



Department of Defense INSTRUCTION

NUMBER 2040.02
July 10, 2008

USD(P)

SUBJECT: International Transfers of Technology, Articles, and Services

References: See Enclosure 1

1. PURPOSE. This Instruction:

a. Reissues DoD Directive 2040.2 (Reference (a)) as a DoD Instruction pursuant to the authority of the Under Secretary of Defense for Policy (USD(P)) in Deputy Secretary of Defense Memorandum (Reference (b)).

b. Establishes policy, assigns responsibility, and provides instructions for the international transfer of dual-use and defense-related technology, articles, and services, by implementing relevant portions of section 1701 et seq. of title 50, United States Code (U.S.C.) (Reference (c)); section 2751 et seq. of title 22, U.S.C. (Reference (d)); National Disclosure Policy No. 1 (Reference (e)); DoD Directive 5230.11 (Reference (f)); DoD Directive 2010.6 (Reference (g)); DoD Directive 5105.72 (Reference (h)); National Security Directive No. 42 (Reference (i)); National Security Telecommunications and Information Systems Security Policy No. 8 (Reference (j)); DoD Directive 5530.3 (Reference (k)); DoD Instruction 5000.2 (Reference (l)); DoD Directive 5200.39 (Reference (m)); section 2537 of title 10, U.S.C. (Reference (n)); DoD 5105.38-M (Reference (o)); DoD Directive 5106.01 (Reference (p)); DoD Instruction 5505.2 (Reference (q)); parts 730- 744 of title 15, Code of Federal Regulations (CFR) (Reference (r)); parts 120-130 of title 22, CFR (Reference (s)); and section 1342b (a)(3) of title 8, U.S.C. (Reference (t)).

c. Directs the use of a DoD automated export license system.

2. APPLICABILITY. This Instruction:

a. Applies to Office of the Secretary of Defense, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (IG DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

b. Applies to all means of technology transfer and shall be implemented through such processes as dual-use export licensing; munitions export licensing; security cooperation (including Foreign Military Sales (FMS)); exceptions to National Disclosure Policy; and DoD research, development, and acquisition activities, including international agreements.

c. Does not affect policies, procedures, and responsibilities contained in References (e) and (f) concerning disclosures of classified military information.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. Dual-use and defense-related technology shall be treated as valuable national security resources, to be protected and transferred only in pursuit of national security and foreign policy objectives. Those objectives include ensuring that: critical U.S. military technological advantages are preserved; transfers which could prove detrimental to U.S. security interests are controlled and limited; proliferation of weapons of mass destruction and their means of delivery are prevented; and diversion of defense-related goods to terrorists is prevented.

b. The sharing of defense technology, properly controlled, is a valuable way to ensure our allies participate with the United States in future military operations. In applying export control and technology security policies, due recognition will be given to the importance of interoperability with allies and coalition partners and to direct and indirect impacts on the defense industrial base in accordance with Reference (g). Consistent with this policy, and in recognition of the importance of international trade and scientific and technological cooperation, the Department of Defense shall apply export control and other technology security policies and procedures in a way that balances economic and scientific interests with those of national security.

c. In considering DoD interests in technology and the means by which those interests are protected, the Department recognizes the increasing velocity of scientific and technological change, as well as significant changes in the ways in which scientific research and technological development are carried out, in considering both defense interests with respect to technology and the means by which those interests are protected and advanced.

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES

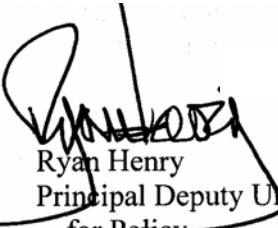
a. While recognizing that constant and rapid changes pose difficult challenges in assessments, formulation of policy options, and implementation of policies, the DoD

Components will utilize all resources available to achieve DoD and United States Government goals and objectives in transfers of technology, articles, and services.

b. See Enclosure 3 for detailed procedures.

7. RELEASABILITY. UNLIMITED. This Instruction is approved for public release. Copies may be obtained through the Internet from the DoD Issuances Web Site at <http://www.dtic.mil/whs/directives>.

