criminal and/or civil penalties, to include debarment, and/or other costs, including reputational damage and the denial or revocation of export licenses. Early detection, reporting, and rapid corrective actions are essential to minimize any harm to U.S. national security and foreign policy and mitigate an organization's legal exposure.

Organizations should establish policies and procedures to detect, stop, investigate, confirm, report, and remediate any suspected ITAR violations immediately. To this end, DDTC recommendations that organizations:

- Implement clear internal reporting procedures for employees to ensure that employees understand that it is their obligation to report suspected ITAR violations. Organizations should widely promulgate these procedures.
- Provide a mechanism through which employees can report suspected ITAR violations anonymously and confidentially and ensure that employees are aware of and can effectively use this mechanism. For example, organizations may remind employees of such reporting mechanisms through regular bulletins or visual reminders (such as posters) and may provide templates to make reporting suspected violations efficient and effective.
- Clearly identify and communicate to employees the office or individuals within the organization assigned the responsibility for receiving reports of suspected ITAR violations along with their contact information.
- Empower employees to speak up if they are unsure about the proper course of action, if they believe they may have been involved in an activity that violated the ITAR, or if they believe another employee is violating or about to violate the ITAR.
- Provide assurances that employees will not suffer any negative consequences for reporting a suspected violation in good faith.

- 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.

ELEMENT 6: RISK ASSESSMENT

A. ITAR Risk Assessments

Basics of ITAR Risk Assessments

Risk assessments are essential tools for building an effective ICP. 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. Risk assessments therefore allow organizations to ascertain and analyze the likelihood that ITAR violations may occur, the most common reasons violations may occur, and the types of violations that are most likely to occur or would result in the greatest harm. After understanding the full spectrum of their compliance risks, organizations should use that data to create effective and tailored ICPs and allocate resources as appropriate to prioritize and mitigate those risks.

Tailoring ITAR Risk Assessments

Risk assessments should be tailored to the organization's ITAR-controlled activities and should identify and analyze all the potential ITAR-related risk factors for the organization, whether those risk arise inside or outside of the organization. Such potential risk factors may include the following:

- Nature and scope of the organization's commodities;
- Organization's customers, suppliers, freight forwarders, partners, or other third parties involved in its activities;
- Organization's physical and cyber security infrastructure;
- Any foreign parents, subsidiaries, or affiliates;
- Structure of the organization's product development, engineering, and sales activities;
- Any foreign person employees; and
- Geographic regions that the organization operates in or exports to.

Development of ITAR Risk Assessments

Organizations should develop a risk-assessment to identify, assess, and track risks associated with ITAR compliance. Organizations should regularly update their ITAR risk assessments to account for changes to their risk factors. For example, if

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:

- Jurisdiction and Classification: ITAR violations frequently result from the incorrect jurisdiction and classification of defense articles and defense services.
- Authorization Management: ITAR violations frequently result from failing to adhere to the terms and conditions of licenses and agreements.
- Foreign Person Employees or Visitors: foreign person employees, visitors, etc. may pose a compliance risk to organizations if they are not properly authorized to have access to defense articles, including technical data, or receive defense services. ITAR violations frequently result from companies that allow foreign person employees to access technical data stored on internal company networks without first obtaining a license.
- Vetting of Parties and Verification of End Users: customers and other parties to a transaction present a compliance risk for exporters. It is the exporter's responsibility to vet customers and other parties to a transaction. ITAR violations regularly occur when organizations fail to perform sufficient due diligence and defense articles are used in a manner that is inconsistent with the DDTC authorization.
- License Exemptions: **t**he ITAR contains various license exemptions that do not require a request for approval from DDTC. ITAR violations routinely result from failing to meet and document each exemption's requirements.
- International Travel: employees that travel internationally with organization-issued hardware or software and employees that can access their employer's networks and databases while overseas may present a substantial compliance risk, particularly if ITAR-controlled technical data is saved on portable devices or if it is accessible or downloadable without adequate IT security measures. Employees may provide defense services during trade shows, business development, or training/maintenance on defense articles.
- Facility Visits: failing to verify the U.S.-person status of all visitors in advance of plant tours or facility visits in the U.S. creates the risk of inadvertent release of ITAR-controlled technical data. Organizations may seek a license or other approval from DDTC, as appropriate, in advance of foreign person visits. For facility visits at non-U.S. subsidiaries, failing to verify citizenship and the organization they represent against the license or other approval.
- Inventory Management: Inventory management and tracking of ITAR-controlled items can also present compliance risks. ITAR violations may

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 risk to consider when analyzing an ITAR compliance program.

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 it meets the criteria set out in 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

Presidential Documents

Executive Order 14268 of April 9, 2025

Reforming Foreign Defense Sales To Improve Speed and Accountability

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:

Section 1. *Purpose*. To serve the interests of the American people, the United States must maintain the world's strongest and most technologically advanced military through a dynamic defense industrial base, coupled with a robust network of capable partners and allies. A rapid and transparent foreign defense sales system that enables effective defense cooperation between the United States and our chosen partners is foundational to these objectives. Reforming this system would simultaneously strengthen the security capabilities of our allies and invigorate our own defense industrial base. This mutually reinforcing approach would enhance United States warfighting capabilities by fostering healthy American supply chains, domestic production levels, and technological development.

Sec. 2. *Policy*. It is the policy of my Administration to:

(a) Improve accountability and transparency throughout the foreign defense sales system to ensure predictable and reliable delivery of American products to foreign partners in support of United States foreign policy objectives.

(b) Consolidate parallel decision-making when determining which military capabilities the United States will choose to provide, and to which countries.

(c) Reduce rules and regulations involved in the development, execution, and monitoring of foreign defense sales and of transfer cases to ensure alignment with United States foreign policy objectives.

(d) Increase government-industry collaboration to achieve cost and schedule efficiencies in the execution of the Foreign Military Sales (FMS) program.

(e) Advance United States competitiveness abroad, revitalize the defense industrial base, and lower unit costs for the United States and our allies and partners by integrating exportability features in the design phase, improving financing options for partners, and increasing contract flexibility overall.

Sec. 3. *Phased Implementation*. (a) The Secretary of State and the Secretary of Defense shall promptly:

(i) Implement National Security Presidential Memorandum 10 of April 19, 2018 (United States Conventional Arms Transfer Policy), or any successor policy directive.

(ii) Reevaluate restrictions imposed by the Missile Technology Control Regime on Category I items and consider supplying certain partners with specific Category I items, in consultation with the Secretary of Commerce.

(iii) Submit a joint letter to the Congress proposing an update to statutory congressional certification (also known as congressional notification) thresholds of proposed sales under the FMS and Direct Commercial Sales (DCS) programs in the Arms Export Control Act (22 U.S.C. 2751 *et seq*.). The Secretary of State shall also work with the Congress to review congressional notification processes to ensure the timely adjudication of notified FMS and DCS cases.

(b) Within 60 days of the date of this order:

(i) The Secretary of State, in consultation with the Secretary of Defense, shall develop a list of priority partners for conventional arms transfers

and issue updated guidance to Chiefs of the United States Diplomatic Missions regarding this list.

(ii) The Secretary of Defense, in consultation with the Secretary of State, shall:

(A) develop a list of priority end-items for potential transfer to priority partners identified by the Secretary of State in the list required by this subsection;

(B) ensure the transfer of priority end-items to priority partners would not cause significant harm to United States force readiness; and

(C) ensure the transfer of priority end-items to priority partners would advance my Administration's goal of strengthening allied burden-sharing, both by sharing the cost of end-item production and by increasing our allies' capacity to meet capability targets independently, without sustained support from the United States.

(c)(i) The Secretary of State and the Secretary of Defense shall review, update, and reissue the lists of priority partners and military end-items on an annual basis.

(ii) The Secretary of State and the Secretary of Defense shall review and update the list of defense items that can only be purchased through the FMS process (the FMS-Only List) and the United States Munitions List, 22 C.F.R. part 121, to focus protections solely on our most sensitive and sophisticated technologies, and shall establish clear criteria for including an item on the FMS-Only List.

(d) Within 90 days of the date of this order, the Secretary of State and the Secretary of Defense, in consultation with the Secretary of Commerce, shall submit a plan to the President, through the Assistant to the President for National Security Affairs (APNSA), to: improve the transparency of United States defense sales to foreign partners by developing metrics for accountability; secure exportability as a requirement in the early stages of the acquisition process; and consolidate technology security and foreign disclosure approvals.

(e) Within 120 days of the date of this order, the Secretary of Defense, with the assistance of the Secretary of State and the Secretary of Commerce, shall submit a plan to the APNSA to develop a single electronic system to track all DCS export license requests and ongoing FMS efforts throughout the case life-cycle.

Sec. 4. *Definitions*. For purposes of this order:

(a) ''Parallel decision-making'' refers to the granting of simultaneous certifications and approvals during the FMS process, as opposed to sequential decision-making where agencies wait for other agencies to make decisions before taking action.

(b) ''Exportability'' means the process to identify, develop, and integrate technology protection features into United States defense systems early in the acquisition process to protect critical technologies, capabilities, and program information and thus enable export to partners.

(c) ''FMS-only'' means defense articles that are exclusively available through the FMS process as opposed to the DCS process, as authorized in the Arms Export Control Act and described in the Security Assistance Management Manual (SAMM), Defense Security Cooperation Agency (DSCA), Chapter 4.

(d) ''End-item'' means the final product when assembled and ready for issue or deployment.

(e) ''Foreign defense sales system'' means the enterprise devoted to the transfer of defense articles, services, and training by the United States Government and United States companies to international partners and organizations.

(f) All other terms related to FMS cases shall have the meanings given to them by the SAMM, DSCA 5105.38M.

Sec. 5. *General Provisions*. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

THE WHITE HOUSE,
April 9, 2025.

[FR Doc. 2025–06464
Filed 4–14–25; 8:45 am]
Billing code 3395–F4–P

PROPOSED CHARGING LETTER

Mr. Marc Baier

Re: Charged Violation of the Arms Export Control Act and the International Traffic in Arms Regulations

Dear Mr. Baier:

The Department of State (Department) charges you (Respondent) with a violation of the Arms Export Control Act (AECA) (22 U.S.C. 2751 *et seq.*) and the International Traffic in Arms Regulations (ITAR) (22 C.F.R. Parts 120-130) in connection with the unauthorized provision of defense services to the United Arab Emirates (UAE). A total of one charge is charged at this time.

