

Cornell University

# Export Control Compliance Manual

CORNELL UNIVERSITY

Export Control Compliance Manual

TABLE OF CONTENTS

Summary .....5

I. Commitment to Compliance.....5

II. Purpose and Policy.....6

III. U.S. Export Laws and Regulations .....6

IV. Roles and Responsibilities .....15

V. License Applications .....19

VI. Training .....21

VII. Record Keeping.....21

VIII. Internal Audits and Reviews .....22

IX. Violations and Reporting .....22

Appendices

**APPENDIX****TITLE**

A	Technology Control Plan – Template
B	OSP Pre- and Post- Award Review Criteria
C	NSDD 189 Ashton Carter Memo
D	Restricted Party Screening Procedure
E	TMP Self Certification Letter
F	Definitions - Export Control Terms
G	Cornell Export and Import Control Compliance Policy

## **LIST OF ABBREVIATIONS**

BIS	Department of Commerce, Bureau of Industry and Security
CCL	Commerce Control List
CJ	Commodity Jurisdiction
CRCO	Chief Research Compliance Officer
DDTC	Department of State, Directorate of Defense Trade Controls
EAR	Export Administration Regulations
ECA	Export Control Associate
ECCN	Export Control Classification Number
ECCM	Export Control Compliance Manual
ECO	Export Control Office
ECCO	Export Control and Compliance Officer
EHS	Environmental Health and Safety
EICCP	Export and Import Control Compliance Policy
EO	Empowered Official
FBSC	Finance and Business Service Center
FN	Foreign Nationals
FRE	Fundamental Research Exclusion
GCO	Grant and Contract Officer
ITAR	International Traffic in Arms Regulations
OFAC	Department of the Treasury, Office of Foreign Assets Control
OGC	Office of General Counsel
OVPRI	Office of the Vice President for Research and Innovation
OVPIA	Office of the Vice Provost for International Affairs
PI	Principal Investigator

PPS	Procurement and Payment Services
SDN	Specially Designated Nationals and Blocked Persons List
SRA	Sponsored Research Agreement
TAA	Technical Assistance Agreement
TCP	Technology Control Plan
USML	United States Munitions List
VPRI	Vice President for Research and Innovation

## SUMMARY

The Cornell University Export Control Compliance Manual (ECCM) addresses obligations set forth by various U.S. Government Agencies. These laws and regulations relate to:

- Sharing proprietary, confidential or otherwise controlled information, source code, or technology with foreign nationals located in the U.S. or abroad;
- Sending or taking tangible items or controlled technology or source code to another country;
- Collaborations with foreign entities;
- Interactions with embargoed or sanctioned countries, organizations, or individuals.

The relevant federal regulations found in the Code of Federal Regulations are as follows:

- Title 15, the Export Administration Regulations (EAR);
- Title 22, the International Traffic in Arms Regulations (ITAR); and
- Title 31, the Office of Foreign Asset Control (OFAC)

Individuals, faculty, researchers, employees, and students at Cornell University are therefore encouraged to contact Cornell University's Export Control and Compliance Officer whenever they expect to be involved with any export control issues.

Cornell University's Empowered Official and Export Control and Compliance Officer is:

Sarah Schlagter

Email: [sms655@cornell.edu](mailto:sms655@cornell.edu)

General Inquiries: [exportcontrols@cornell.edu](mailto:exportcontrols@cornell.edu)

Website: <https://researchservices.cornell.edu/export-controls>

This ECCM is implemented in accordance with the Export and Import Control Compliance Policy (EICCP).

## I. COMMITMENT TO COMPLIANCE

Cornell University is fully committed to complying with all U.S. Government export control laws and regulations. In compliance with federal regulations, it is Cornell University's strategy to protect its fundamental research exclusion by negotiating the elimination of all contractual clauses that restrict publication rights or limit participation of foreign nationals in its research and sponsored projects.

Cornell University conducts research to advance knowledge, enhance student learning experiences, and build its reputation in the scientific and technical communities while fostering productive experiences for its sponsoring partners. Cornell University endorses the principles of freedom of inquiry and open exchange of knowledge and is committed to compliance with export control regulations.