8. EFFECTIVE DATE. This Instruction is effective immediately.



Ryan Henry
Principal Deputy Under Secretary of Defense
for Policy

Enclosures

1. References
 2. Responsibilities
 3. Procedures
 4. Release of Controlled Technology or Technical Data to Foreign Persons
- Glossary

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 2040.2, "International Transfers of Technology, Goods, Services, and Munitions," January 17, 1984 (hereby canceled)
- (b) Deputy Secretary of Defense Memorandum, "Delegations of Authority," November 30, 2006¹
- (c) Section 1701 et seq. of title 50, United States Code
- (d) Section 2751 et seq. of title 22, United States Code
- (e) National Disclosure Policy No. 1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," October 1, 1988²
- (f) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
- (g) DoD Directive 2010.6, "Material Interoperability with Allies and Coalition Partners," November 10, 2004
- (h) DoD Directive 5105.72, "Defense Technology Security Administration (DTSA)," July 28, 2005
- (i) National Security Directive No. 42, "National Policy for the Security of National Security Telecommunications and Information Systems", July 5, 1990³
- (j) National Security Telecommunications and Information Systems Security Policy No. 8, "National Policy Governing the Release of Information Systems Security (INFOSEC) Products or Associated INFOSEC Information to Foreign Governments," February 13, 1997⁴
- (k) DoD Directive 5530.3, "International Agreements," June 11, 1987
- (l) DoD Instruction 5000.2 "Operation of the Defense Acquisition System." May 12, 2003
- (m) DoD Directive 5200.39, "Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection," September 10, 1997
- (n) Sections 134 et seq. and 2537 of title 10, United States Code
- (o) DoD 5105.38-M, "Security Assistance Management Manual," October 3, 2003
- (p) DoD Directive 5106.01, "Inspector General of the Department of Defense," April 13, 2006
- (q) DoD Instruction 5505.2, "Criminal Investigations of Fraud Offenses," February 6, 2003
- (r) Parts 730-774 as amended, of title 15, Code of Federal Regulations
- (s) Parts 120-130 of title 22, Code of Federal Regulations
- (t) Section 1324b (a)(3) of title 8, United States Code
- (u) DoD Instruction S-5230.28, "Low Observable (LO) and Counter Low Observable (CLO) Programs," October 1, 2002⁵

¹Copies may be obtained from USD(P)

² Classified document; responsibility of Executive Secretariat of National Disclosure Policy Committee

³ Classified document; responsibility of National Security Council

⁴ For Official Use Only; responsibility of Committee on National Security Systems Secretariat, National Security Agency

⁵ Classified document; responsibility of Director of Special Programs, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics

- (v) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987
- (w) DoD Directive 5230.25, "Withholding of Unclassified Technical Data From Public Disclosure," November 6, 1984
- (x) DoD 5200-1.R, "Information Security Program," January 1997
- (y) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005
- (z) Defense Federal Acquisition Regulations Supplement⁶

⁶ Copies may be obtained from <http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html>

ENCLOSURE 2

RESPONSIBILITIES

1. USD(P). The USD(P) shall:

a. Provide policy oversight for all DoD activities and efforts related to international technology transfer according to section 134(b) of Reference (n) and Reference (k).

b. Develop, coordinate, and provide policy direction and overall management for DoD technology security programs and policy on international technology transfer, to include dual-use and munitions export licensing and other export controls, international cooperation in technology security matters, and support for enforcement and intelligence activities in this area.

c. Consider and establish, as appropriate, additional policies and procedures to protect technology from use and exploitation by adversaries, potential adversaries, or countries of concern.

d. Provide and maintain automated processes and technologically advanced systems for export license review, including electronic data transfer to and from other U.S. Government departments and agencies, as requirements and funding permit.