The essential facts constituting the charged violation are described herein. The Department reserves the right to amend this proposed charging letter, including through a revision to incorporate additional charges stemming from the same misconduct of Respondent. Please be advised that this proposed charging letter, pursuant to 22 C.F.R. § 128.3, provides notice of our intent to impose debarment or civil penalties or both in accordance with 22 C.F.R. §§ 127.7 and 127.10.

When determining the charges to pursue in this matter, the Department considered several aggravating factors, including: (a) Respondent did not disclose the charged violation to the Department; (b) the charged violation and surrounding circumstances demonstrate Respondent's charged disregard for the requirements of the ITAR and for Respondent's export compliance responsibilities; and (c) the required license or other approval for some of the conduct at issue would have not been granted by the Department.

The Department also considered a mitigating factor. Respondent entered into agreements with the Directorate of Defense Trade Controls (DDTC) tolling the statutory period that applies to enforcement of the AECA and the ITAR.

This proposed charging letter describes one charged violation for the period from January 2016 to November 2019.

JURISDICTION

Respondent is a U.S. person within the meaning of § 120.15 of the ITAR. Respondent is subject to the jurisdiction of the United States.

During the period covered by the charged violation set forth herein, Respondent was engaged in the provision of defense services and was not registered with DDTC, in accordance with § 38 of the AECA and § 122.1 of the ITAR. The described charged violation relates to defense articles described in Category XI(b) and defense services described in Category XI(d) of the United States Munitions List (USML), § 121.1 of the ITAR, at the time the charged violation occurred.

BACKGROUND

Between January 2016 and November 2019, Respondent was employed by the DarkMatter Group (DarkMatter), a privately held technology and cyber services company headquartered and organized in the UAE that provided cyber services to the UAE government. Prior to working at DarkMatter, a foreign corporation registered in the UAE, Respondent was employed by CyberPoint International LLC (CyberPoint), a U.S.-based company that provided cyber services to the UAE government pursuant to ITAR licenses or other approvals, including technical assistance agreements. CyberPoint and DarkMatter were competitors, and in late 2015 and early 2016, the UAE government transitioned its contracts for cyber services from CyberPoint to DarkMatter. During this time period, DarkMatter hired certain U.S.-person former managers of CyberPoint, including Respondent.

Respondent possessed computer network exploitation (CNE) expertise that included the development, maintenance, deployment, and operation of software and hardware designed to obtain unauthorized access to electronic devices and accounts. Respondent used his CNE expertise to provide and support CNE services that DarkMatter provided for the benefit of the UAE government.

The systems developed, maintained, deployed, and operated by Respondent and others allowed DarkMatter to gain unauthorized access to, and to thereby acquire data from, computers, electronic devices, and servers around the world, including on computers and servers in the United States, as well as computers and servers that communicated with computers in the United States and were

connected to and part of the Internet, in support of the UAE's intelligence gathering efforts. In addition, at least one of the CNE systems developed and deployed by Respondent, and others was an ITAR-controlled defense article, and Respondent did not obtain the required license or other approval from the Department to provide defense services to foreign persons in connection with such an article.

On September 14, 2021, Respondent, along with two other individuals, entered into a deferred prosecution agreement (DPA) with the U.S. Department of Justice to resolve charges related to his activities with DarkMatter. Respondent acknowledged and agreed to the filing of a two-count Criminal Information charging him with: (1) knowingly and willfully conspiring, in violation of 18 U.S.C. § 371, to violate the AECA and ITAR; and (2) knowingly conspiring, in violation of 18 U.S.C. § 371, to commit access device fraud, and computer fraud and abuse, in violation of 18 U.S.C. §§ 1029 and 1030. Respondent admitted, accepted, and acknowledged under oath that the facts and description of his conduct, as set forth in the Factual Statement attached to the DPA, are true and accurate.

VIOLATIONS

The facts underlying the charged ITAR violation addressed in this proposed charging letter are derived primarily from the Factual Statement attached to the DPA. The charged violation involved the unauthorized provision of defense services to DarkMatter and the UAE government.

Unauthorized Provision of Defense Services to the UAE

Between approximately January 2016 and November 2019, Respondent was employed by DarkMatter to provide the UAE government with various cyber services, including CNE services and related support activities. Prior to hiring former employees of CyberPoint, DarkMatter did not have sufficient CNE experience or expertise to engage in CNE activity. Accordingly, DarkMatter obtained that CNE expertise, in part, by hiring key U.S. person managers of CyberPoint, including Respondent.

CyberPoint, through its employees and legal counsel, informed Respondent that if Respondent joined DarkMatter, Respondent would need his own TAA or license from DDTC to continue to provide the defense services Respondent had

been previously providing to the UAE government under CyberPoint's TAA. Despite this warning and Respondent's awareness that DarkMatter hired him and his former CyberPoint coworkers to provide the same CNE operations and related services for intelligence purposes to the UAE government, Respondent did not seek or obtain a license or other approval from the Department.

Many of the CyberPoint employees, known as the "Raven Team," were former U.S. Intelligence Community employees, and some had active U.S. security clearances or had previously held active security clearances, including Respondent. DarkMatter offered these managers higher compensation packages as compared to the compensation they had received from CyberPoint if they accepted employment with DarkMatter.

The U.S.-person managers who accepted employment with DarkMatter, including Respondent, became the founding members of a Raven Team successor at DarkMatter, which was referred to as the Cyber Intelligence-Operations (CIO) group. When the CIO group was created, its employees, including Respondent, operated in the same building, with the same terminals, setup, and computer infrastructure from which they operated under CyberPoint.

Starting in or about January 2016, Respondent became the senior U.S. executive of the CIO group. Between approximately January 2016 and October 2017, and between approximately Spring 2018 and November 2019, Respondent was Executive Cybersecurity Adviser at the CIO group, and the lead manager for the U.S. person employees of CIO group. As Executive Cybersecurity Adviser, Respondent advised executives at DarkMatter, and his duties included consulting with the UAE government, receiving orders and taskings from and relaying updates to the UAE government, assisting in creating and implementing the CIO group's strategic vision, managing CIO group employees, overseeing CNE product acquisition and development, and supervising the CIO group's operations (including exploitation, collection of exfiltrated information, and development of CNE tools).

The CIO group was principally dedicated to conducting CNE operations, as well as providing all manner of support for CNE operations, on behalf of and for UAE government agencies. The CNE services conducted by the CIO group provided access to information and data from thousands of targets around the world, and involved the following services: (a) the acquisition, integration, and development of computer exploits from the United States and elsewhere; (b) the

acquisition, development, and deployment of customized systems and infrastructure to support CNE activities, including anonymizing software servers, and hardware systems; and (c) collecting exfiltrated data from exploited devices, computers, and servers, and passing such data to the CIO group and UAE government agencies, for further analysis.

Among his other activities, Respondent created certain zero-click computer hacking and intelligence gathering systems that were specially designed, developed, maintained and operated by Respondent to access tens of millions of devices for the UAE government's intelligence purposes. he services performed by Respondent in connection with the relevant systems constituted defense services under USML Category XI(d) because: (a) the relevant systems were electronic systems, equipment, or software that were specially designed for intelligence purposes that collect, survey, monitor, or exploit, or analyze or produce information from the electromagnetic spectrum as described in USML Category XI(b); and (b) Respondent assisted foreign persons in the use, design, development, engineering, production, modification, testing, maintenance, processing, or operation of the relevant systems. Respondent did not have a license or other approval to furnish such ITAR-controlled defense services.

RELEVANT ITAR REQUIREMENTS

The relevant period for the charged conduct is January 2016 through November 2019. The regulations effective as of the relevant period are described below. Any amendments to the regulations during the relevant period are identified in a footnote.

Part 121 of the ITAR identifies the items that are defense articles, technical data, and defense services pursuant to § 38 of the AECA.

Section 124.1(a) of the ITAR provides that any U.S. person who intends to furnish a defense service must obtain the approval of the DDTC prior to the furnishing of defense services, unless the furnishing qualifies for an exemption under the provisions of the ITAR.

Section 127.1(a)(1) of the ITAR provides that is unlawful to export or attempt to export from the United States, any defense article or technical data, or to furnish any defense service for which a license or written approval is required by

the ITAR without first obtaining the required license or written approval from DDTC.

CHARGES

Charge 1: Unauthorized Provision of Defense Services to DarkMatter

Respondent violated 22 C.F.R. § 127.1(a)(1) one time when Respondent provided ITAR-controlled defense services to DarkMatter and the UAE government without a license or other approval from the Department.

ADMINISTRATIVE PROCEEDINGS

Pursuant to 22 C.F.R. § 128.3(a), administrative proceedings against a respondent are instituted by means of a charging letter for the purpose of obtaining an Order imposing civil administrative sanctions. The Order issued may include an appropriate period of debarment, which shall generally be for a period of three (3) years, but in any event will continue until an application for reinstatement is submitted and approved. Civil penalties, not to exceed $1,272,251, per violation of 22 U.S.C. § 2778, may be imposed as well, in accordance with 22 U.S.C. § 2778(e) and 22 C.F.R. § 127.10.

A respondent has certain rights in such proceedings as described in 22 C.F.R. Part 128. This is a proposed charging letter. In the event, however, that the Department serves Respondent with a charging letter, Respondent is advised of the following:

You are required to answer a charging letter within 30 days after service. If you fail to answer the charging letter, your failure to answer will be taken as an admission of the truth of the charges and you may be held in default. You are entitled to an oral hearing, if a written demand for one is filed with the answer, or within seven (7) days after service of the answer. You may, if so desired, be represented by counsel of your choosing.

Additionally, in the event that Respondent is served with a charging letter, Respondent's answer, written demand for oral hearing (if any), and supporting evidence required by 22 C.F.R. § 128.5(b), shall be in duplicate and mailed to the administrative law judge designated by the Department to hear the case at the following address:

USCG, Office of Administrative Law Judges G-CJ,
2100 Second Street, SW
Room 6302
Washington, DC 20593

A copy shall be simultaneously mailed to the Deputy Assistant Secretary for Defense Trade Controls:

Deputy Assistant Secretary Michael Miller
U.S. Department of State
PM/DDTC
SA-1, 12th Floor
2301 E Street, NW
Washington, DC 20522-0112

If Respondent does not demand an oral hearing, Respondent must transmit within seven (7) days after the service of its answer, the original or photocopies of all correspondence, papers, records, affidavits, and other documentary or written evidence having any bearing upon or connection with the matters in issue.