The export of certain "*technologies*", "*software*" and "*commodities*" [definition 15 CFR 772] is regulated and controlled by federal law for reasons of national security, foreign policy, competitive trade reasons, and preventing the spread of weapons of mass destruction. Cornell University and all

of its employees have the burden of knowing what information is export controlled during the course of collaborative research, understanding the limitations of exclusions such as fundamental research, and understanding what activities might be export controlled.

While exports are commonly associated with the shipment of a tangible item across the U.S. border, export controls have a much broader application. One of the most difficult issues related to export controls, and one central to Cornell University, is that an export is also defined to include the transfer of controlled “information or services” to foreign nationals *within the territory of the U.S.* Though the transfer is taking place inside the U.S., the transfer is “deemed” to be an export to the country of the foreign national.

Export control regulations affect not only research conducted on campus, but also financial dealings, traveling, and shipping items outside the U.S. Simply traveling to certain sanctioned countries could require an export license.

## II. PURPOSE AND POLICY

The purpose of Cornell University’s Export Control Compliance Manual is to provide the basis for the operational program and procedures which manage export decisions and transactions in compliance with the three major components of the export control laws and regulations, i.e., the Export Administration Regulations (EAR), the International Trade in Arms Regulations (ITAR) and the Office of Foreign Assets Control (OFAC).

Cornell University, including each individual employee and student, must comply with export control regulations. The associated penalties for non-compliance are severe and impact both Cornell University and the individual.

As export control laws apply to and affect the full range of Cornell University’s activities, it is important to maintain procedures regarding the actual and deemed export of strategically important items, materials, information, software, data, technology, and technical assistance to foreign countries, entities, and individuals.

***No member of the Cornell University community may engage in any activity, or commit the University to engage in any activity, that is contrary to U.S. export control laws and regulations. Any inconsistency between the content of this manual and U.S. export control laws and regulations is unintentional. In all cases the requirements of the applicable law or regulation shall take precedence***

The following information will provide guidance in determining how the regulations may apply to University activities and how one meets the prescribed requirements of the export control laws.

## III. UNITED STATES EXPORT CONTROL LAWS AND REGULATIONS

Export controls are intended to advance U.S. economic interests at home and abroad, prevent the proliferation of weapons of mass destruction, aid regional stability, implement anti-terrorism and crime controls, and protect human rights. In addition, the United States maintains economic embargoes against a number of countries whose governments consistently violate human rights or support global terrorism. Export control laws and regulations have grown in scope and complexity

over the years, especially since September 11, 2001. Export regulations are lengthy, difficult to interpret, and subject to frequent change.

## **A. AGENCIES, REGULATIONS, AND TECHNOLOGIES**

Several federal departments and agencies have promulgated export control regulations in response to specific statutes, executive orders, and presidential declarations.

Given the nature of research and education at Cornell University, this manual is driven principally by the requirements of the three below mentioned federal agencies and their regulations:

<b>LAW</b>	<b>U.S. DEPARTMENT</b>	<b>REGULATION CONTROLS</b>
EAR	Commerce	Dual-use goods, technology, chemicals, and software
ITAR	State	Military items, services, and research
OFAC	Treasury	Trade and travel prohibitions with embargoed/sanctioned countries, individuals, and entities

The following brief descriptions of the export control laws are meant to be only an overview of the regulations as they impact activities at Cornell. The information should be used with caution, and the Cornell community is encouraged to consult with the Export Control and Compliance Officer when contemplating new export-related activities.

### **1. EAR (15 CFR 730-774)**

#### **Regulatory Authority and Scope**

The EAR controls the export of “dual use” items, which are items that have civilian uses, but which may also have military or other strategic applications. Common, real-life examples from Cornell include certain plasmids, genetic material, chemicals, microorganisms, vectors and toxins as well as laboratory equipment such as centrifuges, analyzers and fabrication equipment such as milling machines and etching equipment for electronics. The EAR also controls the export of certain low-technology consumer goods which are not specifically noted on the CCL. These items are classified as EAR99 and have very few export restrictions. However, the export of an EAR99 item to an embargoed country, an end user of concern or in support of a prohibited end use may require a license.