2. ASSISTANT SECRETARY OF DEFENSE FOR GLOBAL SECURITY AFFAIRS

(ASD(GSA)). The ASD(GSA), under the authority, direction, and control of the USD (P), shall:

a. Monitor compliance with this Instruction through the Deputy Under Secretary of Defense for Technology Security Policy and National Disclosure Policy (DUSD(TSP&NDP)).

b. Serve as the DoD representative to the Committee on Foreign Investment in the United States (CFIUS) or designate a representative in his/her stead.

c. Serve as the DoD representative to the Advisory Committee on Export Policy.

3. DUSD(TSP&NDP). The DUSD(TSP&NDP), under the authority, direction, and control of the ASD(GSA), shall:

a. Serve concurrently as Director, Defense Technology Security Administration (DTSA), according to section 134(b) of Reference (n) and Reference (h).

b. Prepare technology transfer control and enforcement policy guidance and coordinate overall application of DoD policy.

- c. Represent the Department of Defense in interagency, national, and international forums concerning policy for technology transfer, export control, and enforcement matters.
- d. Serve, or designate a representative to serve, as the primary DoD point of contact for technology security policy matters for foreign governments, international agencies, other Federal agencies, interagency groups, industry, and DoD Components.
- e. Act, except as otherwise delegated, as the DoD receiving point for dual-use and munitions export license applications requiring DoD review.
- f. Conduct policy reviews on export licenses or foreign requests for technology, articles, or services.
- g. Prepare the coordinated DoD position for those dual-use and munitions export license applications reviewed by the Department of Defense.
- h. Issue coordinated DoD recommendations on dual-use and munitions export license applications reviewed by the Department of Defense to the Departments of State and Commerce.
- i. As appropriate, participate in the development, review, and negotiation of international agreements to address technology transfer and security concerns in accordance with this Instruction.
- j. Assess, with the support of the Director, Defense Intelligence Agency (DIA), and the National Disclosure Policy Committee, recipient nations' dependability and reliability in both maintaining control over controlled technology, article(s), and services that originate in the United States, and in securing prior U.S. Government approval for further transfers.
- k. Support U.S. intelligence and enforcement authorities, as appropriate, in their efforts to halt or control the illicit flow of dual-use and defense-related technology, article(s), and services to adversaries, potential adversaries, and countries of concern.
- l. Coordinate and issue, for the ASD(GSA), DoD positions on matters concerning CFIUS cases.
- m. Assist in identification and definition of items on the Militarily Critical Technologies List (MCTL) that should be controlled for export and assist with necessary guidelines for such.
- n. Collaborate with the Defense Security Cooperation Agency (DSCA) in developing consistent and harmonized approaches to technology transfer in the provision of technology, articles, and services to foreign governments, accomplished either through FMS or direct commercial sales.
- o. Provide technical and policy analyses and recommendations on requests for exceptions to Reference (e) and DoD Instruction S-5230.28 (Reference (u)).

p. Develop DoD policy on DoD use of International Traffic in Arms Regulations (ITAR) exemptions in accordance with the process detailed in the regulations.

q. Maintain a comprehensive technical database for defense technology, article(s), and services transfer cases.

4. UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, & LOGISTICS (USD(AT&L)). The USD(AT&L) shall:

a. Manage overall DoD acquisition efforts related to technology, articles, services, and munitions transfer, including armaments cooperation programs in accordance with Reference (k).

b. Oversee implementation of DoD technology transfer policy for all research, development, and acquisition matters in accordance with this Instruction and Reference (l). Ensure Technology Protection Plans and Program Protection Plans include provisions for the continual protection of Critical Technology Information and Critical Program Information when transferred in an international cooperative venture according to Reference (l).

c. Supervise and direct the MCTL. Ensure the MCTL maintains relevance and currency in order to enable the DoD Components to utilize the MCTL in making technology transfer decisions and recommendations for control of critical technologies when included in an international program.

d. Provide advice to the USD(P), and, when requested by USD(P), to the Under Secretary of State for Arms Control and International Security, and the Under Secretary of Commerce for Industry and Security, on technological aspects of technology transfer, security cooperation, export controls, and technology security in accordance with References (e) and (u).

e. Act as the DoD point of contact with industry, other Federal agencies, interagency groups, the DoD Components, academia, and appropriate international forums for defense research, development, and acquisition matters.

f. Manage the overall DoD process for USD(AT&L)-related international agreements in accordance with References (k) and (l).

g. Support the U.S. intelligence and enforcement communities in their efforts to halt or control the illicit flow of controlled dual-use and defense-related technology, technical data, articles, services, and munitions to adversaries, potential adversaries, and countries of concern.

h. Provide recommendations on CFIUS cases to the ASD(GSA) or his designee.

5. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I) shall:

a. Provide advice and assistance as appropriate to the USD(P) and USD(AT&L) concerning transfers of technology, articles, services, and programs dealing with such transfers, including those which may significantly affect defense intelligence, counterintelligence, and security programs.

b. Develop, coordinate, and oversee the implementation of DoD policy, programs, and guidance for security related to transfers of technology, articles, and services as well as the security of defense research and technology which may be transferred.

6. DIRECTOR, DIA. The Director, DIA, under the authority, direction, and control of the USD(I), in addition to the responsibilities in paragraph 11, shall:

a. Formulate DoD-coordinated intelligence assessments concerning types and numbers of illegal transfers of dual-use and defense-related technology, articles, services, and associated transfer mechanisms.

b. Designate a point of contact to represent the DIA on dual-use and defense-related technology, articles, and services transfer matters.

c. Conduct analyses and provide intelligence assessments of risks to U.S. national security on dual-use and defense-related technology, articles, and services transfer cases, including those related to foreign investment in, or acquisition of, U.S. and U.S.-based companies.

d. Assess foreign availability of dual-use and defense-related technology, articles, and services proposed for transfer.

e. Conduct end-user checks on the declared ultimate consignee on dual-use and defense-related technology, articles, and services transfer cases.

f. Provide intelligence expertise in interagency, national, and international forums on dual-use and defense-related technology, articles, and services transfer matters.

g. Provide intelligence concerning the total effect of transfers of dual-use and defense-related technology, articles, and services on U.S. security.

h. Assist in identifying and assessing critical technologies.

i. Coordinate an assessment of risk of diversion of critical technologies in CFIUS cases, in accordance with Reference (m).

7. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. The Chairman of the Joint Chiefs of Staff shall:

a. Conduct and provide operational and military mission impact assessments on the transfer of dual-use and defense-related technology, articles, and services, as requested.

b. Provide operational expertise and military judgments in interagency, national, and international forums on dual-use and defense-related technology, articles, and services transfer matters.

c. Provide recommendations on CFIUS cases to the ASD(GSA) or his designee.

8. DIRECTOR, DSCA. The Director, DSCA, under the authority, direction, and control of the USD(P), in addition to the responsibilities in paragraph 11, shall:

a. Advise DTSA of proposed transfers of significant new technologies and/or weapons systems and determinations of whether significant items must be sold exclusively through FMS and determinations that specific sales must be exclusively through FMS in accordance with Reference (o).

b. Provide DTSA, when requested, with recommendations on munitions export licenses which may have implications for FMS.

9. DIRECTOR, NATIONAL SECURITY AGENCY (NSA). The Director, NSA, under the authority, direction, and control of the USD(I), in addition to the responsibilities in paragraph 11, shall, in his capacity as the National Manager for National Security Telecommunications and Information Systems in accordance with Reference (i), coordinate all releases of Information Systems Security/Information Assurance (INFOSEC/IA) products or information as authorized by Reference (j).

10. IG DoD. The IG DoD, in addition to the responsibilities in paragraph 11, shall:

a. In accordance with References (p) and (q), provide oversight of component Inspector General audits, evaluations, inspections, and law enforcement activities for compliance with this Instruction and related issuances.

b. Develop a uniform system of periodic inspections, using the existing Military Department and Agency inspection process, for research, development, test and evaluation site compliance with directives or instructions concerning technology protection.

11. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

a. Designate a point of contact in their respective components for dual-use and defense-related technology, articles, and services transfer matters.