Please be advised also that charging letters may be amended upon reasonable notice. Furthermore, pursuant to 22 C.F.R. § 128.11, cases may be settled through consent agreements, including after service of a proposed charging letter.

The U.S. government is free to pursue civil, administrative, and/or criminal enforcement for AECA and ITAR violations. The Department of State's decision to pursue one type of enforcement action does not preclude it, or any other department or agency, from pursuing another type of enforcement action.

Sincerely,

Michael F. Miller
Deputy Assistant Secretary
Bureau of Political-Military Affairs

§ 165.7 [Amended]

■ 2. In § 165.7(e)(1), remove the words ''by the Director of the Division of Enforcement.''

■ 3. Amend § 165.9 by:

■ a. Redesignating paragraph (d) as paragraph (e); and

■ b. Adding a new paragraph (d) to read as follows:

§ 165.9 Criteria for determining amount of award.

* * * * *

(d) *Additional considerations in connection with certain awards of $5 million or less.* (1) This paragraph (d) applies when the Commission is considering any meritorious award application where:

(i) The statutory maximum award of 30 percent of the monetary sanctions collected in any covered and related action(s), in the aggregate, is $5 million or less, and the Commission determines that it does not reasonably anticipate that future collections would cause the statutory maximum award to be paid to any whistleblower to exceed $5 million in the aggregate;

(ii) None of the negative award factors specified in paragraphs (c)(1) or (c)(3) of this section were found present with respect to the claimant's award application and the award claim does not trigger § 165.17 (concerning awards to whistleblowers who engage in culpable conduct);

(iii) The claimant did not engage in unreasonable reporting delay under paragraph (c)(2) of this section (although the Commission, in its discretion, may in certain limited circumstances determine to waive this criterion if the claimant can demonstrate that doing so based on the facts and circumstances of the matter is consistent with the public interest and the objectives of the whistleblower program); and

(iv) The Commission does not otherwise determine in its discretion that application of the enhancement afforded by this paragraph (d) would be inappropriate because either:

(A) The whistleblower's assistance in the covered action or related action (as assessed under paragraph (b)(2) of this section) was, under the relevant facts and circumstances, limited; or

(B) Providing the enhancement would be inconsistent with the public interest, or the objectives of the whistleblower program.

(2) If the Commission determines that the criteria in paragraph (d)(1) of this section are satisfied, the resulting payout to a claimant for the original information that the claimant provided that led to one or more successful covered or related action(s), collectively, will be the maximum allowed under the statute.

(3) Notwithstanding paragraph (d)(2) of this section, if two or more claimants qualify for an award in connection with any covered action or related action and at least one of those claimants' award applications qualifies under paragraph (d)(1) of this section, the aggregate amount awarded to all meritorious claimants will be the statutory maximum. In allocating that amount among the meritorious claimants, the Commission will consider whether an individual claimant's award application satisfies paragraphs (d)(1)(ii) and (d)(1)(iii) of this section.

§ 165.10 [Amended]

■ 4. In § 165.10(a)(7), remove the words ''Division of Enforcement.''

■ 5. Revise § 165.15 to read as follows:

§ 165.15 Administering the whistleblower program.

(a) *Specific authorities*—(1) *Payments, deposits, and credits.* The Executive Director is authorized to deposit into or credit collected monetary sanctions to the Fund, and to make payment of awards therefrom, with the concurrence of the General Counsel, or of their respective designees.

(2) *Designation of claims review staff.* The Claims Review Staff referenced in § 165.7 shall be composed of no fewer than three and no more than five staff members from at least two of the Commission's Offices or Divisions (except the Office of the General Counsel) who have not had direct involvement in the underlying enforcement action, as designated by the General Counsel in consultation with the Executive Director.

(3) *Disclosure of whistleblower identifying information.* The General Counsel is authorized on behalf of the Commission to exercise its discretion to disclose whistleblower identifying information under § 165.4(a).

(b) *General authority to administer the program.* The General Counsel shall have general authority to administer the whistleblower program except as otherwise provided under this part.

Issued in Washington, DC, on June 11, 2026, by the Commission.

Christopher Kirkpatrick,

Secretary of the Commission.

NOTE: The following appendix will not appear in the Code of Federal Regulations.

Appendix to Whistleblower Award Determination—Commission Voting Summary

On this matter, Chairman Selig voted in the affirmative. No Commissioner voted in the negative.

[FR Doc. 2026–12006 Filed 6–12–26; 8:45 am]

BILLING CODE 6351–01–P

DEPARTMENT OF STATE

22 CFR Parts 122, 123, 124, 126, and 130

[Public Notice: 13021]

RIN 1400–AF94

International Traffic in Arms Regulations (ITAR): Part 130 Changes To Reduce Reporting Burden

AGENCY: Department of State.

ACTION: Proposed rule.

SUMMARY: In support of the policy directed in Executive Order 14268 to reduce rules and regulations involved in the development, execution, and monitoring of foreign defense sales and of arms transfer cases, the Department of State proposes to amend the International Traffic in Arms Regulations (ITAR) to modernize and streamline reporting on certain political contributions and fees or commissions.

DATES: Send comments on or before August 14, 2026.

ADDRESSES: Interested parties may submit comments to the Department by any of the following methods:

- Visit the *Regulations.gov* website at: *https://www.regulations.gov* and search for the docket number DOS–2026–0562.
- *Email:DDTCPublicComments@state.gov.* Commenting parties must include RIN 1400–AF94 in the subject line of the email message.

Comments received after that date may be considered if feasible, but consideration cannot be assured. Those submitting comments should not include any personally identifying information they do not desire to be made public or information for which a claim of confidentiality is asserted, because any such claim will be deemed waived and comments and/or transmittal emails may be made publicly available. Parties who wish to comment anonymously may do so by submitting their comments via *www.regulations.gov,* leaving the fields that would identify the commenter blank and including no identifying information in the comment itself.

FOR FURTHER INFORMATION CONTACT: Rob Hart, Office of Defense Trade Controls

Policy, Department of State, email *DDTCCustomerService@state.gov; Subject:* International Traffic in Arms Regulations: Part 130 Changes to Reduce Reporting Burden (RIN 1400–AF94).

SUPPLEMENTARY INFORMATION: The Department of State's Directorate of Defense Trade Controls (DDTC) administers the International Traffic in Arms Regulations (ITAR) (22 CFR parts 120–130). The regulations implement certain authorities of the Arms Export Control Act (AECA) (22 U.S.C. 2751 *et seq.*) delegated to the Secretary of State pursuant to Executive Order 13637. In accordance with 5 U.S.C. 553(b)(4), a summary of this rule may be found at *www.regulations.gov.*

In accordance with § 39(a) of the AECA (22 U.S.C. 2779(a)), the Secretary of State requires ''adequate and timely reporting on political contributions, gifts, commissions and fees paid, or offered or agreed to be paid,'' in connection with the sale or export of certain defense articles, defense services, and design and construction services, under AECA §§ 22, 29, 38, and 38(j)(1)(C)(i) (22 U.S.C. 2762, 2769, 2778, and 2778(j)(1)(C)(i)) to or for the armed forces of a foreign country or international organization. Part 130 of the ITAR implements AECA § 39(a), governing the reporting of covered political contributions and fees or commissions, and related recordkeeping. While AECA § 39 references ''political contributions, gifts, commissions and fees,'' the ITAR defines ''Fee or commission'' and ''Political contribution'' at § 130.5 and § 130.6, respectively, to collectively include the reference to ''gifts,'' as well as two terms not explicit in the statute, ''loan'' and ''donation.'' In this preamble, the Department will use the phrase ''political contributions and fees or commissions'' to encompass the collective activities defined in those two sections and implementing the text of AECA § 39(a). Similarly, in this preamble, the Department will use the term ''payment'' to include gifts, loans, donations, and in-kind transactions.

Pursuant to § 130.9(a), an applicant (as defined in § 130.2) must inform DDTC as to whether the applicant or its vendors (as defined in § 130.8) have paid, or offered or agreed to pay, in respect of any sale: (1) political contributions in an aggregate amount of $5,000 or more; or (2) fees or commissions in an aggregate amount of $100,000 or more. If an applicant or their vendors has paid, or offered or agreed to pay, such payments relating to a qualifying transaction, the applicant must report to DDTC the information specified in § 130.10 (herein referred to as a ''part 130 report''). Reporting this information to DDTC, or providing a satisfactory explanation as to why the information cannot be reported at that time, is a condition precedent to the granting of the relevant license or approval. Similarly, under § 130.9(b), a supplier (as defined in § 130.7) must also inform DDTC as to whether the supplier or its vendors have paid, or offered or agreed to pay, political contributions or fees or commissions in the same amounts. If so, the supplier must submit a part 130 report to DDTC ''no later than 30 days after the contract award to such supplier, or such earlier date as may be specified by the Department of Defense.''

The Department proposes to amend part 130 and related sections of the ITAR to reduce the reporting burden on the regulated community by raising the threshold value to which part 130 requirements apply and the aggregate totals that require reporting, to streamline the reporting process by consolidating submissions to an annual report, and to create a more efficient system for both the regulated community and the Department by introducing a standardized form.

Background

The Department last raised the threshold value for defense articles or defense services to which the requirements in part 130 apply (herein referred to as the ''value threshold'') from $250,000 to $500,000 on July 22, 1993 (58 FR 39280). The Department now proposes to raise the value threshold from $500,000 to $1,000,000. To determine the new threshold amount, the Department used the U.S. Bureau of Labor Statistics Consumer Price Index (CPI) to assess the cumulative impact of inflation since 1993. According to the CPI calculator on the Bureau of Labor Statistics website (*https://www.bls.gov/data/inflation_calculator.htm*), $500,000 in July 1993 would have the same buying power as $1,140,434.78 in January 2026. The proposed value threshold increase, from $500,000 to $1,000,000, is rounded down from the calculated adjustment for inflation to maintain a memorable number for compliance for the regulated community, while modernizing the requirement.