Many activities are not subject to the EAR. In addition to activities subject to the exclusive authority of another agency, e.g. the export of a defense article which is controlled under the ITAR, the EAR lists several exclusions from the regulations. These include published information, information resulting from fundamental research, educational information and the export or reexport of items with less than *de minimis* U.S. content (where applicable). It is important to understand the definitions and limitations of each of these exclusions in order to correctly evaluate their applicability to specific activities.



## **Important EAR Definitions and Concepts**

**Export** is defined in 15 C.F.R. § 734.13 as shipping, transmitting or taking items subject to the EAR out of the U.S. as well as the release of technology or source code subject to the EAR in or to a foreign country or to a foreign national either in the U.S. or abroad.

**Deemed Export** is defined in 15 C.F.R. §734.13(b). A deemed export is any release of technology or source code subject to the EAR to a foreign national, regardless of location. The release is deemed to be an export to the home country or countries of the foreign national. For the purposes of the EAR, legal U.S. permanent residents, naturalized citizens, and individuals protected under the Immigration and Naturalization Act (8 U.S.C. § 1324b(a)(3)), are not considered to be foreign nationals.

**Reexport** means an actual shipment or transmission of items subject to the EAR from one foreign country to another foreign country. It also means the release of technology or software subject to the EAR to a foreign national outside the United States (**Deemed Reexport**). Reexport is defined in 15 C.F.R. §734.14.

**De Minimis U.S. content** is the amount of U.S. content, as determined by percentage of value of the U.S. content in the end item, required to make a foreign produced item subject to the EAR. For some items, there is no *de minimis* content, meaning that any U.S. content will make the foreign-produced item controlled under the EAR. For other items the *de minimis* U.S. content for foreign produced items may be 10% or 25% of the total value. See 15 C.F.R. § 734.4 for a complete discussion of the *de minimis* U.S. content rules.

**Published Information and Software** is defined in 15 C.F.R. § 734.7. Information is published when it is accessible to the public without restrictions upon its further dissemination. Publications may take the form of periodicals, books, print, electronic, public websites, or any other media available to the public. Articles submitted to journals for consideration with the intent that they be made publicly available are considered to be published, regardless of whether or not they are accepted. Published information also includes information readily available in libraries (including university libraries), as well as patents and published patent applications. Finally, release of information at a conference open to the participation of all interested persons, is considered to be publication of that information. Software is published when it is made available to the public without restrictions upon further dissemination, either for free or at the cost of distribution. *However, strong encryption software remains controlled, regardless of general availability.*

**Fundamental Research** means *research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons.* The complete definition and discussion of fundamental research, including University based research is found at 15 C.F.R. § 734.8. University research is considered to be fundamental to the extent that researchers do not accept restrictions on the publication of information resulting from the research. Temporary delays in publication solely for the protection of sponsor proprietary information or to ensure that the publication will not compromise patent rights do not remove the research from the fundamental domain. Note that controlled technology or software that is *used to conduct* fundamental research is not considered fundamental research itself simply because it is used in fundamental research.

**Educational Information**, as set forth in 15 C.F.R. § 734.3(b), is information released as part of a course listed in the University's course catalog, and through instruction in the classroom or

teaching laboratory. Participation in the course should be open to any qualified student enrolled at the academic institution. Educational information is not subject to the EAR.

### **The Commerce Control List**

The CCL is found at 15 C.F.R. § 774, which may be accessed at:

<https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl>. Items included on the CCL are assigned an export control classification number (ECCN) based on a category and product group. There are 10 categories, numbered 0 – 9, and five product groups, labeled A- E, within each category. The category and product group generally describe the item being classified, and the remaining three digits of the ECCN relate to the item specifications. An ECCN follows the nomenclature of “#α###”, where the first “#” is the category, “α” is the product group, and “###” identifies the reasons for control. As an example, a plasmid with certain genetic characteristics has an ECCN of 1C353. In general, “###”, with lower numbers are controlled to more destinations than those with higher numbers. The categories and product groups are as follows:

<b>Commerce Control List Categories</b>	
0	Nuclear and Miscellaneous items
1	Materials, Chemicals, Microorganisms, and Toxins
2	Materials Processing
3	Electronics
4	Computers
5 (Part 1)	Telecommunications
5 (Part 2)	Information Security
6	Sensors and Lasers
7	Navigation and Avionics
8	Marine
9	Aerospace and Propulsion