- b. Conduct assessments of proposed dual-use and defense-related technology, articles, and services transfer cases as requested and provide coordinated positions to the Director, DTSA.
- c. Assist in identifying and assessing critical technology and in supporting DoD participation in export-control list reviews.
- d. Assign personnel and resources to process CFIUS cases effectively.
- e. Consistent with this Instruction and Reference (k), coordinate development and negotiation of international agreements pertaining to transfers of dual-use and defense-related technology, articles, and services.
- f. Advise DTSA and DSCA of determinations of whether significant items must be sold exclusively through FMS in accordance with Reference (o).
- g. Report to the appropriate Defense criminal investigative organization suspected instances of fraud, abuse, bribery, or other violations of law related to the Arms Export Control Act and implementing regulations; other laws governing exports or illicit diversion of U.S. export-controlled technology, articles, or services; or other violations of law or regulation pertaining to DoD programs and operations for investigation in accordance with Reference (q).

ENCLOSURE 3

PROCEDURES

1. INTERNATIONAL TRANSFERS OF TECHNOLOGY, ARTICLES, AND SERVICES.

The DoD Components, within their respective authorities, shall:

- a. Manage and participate in management of transfers of technology, articles (including components), and services, consistent with U.S. foreign policy and national security objectives. These objectives include, but are not limited to, regional security, non-proliferation efforts and policies, counterterrorism policies, human rights concerns, and international commitments.
- b. Consider the effects of transfers and denials of transfers of technology, articles, and services on the relative technological advantage of U.S. and allied and coalition warfighting and other operational capabilities.
- c. Control and participate in controlling, as appropriate, export of technology, articles, and services that contribute to the military potential of any country or countries, groups, or individuals that could prove detrimental to U.S. national security or critical interests.
- d. Facilitate and expedite sharing of dual-use and defense-related technology with allies, coalition partners, and other friendly nations able and willing to protect such technology and, as appropriate, in response to the needs of U.S. foreign policy and national security.
- e. Facilitate and foster cooperation with allies, coalition partners, and friendly nations in fundamental research, technological development, and defense exploitation of commercial technologies.
- f. Give special attention to rapidly emerging technologies to protect against any possibility that militarily-useful technology might become available to adversaries, potential adversaries, or countries of concern before adequate safeguards can be implemented.
- g. Seek to strengthen other countries' procedures for protecting sensitive, dual-use, defense, and defense-related technology and to improve our own procedures through improved international cooperation and exchanges of information.
- h. Process export license requests through a single DoD automated export licensing system and/or other technologically-advanced means, to assist decision makers and analysts in reviewing, disseminating, and coordinating on export license cases and relevant materials. Export data should be exchanged among U.S. Government agencies through protected electronic means.

2. INTERNATIONAL CONTROLS ON TRANSFERS OF TECHNOLOGY, ARTICLES, AND SERVICES

a. DoD Components shall seek to strengthen and increase the efficiency of international controls on transfers of sensitive technology, articles, and services through multilateral and bilateral modes of cooperation. Multilateral cooperation may be accomplished through international organizations, institutions, regimes, groups, committees, or ad hoc arrangements, including, but not limited to:

(1) The Wassenaar Arrangement on Conventional Arms and Dual-use Goods and Technologies for control of transfers of conventional arms and dual-use article(s) and technologies.

(2) The Missile Technology Control Regime, for control of missile-related technologies and components, and certain unmanned air vehicles.

(3) The Nuclear Suppliers Group, for control of nuclear-related technology and materials.

(4) The Australia Group, for control of chemical weapons; chemical weapons precursors; biological agents; and chemical equipment, technology, components, and materials that can be used in the manufacture of chemical, toxin, or biological weapons.

(5) The United Nations, whose bodies may impose and administer sanctions or control regimes, and its affiliated organizations and agencies, such as the International Atomic Energy Agency, as well as reporting through those bodies, such as the United Nations Transparency in Armament.

b. The DoD Components concerned with strategic trade, dual-use, and munitions policy shall seek to rationalize and strengthen international controls on sensitive technology, articles, and services by:

(1) Promoting rationalization and currency of control lists for articles and technologies of concern such as the MCTL (Reference (h)).