The Department also proposes to raise the aggregate total of political contributions that must be reported to DDTC from $5,000 to $10,000, as reflected in proposed paragraphs § 130.9(a)(1) and (c)(1). Additionally, the Department proposes to raise the aggregate total of fees or commissions that must be reported to DDTC from $100,000 to $200,000, as reflected in proposed paragraphs § 130.9(a)(2) and (c)(2). Increasing these amounts by 100% would maintain the 1:100 ratio between the aggregate total of political contributions and the value threshold for defense articles or defense services (currently $5,000 to $500,000; proposed $10,000 to $1,000,000) and the 1:5 ratio between the aggregate total of fees or commissions and the value threshold (currently $100,000 to $500,000; proposed $200,000 to $1,000,000). Furthermore, the Department would raise the miscellaneous payment thresholds in § 130.10(c)(1) and (c)(2) to half of the proposed aggregate totals in order to maintain the 1:2 ratio between those values. The threshold below which a payment may be labeled a miscellaneous political contribution would increase from $2,500 to $5,000 and the threshold below which a payment may be labeled a miscellaneous fee or commission would increase from $50,000 to $100,000.

In addition to the proposed updates to the value and payment thresholds in part 130, the Department proposes to streamline the reporting process altogether to improve efficiency and reduce common reporting errors. The current requirement that an applicant's part 130 report accompany an application for authorization and a supplier's part 130 report be submitted within 30 days of contract award, or as specified by the Department of Defense, can result in applicants and suppliers reporting estimated and forecasted payments, and offers and agreements of payments, particularly those which may be contingent upon a future license or contract award, or various other factors. These estimates may or may not be updated with accurate values in a supplementary report. The supplementary report, for example, may not always clarify whether it was submitted to make a correction to a previously reported payment or to add an additional payment, leading to duplicative reporting. In other cases, DDTC has received part 130 reports that include information on political contributions or fees or commissions collectively described as ''paid, or offered or agreed to be paid,'' failing to indicate whether a particular fee has been paid or whether it was only offered or agreed to be paid.

The lack of consistency and standardization of part 130 reports received by the Department impacts the accuracy of the reports provided to Congress pursuant to AECA § 36(a). As such, in order to produce the information required by § 36(a), the

Department must conduct an extensive manual review of every report it receives from the regulated community.

The Department's position is that ''adequate and timely'' reporting required by AECA § 39(a) can be achieved through an annual submission process as proposed by this rule. The revisions to the ITAR proposed by this rule would not only improve the ease of compliance with the requirements of part 130, but would also improve the reporting process for the regulated community and the accuracy of the resulting information collected by the Department.

Analysis

In 2020, the Department initiated a review of the process for reporting political contributions and fees or commissions to determine how to improve the information collected pursuant to part 130 in order to better inform the Department and Congress. To support this effort, the Department tasked the Defense Trade Advisory Group (DTAG), a federal advisory committee, with proposing recommendations to address challenges related to reporting and compliance with part 130. Based on the DTAG's recommendations and the Department's own analyses, the Department determined that duplicative reporting across multiple programs or products, over-reporting based on estimates, and the absence of a standard form affect the accuracy of the information.

The Department intends to improve the process for reporting pursuant to part 130 by proposing a new form to standardize submissions and changing to a single report that would be submitted to DDTC at the time of an applicant's or supplier's annual registration renewal under part 122 of the ITAR. A supplier that is not registered with DDTC under part 122 would report by the end of the federal fiscal year, September 30. The Department would no longer require a statement regarding part 130 to be made in an application for authorization under ITAR parts 123, 124, and 125; thus, the section relating to compliance with part 130 would be removed from the DSP–5, DS–6004, and DSP–85 forms.

The new part 130 annual reporting form would include distinct fields for applicants and suppliers to provide payments and offers or agreements, and, for example, to indicate repeating entries, allowing industry to better communicate different or unique scenarios, such as recurring payments and offers across multiple sales. Currently, DDTC receives part 130 reports under the approved information collection ''Statement of Political Contributions, Fees, and Commissions Relating to Sales of Defense Articles and Defense Services'' (OMB Control Number: 1405–0025), without a standard form. For this reason, DDTC receives submissions in various formats with inconsistent levels of detail, requiring significant labor to manually process the information for congressional reports and compliance purposes. The inconsistent formatting and information reported often requires DDTC to contact the applicant or supplier with questions or clarifications. A standardized form would reduce errors during the initial submission process, decreasing the need for the Department to follow-up with applicants or suppliers.

The standardized form would improve the reporting process and the accuracy of the information collected by the Department. The proposed change to an annual submission would enable applicants and suppliers to review the previous 12 months of relevant activity and report based on what has occurred during that time, rather than on forecasts or estimates. Finally, consolidating reporting into a single annual submission would simplify the reporting process for entities managing numerous reports across multiple programs or subsidiaries.

Proposed Implementation

An applicant or supplier that pays, or offers or agrees to pay, political contributions or fees or commissions in aggregate totals specified in § 130.9 would still be required to furnish that information to DDTC. Instead of furnishing the information with a request for authorization under parts 123, 124, and 125, or within 30 days of a contract award to a supplier, as under the current regulations, the Department proposes that information be furnished in an annual report submitted to DDTC with the applicant's or supplier's registration renewal. If a supplier is not registered with DDTC, the report would be due by September 30 of the relevant year (to coincide with the closing of the Department financial year). The requirement for the annual report is described in proposed paragraphs § 130.9(a) and (c). If an applicant or supplier does not pay, or offer or agree to pay, political contributions or fees or commissions in qualifying aggregate totals during a reporting period, the applicant or supplier would not be required to furnish an annual report for that period. If a vendor elects to furnish information directly to DDTC under § 130.12(c), the vendor would submit such report at the time of the vendor's annual registration renewal; if a vendor is not registered with DDTC pursuant to part 122, the report would be due by the end of the federal fiscal year, September 30.

If an applicant or supplier needs to correct or amend a previous report or submit a report for a previous reporting period, proposed § 130.11 would contain two reporting requirements distinct from the proposed annual submission—a supplementary report and an interim report. Under the proposed regulations, a supplementary report would only be required as described in proposed paragraphs (a)(1) and (a)(2). A supplementary report described in proposed paragraph (a)(1) would be required when new information, or a subsequent development, necessitates an amendment, correction, or supplement to an annual report that was already furnished to DDTC for a previous reporting period. Subsequent developments that would necessitate a supplementary report include, for example: an applicant discovering that a payment made during a previous reporting period was not included in the appropriate report; or a payment actually made is substantially different than the previously reported estimate. A supplementary report described in proposed paragraph (a)(2) would be required if DDTC requests additional information regarding miscellaneous payments.

The requirement in current paragraph (a)(1) for applicants and suppliers to submit a supplementary report to DDTC when certain political contributions or fees or commissions not previously reported are paid, or offered or agreed to be paid, in connection with a sale for which the applicant or supplier has previously been required to furnish information, would no longer be necessary because that information would be captured in the annual reporting requirement. For that reason, proposed paragraph (a)(1) would replace the current paragraph (a)(1). Under the proposed regulations, an applicant or supplier would submit an annual report to DDTC that includes information on payments, or offers or agreements to pay, that have occurred since the date of their most recent part 130 report, even if, for example, previous payments were reported with respect to that same authorization in a prior year.

An interim report, as described in proposed paragraphs (c) and (d), would be required when new information creates an obligation for an applicant or supplier to furnish an annual report to DDTC for a previous reporting period

and the applicant or supplier did not furnish an annual report to DDTC for that period. New information that would necessitate an interim report includes, for example, an applicant discovering that its vendors have paid a commission with respect to a qualifying sale in an amount that required a report to DDTC, after the applicant renewed its registration and did not submit a report.

Both a supplementary report under (a)(1) and an interim report under (c) would be required to be furnished to DDTC within 30 days of discovering the new information or subsequent development. A supplementary report under (a)(2) would be required to be furnished to DDTC within 30 days of the request from DDTC.

If an applicant or supplier ceases to operate, or their registration expires, the Department would require a part 130 report be submitted to DDTC within 30 days of their registration expiration date or within 30 days of the cessation of operations, to include all information since their last report. In the case of a merger or acquisition of registrants, the parent, acquiring entity, or new entity that maintains the registration number would be responsible for reporting all of the information required under part 130 not yet been reported by the absorbed or acquired entity. The parent, acquiring entity, or new entity would be required to make an initial part 130 report of the absorbed or acquired entity's information no later than six months after the effective date of the merger or acquisition. The parent, acquiring entity, or new entity would be able to report at the time of its registration renewal, if that renewal occurs within six months of the effective date of the merger or acquisition. After the initial report of the absorbed or acquired entity's information, the parent, acquiring entity, or new entity would then be required to report all subsequent activities for any and all subsidiaries with the annual submission during its registration renewal. In the event an entity is sold or restructured more than once in the six-month time period, the obligation to report its prior information to DDTC within six months of the effective date of the original merger or acquisition would remain with the original parent, acquiring entity, or new entity. Each new purchaser or new entity would be required to report all historical information for absorbed or acquired entities not yet been reported to DDTC.

General Revisions

In addition to the proposed substantive changes, the Department takes this opportunity to propose additional revisions to continue the Department's ITAR reorganization efforts initiated by 87 FR 16396 (Mar. 23, 2022). In keeping with those efforts, the Department further proposes to clarify, organize, and eliminate duplicative text throughout the ITAR in sections that are within part 130 and those that reference part 130. The following proposed revisions incorporate both substantive changes and reorganization efforts; however, where there is purely a clarifying or organizational revision and no change in policy or scope of the regulation, it will be indicated as such. The Department notes that there are other minor changes in part 130 that will be addressed in a future rulemaking; as such, the Department does not address those minor changes here.

Throughout part 130, the Department proposes to remove each reference to ''license or approval'' and add in its place ''authorization.'' This revision is to make consistent references to licenses and the controlled activities for which they are issued and does not implement a change in policy or regulation. The Department proposes to revise acronyms and initialisms in part 130 to follow a standard format. Where a single term for which there is a known acronym appears on more than two occasions within any one section, the first instance is followed by a parenthetical containing the acronym and subsequent use of the term is by acronym. This provides consistency of format without sacrificing clarity and limits unnecessary text.

Section-Specific Revisions

The Department proposes to amend § 122.4 by adding note 3 to paragraph (c), which would reference the six-month part 130 reporting requirement applicable to mergers and acquisitions, in order to assist industry with the new requirement. Section 123.1 would be amended by removing paragraph (c)(6) in order to remove the requirement that a statement concerning the payment of political contributions and fees or commissions accompany an application for permanent export. Switching to an annual report would eliminate the need for this statement to be included in an application for authorization. For the same reason, the Department also proposes to amend § 124.12(a)(6) by striking the last sentence that requires letters of transmittal to include a statement pursuant to part 130.