<b>Commerce Control List Product Groups</b>	
A	Systems, equipment and components
B	Test, inspection and production equipment
C	Material

D	Software
E	Technology

The EAR export licensing regime is much more flexible than that of the ITAR. Under the EAR, licensing requirements for export activities depend on what is being exported, the export destination, who will be using it, and what it will be used for. ECCN entries include a listing of the reasons for control that can be used in determining if an export license is necessary. While the most common controls are for anti-terrorism and national security, many other potential controls exist. The complete list of controls is found in 15 CFR§ 742. The control list can be matched to the country chart to make a determination of whether or not a license is required and if an applicable license exception is available.

### **License Exceptions**

While the CCL is much more extensive than the USML, many fewer licenses are required for items controlled under the EAR than under the ITAR. This is because of the many license exceptions that may be available for EAR controlled exports. It is important to understand that there are limitations on the use of license exceptions (see 15 C.F.R. § 740.2), and that the use of a license exception may have an associated recordkeeping and notification requirement. More than one license exception may be available for a proposed activity. In such cases, the use of the exception with the fewest restrictions on use and least notification and recordkeeping requirements minimizes compliance burden. Members of the Cornell community are encouraged to consult with the Export Control and Compliance Officer when making decisions as to the applicability of EAR license exceptions for proposed export activities.

A complete listing of EAR license exceptions may be found in 15 C.F.R. § 740. Exceptions commonly applicable to members of the Cornell community travelling abroad are TMP, which applies to the temporary export of Cornell-owned equipment, including laptop computers and other equipment listed on the CCL, for work-related activities, including professional presentations, teaching, and field research, and BAG, which applies to personally-owned items taken abroad for personal use while abroad. It is important to note that there are limitations on the use of the TMP license exception: items must be returned to the U.S. within one year of export, or if not returned, documentation of disposal is required. Items exported using the TMP license exception must be kept under the effective control of the traveler while abroad. Additionally TMP is not applicable to some restricted locations, such as Cuba. A TMP self-certification letter is available on Cornell's export control website at: <https://researchservices.cornell.edu/resources/export-controls-and-international-travel>.

### **Commodity Classification**

BIS encourages exporters to use the detailed descriptions in the CCL to self-classify items to be exported. However, in the event of an incorrect classification, the exporter is liable for any resulting violations of the EAR and may be subject to resulting penalties. Self-classification may be particularly difficult in the university environment where cutting edge-research pushes the boundaries of existing technologies, and in fact may not precisely meet the technical specifications as described in the existing CCL listings. When unsure about a self-classification, the exporter may

submit the item/technology to BIS for a formal classification. Members of the Cornell community who need assistance with classifying items should contact the ECCO.

### **Anti-Boycott Restrictions**

The anti-boycott provisions of the EAR were designed and implemented to address foreign governments' boycott of countries friendly to the U.S. The provisions were first implemented in response to the Arab League Boycott of Israel. As of January 2018, Arab Countries including Kuwait, Lebanon, Libya, Qatar, Saudi Arabia, Syria, the United Arab Emirates, and Yemen continue to impose boycott restrictions on Israel and "blacklist" companies that do business with Israel. The anti-boycott provisions are found in 15 C.F.R. § 760. The provisions apply to any person or entity in the U.S. as well as to U.S. persons or entities abroad. For example, Cornell is a U.S. person because it is located and organized under U.S. law. The anti-boycott provisions specifically prohibit the following activities:

- Agreement to refuse or actual refusal to do business with a boycotted country or with blacklisted person
- Agreement to discriminate or actual discrimination against other persons based on race, religion, sex, national origin, or nationality (for example, agreeing to refuse to hire Israeli nationals)
- Providing information about race, religion, sex, or national origin of another person
- Furnishing information about business relationships with boycotted countries or blacklisted persons (for example, providing information about current or previous business in Israel)
- Furnishing information about membership concerning associations with charitable and fraternal organizations
- Paying or otherwise implementing letters of credit containing prohibited conditions or requirements.