(2) Encouraging effective enforcement of international controls.

(3) Considering thresholds for items on international control lists beyond which technology and article(s) cannot be transferred to countries of concern.

(4) Promoting other measures that rationalize and strengthen international organizations and regimes in furtherance of U.S. national security, allied and coalition security, and technology security objectives.

3. RELEASE OF INFOSEC/IA PRODUCTS. In accordance with Reference (i), any release of INFOSEC/IA products or information shall be specifically authorized by the Committee on National Security Systems under the conditions and requirements stated in Reference (j). The inclusion of INFOSEC/IA information in weapons, communications, or other major defense systems, to provide a complete package for FMS, or as initiatives to promote international competition for a systems procurements, are not, in and by themselves, acceptable justifications for seeking release of those products or information.

ENCLOSURE 4

RELEASE OF CONTROLLED TECHNOLOGY OR TECHNICAL DATA TO FOREIGN
PERSONS

1. References (r) and (s) establish the following policies and procedures:

a. Any release or disclosure of controlled technology or technical data to any foreign person, whether it occurs in the United States or abroad, is deemed to be an export, requiring either an export license (for dual-use items) or an authorization for disclosure (for munitions list items). Foreign persons include foreign individuals, corporations, government agencies, or other foreign entities.

b. Controlled technology or technical data is considered to be released or disclosed when information is transferred to foreign persons by means of:

(1) A visual inspection;

(2) An oral exchange;

(3) An application of the technology or data; and/or

(4) The use of any other medium of communication, including but not limited to electronic, magnetic, internet, or laser technology.

c. Controlled technology, as defined in part 772 of Reference (r), is information necessary for the development, production, or use of a controlled product. Specific technology controls are identified in each export-control classification of the Export Administration Regulations (EAR) and govern export-control requirements.

d. Technical data, as defined in section 120.10 of Reference (s), is information which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles; classified information relating to defense articles and defense services; information covered by an invention secrecy order; or software as defined in section 121.8(f) of Reference (s) directly related to a defense article.

e. These procedures do not apply to lawfully admitted permanent residents nor to persons protected under section 1324b(a)(3) of Reference (t). For the purposes of the ITAR and EAR, they are considered U.S. persons.

2. This applies to all situations involving the release or transfer of controlled technology or technical data, including but not limited to:

- a. Foreign persons visiting or holding positions at government or private research institutions or laboratories;
- b. Foreign persons visiting or working at U.S. military installations;
- c. Foreign persons visiting or working at U.S. manufacturing plants;
- d. Foreign persons visiting or working with U.S. defense contractors;
- e. Shipments of controlled items from U.S. facilities to facilities abroad, whether U.S. or foreign owned; and
- f. Shipments of controlled items to foreign persons or foreign-owned facilities, whether in the United States or abroad.

3. In addition, to ensure compliance with References (d), (r), and (s):

a. DoD Components shall, in coordination with DoD counterintelligence, security, and foreign disclosure personnel:

(1) Identify and mark unclassified and classified export-controlled information and technology, as appropriate, to restrict access and use by unauthorized foreign nationals in accordance with References (e), (f), (i), (j), (m), (v), and (w).

(2) Identify threats by foreign countries that are targeting the specific unclassified or classified export-controlled information and technologies in accordance with Reference (m).

(3) Identify vulnerabilities and countermeasures to protect such unclassified or classified export-controlled information and technology in accordance with References (l), (m), and (x).

b. DoD Components shall ensure that appropriate internal controls within DoD facilities are established and maintained to prevent unauthorized access by foreign nationals to unclassified and classified export-controlled information and technologies consistent with the requirements set forth in References (e), (f), (j), (m), (r), (s), (v), (x), and (y). Such internal controls may take many forms typically used by DoD Components to protect unclassified or classified export-controlled information and technology, including unique badging requirements for foreign nationals, separate work areas for export-controlled information and technology, periodic foreign disclosure and export control training, and periodic self-assessments of the effectiveness of such measures.

c. DoD Components shall ensure that all appropriate solicitations and contracts include a clause stating that the contractor shall comply with all applicable export control laws and regulations in accordance with Reference (z).