The Department proposes to amend § 126.16 and § 126.17 (exemptions that implement the Defense Trade Cooperation Treaty between the United States and Australia and the Defense Trade Cooperation Treaty between the United States and the United Kingdom, respectively), to revise paragraph (m) relating to political contributions and fees or commissions in both sections. The Department proposes to remove the reference to ''§ 130.10'' and add in its place ''§ 130.9,'' and to remove the threshold amount. Section 130.10 specifies the information that is required to be submitted to DDTC, while § 130.9 contains the relevant obligation to report to DDTC. The obligation to furnish the information specified in § 130.10 exists only for defense articles or defense services valued at the threshold amount defined in part 130, thus adequately conveying the requirements and making the specific references in §§ 126.16–.17 to both the information that must be reported and the threshold unnecessary.

In § 130.2, the Department proposes to clarify within the definition of ''applicant'' that an applicant includes a person who applies for authorization, who is issued authorization, and a person who utilizes or plans to utilize one of the exemptions implementing the Defense Trade Cooperation Treaties in § 126.16 or § 126.17. In §§ 130.2, 130.7, and 130.8, the Department proposes to increase the $500,000 threshold to $1,000,000 for the reasons explained in this preamble. The Department proposes to move the section defining ''political contribution'' from § 130.6 to § 130.5 and the section defining ''fee or commission'' from § 130.5 to § 130.6, to match the order in which the terms are used in the AECA and their initial implementation in the ITAR (41 FR 40608 (Sept. 16, 1976)). This proposed revision is organizational and would not impact the scope of the definitions.

The Department proposes to revise the section headings for § 130.9 and § 130.10, to simplify and better describe the contents in each section. The proposed changes to these section headings would not impact the scope of the regulations. The section heading for § 130.9 would be revised from ''Obligation to furnish information to the Directorate of Defense Trade Controls.'' to ''Annual reporting requirement.'' The section heading for § 130.10 would be revised from ''Information to be furnished by applicant or supplier to the Directorate of Defense Trade Controls.'' to ''Required information.'' In § 130.9 through § 130.12, the Department proposes to add a unique paragraph heading for each paragraph to indicate its subject—a standard convention to assist readers with the regulations.

Additionally, in § 130.9, the Department proposes the following

revisions in order to implement the substantive changes discussed herein and also reorganize and clarify existing text:

- Restructuring paragraph (a), which describes the applicant's obligation to report information to DDTC, to mirror the structure of the paragraph regarding the supplier's obligation to report to DDTC (current paragraph (b)) by redesignating current paragraphs (a)(1), (a)(1)(i), and (a)(1)(ii), as paragraphs (a), (a)(1), and (a)(2); and subsequently removing paragraphs (a)(1)(i) and (a)(1)(ii).
- Raising the aggregate total for political contributions in proposed paragraph (a)(1) from $5,000 to $10,000 and the aggregate total for fees and commissions in proposed paragraph (a)(2) from $100,000 to $200,000 for the reasons discussed in the preamble.
- Redesignating current paragraph (a)(2) as new paragraph (a)(3).
- Removing the text requiring applicants and suppliers to furnish the information specified in § 130.10 to DDTC from the paragraph setting the aggregate threshold for reporting fees or commissions (proposed paragraphs (a)(2) and (c)(2)) and placing it into its own paragraph (proposed paragraphs (b) and (d)). This text would also be revised to reflect the annual reporting process.
- Redesignating current paragraph (b)—the obligation for suppliers to report to DDTC—as paragraph (c); redesignating current paragraph (c)—relating to the computation of political contributions—as new paragraph (e) and revising for clarity; and redesignating current paragraph (d)—the obligation to furnish new information to DDTC—as new paragraph (f).
- Revising new paragraph (f) to indicate that when an applicant or supplier discovers new information about a previous reporting period, the applicant or supplier may be required to submit a supplementary or interim report pursuant to § 130.11.
- Adding new paragraph (g) regarding reporting requirements when there is a registration expiration, cessation of operations, merger, or acquisition.
- Adding new paragraph (h) to require applicants and suppliers to submit the report using the new standardized form provided by DDTC and to submit the form using a system accessible through the DDTC website.

The Department proposes to amend § 130.10 by making editorial revisions to the introductory text in paragraph (a) for clarity, and adding the requirement that the part 130 report be signed by a senior officer (*e.g.,* chief executive officer, president, secretary, partner, member, treasurer, general counsel) who has been empowered by the applicant or supplier to sign such documents. The Department also proposes to add new paragraph (e), which would require that the part 130 report include a certification that the submission is complete and accurate made by the senior officer. Currently, part 130 reports are generally submitted with an application for authorization, which requires a signature and certification from an empowered official. The proposed paragraphs (a) and (e) would maintain a similar requirement as part of the new form proposed herein. The Department also proposes to revise paragraph (a)(1) to require that the part 130 report include the DDTC authorization number, applicable exemption, or Department of Defense contract or case number, and the end-item associated with the sale. Because part 130 reports would no longer be provided with the request for authorization, the Department would instead collect the authorization number and a description of the end-item through the annual submission. Similarly, the Department would collect the applicable ITAR exemption or the Department of Defense contract or case number, in order to associate the relevant transaction with the annual submission. Additionally, the Department proposes to revise the introductory text in paragraphs (a)(4) and (b) to remove the reference to a ''statement,'' because the information would be provided in the proposed submission form, rather than a statement. The Department proposes to update the miscellaneous payment thresholds in paragraphs (c)(1) and (c)(2) for the reasons described in the preamble.

The Department proposes revisions to § 130.11 to modify supplementary reporting and create a new type of interim reporting as described in the preamble above. Accordingly, the section heading would be revised from ''Supplementary reports.'' to ''Supplementary and interim reports.'' Current paragraph (a)(1)—which requires applicants and suppliers to submit a supplementary report to DDTC when certain political contributions or fees or commissions not previously reported are paid, or offered or agreed to be paid—would be duplicative with an annual submission process; therefore, the text of that paragraph would be removed. For the same reason, the Department proposes to redesignate paragraph (a)(2) as paragraph (a)(1) with revisions described above, redesignate paragraph (a)(3) as paragraph (a)(2), and remove paragraph (a)(3).

Additionally within § 130.11, the Department proposes to remove both current paragraphs (b)(1) and (b)(2) because the text in paragraph (b)(1) can be incorporated into proposed paragraph (b) and the required information listed in paragraph (b)(2) would be required in proposed § 130.10. New paragraphs (c) and (d) would be added to require the interim reporting process as described above. New paragraph (e) would be added to clarify that furnishing a supplementary report or an interim report under § 130.11 does not relieve an applicant or supplier from any obligation to furnish an annual report to DDTC under § 130.9.

The Department proposes to amend § 130.12 by making editorial revisions in paragraph (a). The Department proposes to revise paragraph (c)—which offers vendors the option to furnish information directly to DDTC and submit an abbreviated statement to applicants and suppliers—to reflect the annual submission process. If a vendor elects to furnish information directly to DDTC, the vendor would submit such report at the time of the vendor's annual registration renewal; if a vendor is not registered with DDTC pursuant to part 122, the report would be submitted by the end of the federal fiscal year, September 30. The Department proposes organizational edits to paragraph (d), so that its structure matches other sections in part 130. Paragraph (d)(1) would be redesignated as paragraph (d); paragraphs (d)(1)(i), (d)(1)(ii), and (d)(1)(iii) would be redesignated as paragraphs (d)(1), (d)(2), and new paragraph (d)(3). Consequently, current paragraph (d)(2) would be redesignated as new paragraph (e). The revisions to paragraph (d) and addition of paragraph (e) do not reflect a change in policy or regulation.

Example Reporting Scenarios

The following scenarios exemplify how reporting would be required under the proposed regulations as described in this proposed rule:

Example 1

In January through June 2026, Company A obtains a technical assistance agreement (TAA) that expires in 10 years, a manufacturing licensing agreement (MLA) that expires in 10 years, a DSP–73 authorization for temporary export, and a DSP–5 authorization for permanent export. The TAA and the DSP–5 meet the requirements of § 130.2 because both involve defense articles and defense services valued at over $1,000,000, which are being sold commercially to the armed forces of a foreign country. In

that same time period, Company A offered four fees in a qualifying aggregate total with respect to the TAA and paid one commission above the qualifying total with respect to the TAA. No payments, or offers or agreements to pay, were made in connection with the DSP–5. Company A plans to renew their registration under part 122 with DDTC in October 2026. Under the proposed regulations, Company A would be required to furnish an annual report to DDTC pursuant to § 130.9(a)(2). In the annual report, Company A would be required to include the information specified in § 130.10 with respect to the four offers of fees and the payment of the commission in connection with the TAA. Company A would not be required to include information with respect to the DSP–5 that meets the requirements of § 130.2 because no payments, or offers or agreements to pay, were made in connection with that authorization.

Example 2

Using the same facts from the previous example, Company A renews its registration with DDTC in October 2026 and furnishes the appropriate annual report pursuant to § 130.9. In January 2027, Company A pays two political contributions in a qualifying aggregate total in connection to the same 2025 TAA that it included in its annual report to DDTC the prior year. Under the proposed regulations, in October 2027, Company A would be required to furnish to DDTC the information specified in § 130.10 with respect to the two payments of political contributions in its annual report submitted during registration renewal.

Example 3

Using the same facts from the previous example, on March 1, 2028, Company A discovers that it paid a fee in a qualifying aggregate total with respect to the DSP–5 it obtained in 2025. On March 10, 2028, Company A offers two commissions in a qualifying aggregate total with respect to a new MLA that meets the requirements of § 130.2. Under proposed § 130.11(a)(1), Company A would be required to furnish to DDTC a supplementary report within 30 days of March 1, 2028, that includes the information specified in § 130.10 with respect to the DSP–5 obtained in 2025 and an explanation as to why Company A did not furnish this information at the time it submitted its annual report for that year. Company A would also be required to furnish its annual report in October 2028 during registration renewal and include the information specified in § 130.10 with respect to the payments made relating to the new MLA.

Example 4

In February 2026, Company B obtains a TAA that expires in 10 years that meets the requirements of § 130.2, but Company B does not make payments, or offers or agreements to pay, political contributions or fees or commissions in relation to that TAA. Company B renews its registration with DDTC in April 2026 and, under the proposed regulations, would not be required to furnish an annual report to DDTC pursuant to § 130.9. From April 2026 to April 2027, Company B does not apply for or obtain authorizations that meet the requirements of § 130.2. However, in April 2027, Company B discovers that, in March 2026, Company B had paid one political contribution above the qualifying total with respect to the 2026 TAA. Pursuant to the proposed § 130.11(c), Company B would be obligated within 30 days of this discovery to furnish to DDTC an interim report that includes the information specified in § 130.10 with respect to the 2026 TAA and an explanation as to why Company B did not furnish this information at the time it renewed its registration. Company B would not be required to file an annual report in April 2027 because Company B did not make any payments or offers or agreements to pay since its most recent registration renewal.

Comments Requested

The Department encourages the public to provide comments directly related to this proposed rule and provide responses to the questions presented herein. To facilitate timely review and assessment, comments should be provided in a concise sentence or paragraph, followed by supporting explanatory paragraphs and examples, with each distinct comment treated separately, as opposed to multiple comments in one paragraph or section. The Department specifically requests comments on the following matters:

1. Do you foresee any operational, administrative, or compliance challenges with the change to annual part 130 reporting?

2. With this rule, the Department would be revising an existing collection of information under OMB control number 1405–0025 titled *Statement of Political Contributions, Fees, and Commissions Relating to Sales of Defense Articles and Defense Services* to add a new form. This proposed form would utilize existing systems accessible through the DDTC website. Information regarding this collection of information—including all current supporting materials—can be found at *https://www.reginfo.gov/public/do/PRAMain* by using the search function to enter either the title of the collection or the OMB Control Number. The Department requests comment on the draft version of the form, available at regulations.gov (see Docket information under **ADDRESSES**, above).

3. Considering different reporting scenarios, do you anticipate any difficulties with using the proposed form to submit information pursuant to part 130? Note that the form at the link is mockup of a web application and applicants and suppliers would not submit the actual form as a PDF.

4. Do you expect that annual reporting and the standard form would result in a more precise and accurate accounting of the appropriate payments?

5. Do the proposed changes in this rule alleviate any difficulties that you currently experience when reporting information pursuant to part 130? If not, why?

Regulatory Analysis and Notices

Administrative Procedure Act

This rulemaking is exempt from the rulemaking requirements of § 553 of the Administrative Procedure Act (APA) (5 U.S.C. 553) pursuant to § 553(a)(1) as a military or foreign affairs function of the United States. Nevertheless, and without prejudice to this determination, the Department elects to seek public comment on this rule.

Regulatory Flexibility Act

Since this rule is exempt from the notice-and-comment rulemaking provisions of 5 U.S.C. 553, it does not require analysis under the Regulatory Flexibility Act.

Unfunded Mandates Reform Act of 1995

This rulemaking does not involve a mandate that will result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector of $100 million or more in any year and it will not significantly or uniquely affect small governments. Therefore, no actions were deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995.

Executive Orders 12372 and 13132

This rulemaking will not have substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government. Therefore, in

accordance with Executive Order 13132, it is determined that this amendment does not have sufficient federalism implications to require consultations or warrant the preparation of a federalism summary impact statement. The regulations implementing Executive Order 12372 regarding intergovernmental consultation on Federal programs and activities do not apply to this rulemaking.

Executive Orders 12866 and 13563

Executive Order 12866, as amended by Executive Order 13563, directs agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. The Department specifically welcomes public comment on the impact, including costs and benefits, of this rule. After review by the Office of Management and Budget (OMB), this rule has been deemed a significant regulatory action.

The Department believes that this proposed rule, if finalized, will result in a decrease in burden on the regulated entities. See the discussion of the Paperwork Reduction Act, below.

Executive Order 12988

The Department of State has reviewed this rulemaking in light of sections 3(a) and 3(b)(2) of Executive Order 12988 to eliminate ambiguity, minimize litigation, establish clear legal standards, and reduce burden.

Executive Order 13175

The Department of State has determined that this rulemaking will not have tribal implications, will not impose substantial direct compliance costs on Indian tribal governments, and will not preempt tribal law. Accordingly, the requirements of Executive Order 13175 do not apply to this rulemaking.

Executive Order 14192

This rule is exempt from the requirements of Executive Order 14192 because it relates to a foreign affairs or national security function of the United States.

Paperwork Reduction Act

The Paperwork Reduction Act (PRA) (44 U.S.C. 3501 *et seq.*) requires all Federal agencies to analyze proposed regulations for potential burdens on the regulated community created by provisions in the proposed regulations that require the submission or retention of the information. The information collection requirements must be submitted to the Office of Management and Budget (OMB) for approval. Persons are not required to respond to a collection of information unless it displays a currently valid OMB control number.

This proposed rule contains proposed revisions to the information collection currently approved under OMB control number 1405–0025, *Statement of Political Contributions, Fees, and Commissions Relating to Sales of Defense Articles and Defense Services.*

Summary of Proposed Changes to the Collection

In addition to the current information collection requirements contained in § 130.10, this proposed rule would make the following modifications to the information collection:

- Creation of a form for submission of the information.
- Change to an annual submission requirement, rather than a requirement to submit with an application for authorization.
- Adding a description of the end-item as well as the DDTC authorization number, ITAR exemption, or Department of Defense contract or case number to the information collected.

The revisions in this proposed rule would reduce the number of estimated respondents, based on the calculations from the proposed increase to the monetary thresholds, from 57 to 47. While there would be an increase in estimated response time per respondent from one hour to five hours due to changing to an annual submission, the number of responses would significantly decrease from 450 to 47 for that same reason. Finally, the estimated total burden time would decrease by nearly half, from 450 hours to 235 hours.

According to the Department of Labor's Bureau of Labor Statistics, the average hourly wage (weighted) for a ''Compliance Officer'' is $81.72.[1] This was calculated by multiplying the average hourly wage ($40.86) by 2 to account for overhead costs. Therefore, the Department estimates the annual hour-cost burden to applicants to be $19,204.20 (235 annual burden hours × $81.72), a 48 percent decrease from the current hour-cost burden.

The resultant new estimated total burdens for OMB Control Number 1405–0025 are described below.

- *Title of Information Collection:* Statement of Political Contributions, Fees, and Commissions Relating to Sales of Defense Articles and Defense Services.
- *OMB Control Number:* 1405–0025.
- *Type of Request:* Revision of Currently Approved Collection.
- *Originating Office:* Bureau of Political-Military Affairs, Directorate of Defense Trade Controls, PM/DDTC.
- *Respondents:* Individuals, businesses, or organizations who have paid, or offered or agreed to pay, political contributions or fees or commissions in certain aggregate totals with respect to defense articles or defense services valued in an amount of $1,000,000 or more that are being sold commercially to or for the use of the armed forces of a foreign country or international organization or individuals, businesses, or organizations who enter into a contract with the Department of Defense for the sale of defense articles or defense services valued in an amount of $1,000,000 or more under section 22 of the AECA.
- *Estimated Number of Respondents:* 47.
- *Estimated Number of Responses:* 47.
- *Average Time per Response:* 5 hours.
- *Total Estimated Burden Time:* 235 hours.
- *Frequency:* Annually.
- *Obligation to Respond:* Mandatory.

We are soliciting public comments to permit the Department to:

- Evaluate whether the proposed information collection is necessary for the proper functions of the Department.
- Evaluate the accuracy of our estimate of the time and cost burden for this proposed collection, including the validity of the methodology and assumptions used.
- Enhance the quality, utility, and clarity of the information to be collected.
- Minimize the reporting burden on those who are to respond, including the use of automated collection techniques or other forms of information technology.

Please note that comments submitted in response to this Notice are public record. Before including any detailed personal information, you should be aware that your comments as submitted, including your personal information, will be available for public review.

[1] Source: Bureau of Labor Statistics; Occupational Employment Statistics *https://www.bls.gov/oes/current/oes131041.htm.*

Methodology

Respondents would submit information electronically through DDTC's electronic system using the new form proposed by this rule.

List of Subjects

22 CFR Parts 122 and 123

Arms and munitions, Exports, Reporting and recordkeeping requirements.

22 CFR Part 124

Arms and munitions, Exports, Technical assistance.

22 CFR Part 126

Arms and munitions, Exports, Reporting and recordkeeping requirements, Technical assistance.

22 CFR Part 130

Arms and munitions, Campaign funds, Confidential business information, Exports, Reporting and recordkeeping requirements.

Accordingly, for the reasons set forth above and under the authority of 22 U.S.C. 2778, 2779 the Department of State proposes to amend title 22, chapter I, subchapter M, parts 122, 123, 124, 126, and 130 as follows:

PART 122—REGISTRATION OF MANUFACTURERS AND EXPORTERS

■ 1. The authority citation for part 122 continues to read as follows:

Authority: Sections 2 and 38, Pub. L. 90–629, 90 Stat. 744 (22 U.S.C. 2752, 2778); 22 U.S.C. 2651a; E.O. 13637, 78 FR 16129.

■ 2. Amend § 122.4 by adding note 3 to paragraph (c) to read as follows:

§ 122.4 Notification of changes in information furnished by registrants.

* * * * *

(c) * * *

Note 3 to paragraph (c):

Information on political contributions and fees or commissions, as required by part 130 of this subchapter, must be reported to the Directorate of Defense Trade Controls in accordance with § 130.9(g).

* * * * *

PART 123—LICENSES FOR THE EXPORT AND TEMPORARY IMPORT OF DEFENSE ARTICLES

■ 3. The authority citation for part 123 continues to read as follows:

Authority: Secs. 2, 38, and 71, Pub. L. 90–629, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2797); 22 U.S.C. 2753; 22 U.S.C. 2651a; 22 U.S.C. 2776; Pub. L. 105–261, 112 Stat. 1920; Sec. 1205(a), Pub. L. 107–228; Sec. 520, Pub. L. 112–55; Section 1261, Pub. L. 112–239; E.O. 13637, 78 FR 16129.

■ 4. Amend § 123.1 by removing paragraph (c)(6):

§ 123.1 Requirement for export or temporary import licenses.

* * * * *

(c) * * *

(6) [removed]

* * * * *

PART 124—AGREEMENTS, OFF-SHORE PROCUREMENT, AND OTHER DEFENSE SERVICES

■ 5. The authority citation for part 124 continues to read as follows:

Authority: Secs. 2, 38, and 71, Pub. L. 90–629, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2797); 22 U.S.C. 2651a; 22 U.S.C. 2776; Section 1514, Pub. L. 105–261; Pub. L. 111–266; Section 1261, Pub. L. 112–239; E.O. 13637, 78 FR 16129.