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(GSA)	Assistant Secretary of Defense for Global Security Affairs
CFR	Code of Federal Regulations
CFIUS	Committee on Foreign Investment in the United States
DIA	Defense Intelligence Agency
DSCA	Defense Security Cooperation Agency
DTSA	Defense Technology Security Administration
DUSD(TSP&NDP)	Deputy Under Secretary of Defense for Technology Security Policy and National Disclosure Policy
EAR	Export Administration Regulations
FMS	Foreign Military Sales
IG DoD	Inspector General of the Department of Defense
INFOSEC/IA	Information Systems Security/Information Assurance
ITAR	International Traffic in Arms Regulations
MCTL	Military Critical Technologies List
NSA	National Security Agency
U.S.C.	United States Code
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy

PART II. DEFINITIONS

Unless otherwise noted, the following terms and their definitions are for the purposes of this Instruction only.

articles. Any articles, materials, supplies, or manufactured products, including inspection and test equipment. This includes all commodities and products considered as “munitions” and governed by the ITAR, as well as all “dual use” commodities and products. Components are also included in this definition. The term, however, excludes technical data, “know-how,” and information in intangible form, such as that electronically transmitted.

critical technology. Technology or technologies essential to the design, development, production, operation, application, or maintenance of an article or service which makes or could make a significant contribution to the military potential of any country, including the United States. This includes, but is not limited to, design and manufacturing know-how, technical data, keystone equipment, and inspection and test equipment.

dual-use. Technology and articles that are potentially used either for commercial/civilian purposes or for military, defense, or defense-related purposes.

items of intrinsic military utility. End items, including components, which have utility for military and/or war-making capabilities, including those useful because of technological content or other characteristics, such as the ability to reveal characteristics of U.S. items of intrinsic military utility.

keystone equipment. Includes manufacturing, inspection, and test equipment that is required for the effective application of technical information and know-how.

know-how. The learned ability for design, development, production, application, operation, or use of technology and articles, as well as provision of services. The term includes processes, procedures, specifications, design data and criteria, and testing methods. For manufacturing, this includes information that provides detailed processes and techniques needed to translate a detailed design into a finished article.

militarily critical technology. See critical technology.

munitions. For the purposes of this Instruction, includes:

Arms, ammunition, and other implements of war.

Any property, installation, commodity, material equipment, supply, or goods used to make military items.

Any machinery, facility, tool, material, supply, or other item necessary for the manufacture, production, processing, repair, servicing, storage, construction, transportation, operation, or use of any article listed above.

Technical data related to State Department munitions list items.

services. Includes any service, test, inspection, repair, training, publication, technical or other assistance, or defense information used to furnish military assistance, including military education and training activities.

technical data. Information of any kind that can be used, or adapted for use, in the design, production, manufacture, assembly, repair, overhaul, processing, engineering, development, operation, maintenance, adapting, testing, or reconstruction of goods or munitions; or any technology that advances the state of the art, or establishes a new art, in an area of significant military applicability in the United States. The data may be in tangible form, such as a model, prototype, blueprint, photograph, plan, instruction or an operating manual, or may be intangible, such as a technical service or oral, auditory, or visual descriptions. Technical data does not include information concerning general scientific, mathematics, or engineering principles commonly taught in schools, colleges, and universities or information in the public domain.

Technical data also does not include basic marketing information on function, purpose, or general system description.

technology. The application of scientific and technical information and know-how to design, produce, manufacture, use, adapt, reconstruct, or reverse-engineer goods. This includes technical information and data in all forms, including electronic form. The term does not include the goods themselves, nor does it include scientific information in the public domain.

transfer mechanisms. The means by which technology, articles, and services are or can be transferred, including, but not limited to: sales, research collaboration, exchanges, consulting arrangements, co-development and co-production arrangements, exhibits, meetings and symposia, technical missions, employment, dissemination of patent information, release of technical reports and technical data, illicit acquisition of technology or articles, and access through ownership or substantial interest in a business or other organization.