■ 6. Amend § 124.12 by revising paragraph (a)(6) as follows:

§ 124.12 Required information in letters of transmittal.

(a) * * *

(6) A statement of the actual or estimated value of the agreement, including the estimated value of all defense articles to be exported in furtherance of the agreement or amendments thereto.

* * * * *

PART 126—GENERAL POLICIES AND PROVISIONS

■ 7. The authority citation for part 126 continues to read as follows:

Authority: 22 U.S.C. 287c, 2651a, 2752, 2753, 2776, 2778, 2779, 2779a, 2780, 2791, 2797, 10423; sec. 1225, Pub. L. 108–375, 118 Stat. 2091; sec. 7045, Pub. L. 112–74, 125 Stat. 1232; sec. 1250A, Pub. L 116–92, 133 Stat. 1665; sec. 205, Pub. L. 116–94, 133 Stat. 3052; and E.O. 13637, 78 FR 16129, 3 CFR, 2013 Comp., p. 223.

■ 8. Revise § 126.16(m) to read as follows:

§ 126.16 Exemption pursuant to the Defense Trade Cooperation Treaty between the United States and Australia.

* * * * *

(m) *Fees and commissions.* Exporters authorized pursuant to paragraph (b)(2) of this section shall, with respect to each export, transfer, reexport, or retransfer, pursuant to the Defense Trade Cooperation Treaty between the United States and Australia and this section, submit to DDTC information in accordance with § 130.9 of this subchapter relating to political contributions and fees or commissions.

* * * * *

■ 9. Revise § 126.17(m) to read as follows:

§ 126.17 Exemption pursuant to the Defense Trade Cooperation Treaty between the United States and the United Kingdom.

* * * * *

(m) *Fees and commissions.* Exporters authorized pursuant to paragraph (b)(2) of this section shall, with respect to each export, transfer, reexport, or retransfer, pursuant to the Defense Trade Cooperation Treaty between the United States and the United Kingdom and this section, submit to DDTC information in accordance with § 130.9 of this subchapter relating to political contributions and fees or commissions.

* * * * *

PART 130—POLITICAL CONTRIBUTIONS, FEES, AND COMMISSIONS

■ 10. The authority citation for part 130 continues to read as follows:

Authority: Sec. 39, Pub. L. 94–329, 90 Stat. 767 (22 U.S.C. 2779); 22 U.S.C. 2651a; E.O. 13637, 78 FR 16129.

■ 11. Revise § 130.2 to read as follows:

§ 130.2 Applicant.

Applicant means a person who applies to the Directorate of Defense Trade Controls for an authorization required under this subchapter for the export, reexport, or retransfer of defense articles or defense services valued in an amount of $1,000,000 or more which are being sold commercially to or for the use of the armed forces of a foreign country or international organization. This term also includes a person who applied for and was issued the required authorization or who utilized or plans to utilize an exemption in § 126.16 or § 126.17 of this subchapter.

■ 12. Revise § 130.5 to read as follows:

§ 130.5 Political contribution.

Political contribution means a loan, gift, donation or other payment of $1,000 or more made, or offered or agreed to be made, directly or indirectly, whether in cash or in kind, which is:

(a) To or for the benefit of, or at the direction of, any foreign candidate, committee, political party, political faction, or government or governmental subdivision, or any individual elected, appointed or otherwise designated as an employee or officer thereof; and

(b) For the solicitation or promotion or otherwise to secure the conclusion of a sale of defense articles or defense services to or for the use of the armed forces of a foreign country or international organization. Taxes, customs duties, license fees, and other charges required to be paid by applicable law or regulation are not regarded as political contributions.

■ 13. Revise § 130.6 to read as follows:

§ 130.6 Fee or commission.

(a) *Fee or commission* means, except as provided in paragraph (b) of this section, a loan, gift, donation or other payment of $1,000 or more made, or offered or agreed to be made directly or indirectly, whether in cash or in kind, and whether or not pursuant to a written contract, which is:

(1) To or at the direction of any person, irrespective of nationality, whether or not employed by or affiliated with an applicant, a supplier or a vendor; and

(2) For the solicitation or promotion or otherwise to secure the conclusion of a sale of defense articles or defense services to or for the use of the armed forces of a foreign country or international organization.

(b) The term fee or commission does not include:

(1) A political contribution or a payment excluded by § 130.5 from the definition of political contribution;

(2) A normal salary, excluding contingent compensation, established at an annual rate and paid to a regular employee of an applicant, supplier or vendor;

(3) General advertising or promotional expenses not directed to any particular sale or purchaser; or

(4) Payments made, or offered or agreed to be made, solely for the purchase by an applicant, supplier or vendor of specific goods or technical, operational or advisory services, which payments are not disproportionate in amount with the value of the specific goods or services actually furnished.

■ 14. Revise § 130.7 to read as follows:

§ 130.7 Supplier.

Supplier means a person who enters into a contract with the Department of Defense for the sale of defense articles or defense services valued in an amount of $1,000,000 or more under § 22 of the Arms Export Control Act (22 U.S.C. 2762).

■ 15. Amend § 130.8 by revising the introductory text to paragraph (a) and paragraph (a)(1) to read as follows:

§ 130.8 Vendor.

(a) *Vendor* means a distributor or manufacturer who, directly or indirectly, furnishes to an applicant or supplier defense articles valued in an amount of $1,000,000 or more which are end-items or major components as defined in § 120.45 of this subchapter. It also means any person who, directly or indirectly, furnishes to an applicant or supplier defense articles or services valued in an amount of $1,000,000 or more when such articles or services are to be delivered (or incorporated in defense articles or defense services to be delivered) to or for the use of the armed forces of a foreign country or international organization under:

(1) A sale requiring authorization from the Directorate of Defense Trade Controls under this subchapter; or

* * * * *

■ 16. Revise § 130.9 to read as follows:

§ 130.9 Annual reporting requirement.

(a) *Applicant obligation to report.* An applicant must submit an annual report to the Directorate of Defense Trade Controls (DDTC) if the applicant or its vendors have paid, or offered or agreed to pay, in respect of any sale:

(1) Political contributions in an aggregate amount of $10,000 or more; or

(2) Fees or commissions in an aggregate amount of $200,000 or more.

(3) The requirements of paragraph (a) do not apply in the case of a sale for which all the information specified in § 130.10 has already been reported to DDTC.

(b) *Timing and content of annual applicant report.* If the applicant or its vendors have paid, or offered or agreed to pay, political contributions or fees or commissions as specified in paragraphs (a)(1) or (a)(2) of this section, the applicant must furnish the information specified in § 130.10 in a report to DDTC. The report shall be submitted at the time of the applicant's registration renewal and include all qualifying payments, or offers or agreements to pay, since the date of the applicant's most recent registration or renewal. If all required information cannot be furnished at the time of submission, the applicant shall include in its report an explanation as to what information cannot be furnished and why.

(c) *Supplier obligation to report.* A supplier must submit an annual report to DDTC if the supplier or its vendors have paid, or offered or agreed to pay, in respect of any sale:

(1) Political contributions in an aggregate amount of $10,000 or more; or

(2) Fees or commissions in an aggregate amount of $200,000 or more.

(d) *Timing and content of supplier annual report.* If the supplier or its vendors have paid, or offered or agreed to pay, political contributions or fees or commissions as specified in paragraphs (c)(1) or (c)(2) of this section, the supplier must furnish the information specified in § 130.10 in a report to DDTC. The report shall be submitted at the time of the supplier's registration renewal or such earlier date as may be specified by the Department of Defense. If the supplier is not registered with DDTC, the supplier must submit such report by the last day of the federal fiscal year, September 30. The report shall include all qualifying payments, or offers or agreements to pay, since the date of the supplier's most recent report made pursuant to this part.

(e) *Aggregate computation of political contributions.* Any political contributions which are paid, or offered or agreed to be paid, by or on behalf of, or at the direction of, any person to whom the applicant, supplier or vendor has paid, or offered or agreed to pay, a fee or commission in respect of a sale, must be included in the total computation of political contributions for that sale under this section. Any such political contributions are deemed for purposes of this part to be political contributions by the applicant, supplier or vendor who paid or offered or agreed to pay the fee or commission.

(f) *Reporting for previous periods.* Any applicant or supplier required to furnish information pursuant to paragraphs (a) or (c) of this section, should include the information relating to all qualifying payments, or offers or agreements to pay, that occur during the standard reporting period in the annual submission. In the event of new information about a previous reporting period, an applicant or supplier may be required to furnish a supplementary or interim report pursuant to § 130.11.

(g) *Reporting after registration expiration, cessation of operations, merger, or acquisition.* An applicant or supplier required to furnish information pursuant to paragraphs (a) or (c) of this section, whose registration expires, who ceases to operate, or who merges with, acquires, or is acquired by another, must submit such a report as follows:

(1) An applicant or supplier that ceases to operate, or whose registration expires, must submit a report to DDTC within 30 days of the cessation of operations or the registration expiration date, respectively, that includes all information specified in § 130.10 that has not been furnished in a previous report submitted pursuant to this part.

(2) The parent, acquiring entity, or new entity formed when a registrant merges with another company or acquires, or is acquired by, another company or a subsidiary or division of another company, must furnish to DDTC for the absorbed or acquired company all of the information specified in § 130.10 that has not been furnished to DDTC in a previous report submitted pursuant to this part, no later than 6 months after the effective date of the merger or acquisition. After that report, the parent, acquiring entity, or new entity shall furnish all subsequent

information with its annual report during registration renewal pursuant to part 122 of this subchapter.

(h) *Form submission.* An applicant or supplier must furnish the information specified in § 130.10 using the reporting form provided by DDTC and submit the report using the DDTC website.

■ 17. Revise and republish § 130.10 to read as follows:

§ 130.10 Required information.

(a) *Information to be reported to DDTC.* Persons required to submit a report under § 130.9 must furnish to the Directorate of Defense Trade Controls (DDTC) an annual report signed by a senior officer (*e.g.,* chief executive officer, president, secretary, partner, member, treasurer, general counsel) who has been empowered by the applicant or supplier to sign such documents, including the following information:

(1) The total contract price of the sale to the foreign purchaser; any relevant Directorate of Defense Trade Controls authorization number or exemption, or Department of Defense contract or case number; and the end-item associated with the sale;

(2) The name, nationality, address and principal place of business of the applicant or supplier and, if applicable, the employer and title;

(3) The name, nationality, address and principal place of business, and if applicable, employer and title of each foreign purchaser, including the ultimate end-user involved in the sale;

(4) Except as provided in paragraph (c) of this section, the following information must be provided with respect to such sale:

(i) The amount of each political contribution paid, or offered or agreed to be paid, or the amount of each fee or commission paid, or offered or agreed to be paid;

(ii) The date or dates on which each reported amount was paid, or offered or agreed to be paid;

(iii) The recipient of each such amount paid, or intended recipient if not yet paid;

(iv) The person who paid, or offered or agreed to pay such amount; and

(v) The aggregate amounts of political contributions and of fees or commissions, respectively, which shall have been reported.

(b) *Specified information relating to certain payments and recipients.* In responding to paragraph (a)(4) of this section, the report must:

(1) With respect to each payment reported, indicate whether such payment was in cash or in kind. If in kind, it must include a description and valuation thereof. Where precise amounts are not available because a payment has not yet been made, an estimate of the amount offered or agreed to be paid must be provided;

(2) With respect to each recipient, state:

(i) Its name;

(ii) Its nationality;

(iii) Its address and principal place of business;

(iv) Its employer and title; and

(v) Its relationship, if any, to the applicant, supplier, or vendor, and to any foreign purchaser or end-user.

(c) *Payments that may be labeled as miscellaneous.* In submitting a report required by § 130.9, the detailed information specified in paragraph (a)(4) and (b) of this section need not be included if the payments do not exceed:

(1) $5,000 in the case of political contributions; and

(2) $100,000 in the case of fees or commissions.

In lieu of reporting detailed information with respect to such payments, the aggregate amount thereof must be reported, identified as miscellaneous political contributions or miscellaneous fees or commissions, as the case may be.

(d) *Required responses.* Every person required to furnish the information specified in paragraphs (a) and (b) of this section must respond fully to each subdivision of those paragraphs and, where the correct response is ''none'' or ''not applicable,'' must so state.

(e) *Senior officer certification.* The senior officer empowered to sign such documents shall include a certification that the submission is complete and accurate.

■ 18. Revise § 130.11 to read as follows:

§ 130.11 Supplementary and interim reports.

(a) *Obligation to submit supplementary report.* An applicant or supplier must furnish to the Directorate of Defense Trade Controls (DDTC) the information specified in § 130.10 in a supplementary report when the applicant or supplier submitted an annual report pursuant to § 130.9 for a reporting period and either:

(1) Subsequent developments cause the information initially reported with respect to that sale to no longer be accurate or complete (*e.g.,* where an applicant is made aware of a payment or offer to pay made during a previous reporting period and not included in a prior annual report, or where a payment actually made is substantially different in amount from a previously reported estimate of an amount offered or agreed to be paid, or where certain information specified in § 130.10 could not be obtained at the time of annual submission); or

(2) Additional details are requested by DDTC with respect to any miscellaneous payments reported under § 130.10(c).

(b) *Timing and content of supplementary report.* A supplementary report required under paragraph (a)(1) of this section must be furnished to DDTC within 30 days of discovering that the information previously reported to DDTC is no longer accurate or complete. A supplementary report required under paragraph (a)(2) of this section must be furnished to DDTC within 30 days of such request. All supplementary reports must include the information specified in § 130.10 required or requested by DDTC and which was not previously reported.

(c) *Obligation to submit interim report.* Every applicant or supplier must furnish to DDTC the information specified in § 130.10 in an interim report if the applicant or supplier did not submit an annual report pursuant to § 130.9 for a reporting period and later discovers that the applicant or its vendors or the supplier or its vendors have paid, or offered or agreed to pay, political contributions or fees or commissions in an aggregate total specified in § 130.9 during that reporting period.

(d) *Timing and content of interim report.* An interim report required under paragraph (c) of this section must be furnished to DDTC within 30 days after discovering the information that, if known to the applicant or supplier at the time, would have obliged the applicant or supplier to submit an annual report pursuant to § 130.9. Any interim report furnished under paragraph (c) must, in addition to the information specified in § 130.10, include a detailed statement of the reasons why applicant or supplier did not furnish the information at the time specified in § 130.9.

(e) *Interaction of supplementary or interim report with annual reporting requirement.* An applicant or supplier who furnishes a supplementary report or an interim report to DDTC pursuant to paragraphs (a) or (c) of this section is not released from any obligation to furnish an annual report to DDTC as specified in § 130.9.

■ 19. Revise § 130.12 to read as follows:

§ 130.12 Information to be furnished by vendor to applicant or supplier.

(a) *Initial vendor statement.* In order to determine whether it is obliged under § 130.9 to furnish the information specified in § 130.10 with respect to a sale, the applicant or supplier must obtain from each vendor, from or

through whom the applicant or supplier acquired defense articles or defense services forming the whole or a part of the sale, a statement containing a full disclosure by the vendor of all political contributions or fees or commissions paid, by the vendor with respect to such sale. Such disclosure must include all the information relating to the vendor that enables the applicant or supplier to comply fully with §§ 130.9 and 130.10. If so required, the applicant or supplier must include the information furnished by each vendor in the report to DDTC made pursuant to § 130.9.

(b) *Time limit for an initial statement.* Any vendor which has been requested by an applicant or supplier to provide an initial statement under paragraph (a) of this section must, except as provided in paragraph (c) of this section, provide such statement in a timely manner and not later than 20 days after receipt of such request.

(c) *Abbreviated vendor statement.* If the vendor believes that furnishing information to an applicant or supplier in a requested statement would unreasonably risk injury to the vendor's commercial interests, the vendor may instead provide an abbreviated statement disclosing only the aggregate amount of all political contributions and the aggregate amount of all fees or commissions which have been paid, or offered or agreed to be paid, or offered or agreed to be paid, by the vendor with respect to the sale. Any abbreviated statement provided to an applicant or supplier under this paragraph must be accompanied by a certification that the requested information will be reported by the vendor directly to DDTC at the time of the vendor's registration renewal or, if the vendor is not registered with DDTC, by the last day of the federal fiscal year, September 30. The vendor must report to DDTC all information the vendor would otherwise have been required to report to the applicant or supplier under this section. Any report must clearly identify the sale with respect to which the reported information pertains.

(d) *Vendor failure to provide initial statement.* If upon the 25th day after the date of its request to any vendor, an applicant or supplier has not received from the vendor the initial statement required by paragraph (a) of this section, the applicant or supplier must submit to DDTC a signed statement attesting to:

(1) The manner and extent of the applicant's or supplier's attempt to obtain from the vendor the initial statement required under paragraph (a) of this section;

(2) Vendor's failure to comply with this section; and

(3) The amount of time elapsed between the date of the applicant's or supplier's request to the vendor and the date of the signed statement;

(e) *Applicant or supplier obligation if vendor fails to provide statement.* The failure of a vendor to comply with this section does not relieve any applicant or supplier otherwise required by § 130.9 to submit a report to DDTC from the obligation to submit such a report.

Thomas G. DiNanno,

Under Secretary, Arms Control and International Security, Department of State.

[FR Doc. 2026–12019 Filed 6–12–26; 8:45 am]

BILLING CODE 4710–25–P

ENVIRONMENTAL PROTECTION AGENCY

40 CFR Parts 174 and 180

[EPA–HQ–OPP–2026–0332; FRL–13201–02–OCSPP]

Receipt of Pesticide Petitions Filed for Residues of Pesticide Chemicals in or on Various Commodities—February 2026

AGENCY: Environmental Protection Agency (EPA).

ACTION: Notice of filing of petitions and request for comment.

SUMMARY: This document announces the Agency's receipt of and solicits public comment on initial filings of pesticide petitions requesting the establishment or modification of regulations for residues of pesticide chemicals in or on various commodities. The Agency is providing this notice in accordance with the Federal Food, Drug, and Cosmetic Act (FFDCA). EPA uses the month and year in the title to identify when the Agency compiled the petitions identified in this notice of filing. Unit II. of this document identifies certain petitions received in 2023, 2024, 2025 and 2026 that are currently being evaluated by EPA, along with information about each petition, including who submitted the petition and the requested action.

DATES: Comments must be received on or before July 15, 2026.

ADDRESSES: Submit your comments, identified by docket identification (ID) number and the pesticide petition (PP) of interest identified in Unit II. of this document, online at *https://www.regulations.gov.* Follow the online instructions for submitting comments. Do not submit electronically any information you consider to be Confidential Business Information (CBI) or other information whose disclosure is restricted by statute. Additional instructions on commenting on and visiting the docket, along with more information about dockets generally, is available at *https://www.epa.gov/dockets.*

FOR FURTHER INFORMATION CONTACT: Each application summary in Unit II. specifies a contact division. The appropriate division contacts are identified as follows:

- RD (Registration Division) (Mail Code 7505T); Charles Smith; main telephone number: (202) 566–1030; email address: *RDFRNotices@epa.gov.*

SUPPLEMENTARY INFORMATION:

I. Executive Summary

A. Does this action apply to me?

This action provides information that is directed to the public in general.

B. What is the Agency's authority for taking this action?

EPA regulations for residues of pesticide chemicals in or on various food commodities are established under section 408 of the Federal Food, Drug, and Cosmetic Act (FFDCA), 21 U.S.C. 346a. FFDCA section 408(d)(3), 21 U.S.C. 346a(d)(3), requires EPA to publish a notice of receipt of these petitions in the **Federal Register** and provide an opportunity for public comment on the requests.

C. What action is the Agency taking?

As specified in FFDCA section 408(d)(3), 21 U.S.C. 346a(d)(3), EPA is publishing notice of the receipt of pesticide petitions filed under FFDCA section 408 that request the establishment or modification of regulations for residues of pesticide chemicals in or on various food commodities. The Agency is taking public comments on the requests before responding to the petitioner. Pursuant to 40 CFR 180.7(f), a summary of the petition identified in this document, prepared by the petitioner, is included in a docket. EPA has determined that the pesticide petitions described in this document contain data or information prescribed in FFDCA section 408(d)(2), 21 U.S.C. 346a(d)(2), and 40 CFR 180.7(b); however, EPA has not fully evaluated the sufficiency of the submitted data at this time or whether the data supports granting the pesticide petitions. After considering the public comments, EPA intends to evaluate whether and what action may be warranted. Additional data may be needed before EPA can make a final determination on these pesticide petitions.