Exceptions to these prohibitions exist but are limited. **Additionally, U.S. persons asked to engage in the prohibited activities are required to report the request to BIS.** The ECcO will provide guidance on anti-boycott language and assistance in determining whether an exception is applicable and if reporting to BIS is required.

## **2. ITAR (22CFR 120-130)**

### **Regulatory Authority and Scope**

The Arms Export Control Act (AECA), 22 U.S.C. § 2778 grants authority to the President of the U.S. to designate and control the export and import of defense articles and services. Presidential executive order 11958 delegates this responsibility to the Secretary of State. The Department of State Directorate of Defense Trade Controls (DDTC) administers this authority through implementation of the International Traffic in Arms Regulations (ITAR), 22 C.F.R. §§ 120-130. The ITAR contains the United State Munitions List (USML), which includes defense articles and related technical data that are controlled for export purposes. In addition to the defense article or related technical data, constituent parts and components of the defense article are controlled under the ITAR. If a commodity contains a part or component that is controlled under the ITAR then that commodity is also controlled under the ITAR, regardless of whether or not that commodity has an inherently military purpose

Many items designed for military use are also used for research completely unrelated to that military use. It is important to understand that the ITAR designation remains intact, even if the item is not being used for military purposes.

### **Important ITAR Definitions and Concepts**

In order to understand the requirements of the ITAR, it is important to understand terminology specific to the regulation such as “defense article,” “technical data,” and “defense service.” Additionally, it is important to understand how the ITAR defines “fundamental research” and “public domain” information.

**Defense article** is defined in 22 C.F.R. § 120.6. It means any item or technical data that is specifically designed, developed, configured, adapted, or modified for a controlled use listed on the USML. In addition to the items on the USML, models or other items that reveal technical data related to USML items are also considered to be defense articles. Defense articles do not include basic marketing information on function or purpose or general system descriptions.

**Technical data** is defined in 22 C.F.R. § 120.10. Technical data includes information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This information includes blueprints, drawings, photographs, plans, instructions and documentation. ITAR technical data also includes classified information relating to defense articles and defense services, information covered by an invention secrecy order and software directly related to defense articles.

**Defense Service** is defined in 22 C.F.R. § 120.9. The definition includes: 1) furnishing of assistance, including training, to a foreign person, whether in the U.S. or abroad, in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles; 2) providing any foreign person any technical data as defined above; and 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.

**Public Domain** is defined in 22 C.F.R. § 120.11. Public domain information is *information which is published and which is generally accessible or available to the public*. The ITAR describes means by which public domain information might be available, which include:

- (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 after approval by the cognizant U.S. government department or agency;

(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. Fundamental research is defined to mean basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. University research will not be considered fundamental research if:

(i) The University or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity, or

(ii) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable.

### **The USML Categories**

The USML defines twenty-one classes of defense articles. The USML is found at 22 C.F.R. § 121. In the interest of brevity, only the main headings of the USML categories are listed here. For detailed descriptions of what is included in each category, the ITAR may be accessed on line at [https://www.pmdotc.state.gov/ddtc\\_public?id=ddtc\\_public\\_portal\\_itar\\_landinghttps://www.ecfr.gov/cgi-bin/text-idx?SID=50ad4343354d279b702e37574d076f62&mc=true&node=pt22.1.121&rgn=div5](https://www.pmdotc.state.gov/ddtc_public?id=ddtc_public_portal_itar_landinghttps://www.ecfr.gov/cgi-bin/text-idx?SID=50ad4343354d279b702e37574d076f62&mc=true&node=pt22.1.121&rgn=div5). Note that category XXI is reserved for use by DDTC for controlling new technologies under the ITAR.

I	Firearms, Close Assault Weapons and Combat Shotguns
II	Guns and Armament
III	Ammunition / Ordnance
IV	Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs and Mines
V	Explosives, Propellants, Incendiary Agents, and their Constituents
VI	Surface Vessels of War and Special Naval Equipment
VII	Ground Vehicles
VIII	Aircraft and Related Articles
IX	Military Training Equipment and Training
X	Personal Protective Equipment
XI	Military Electronics
XII	Fire Control, Laser, Imaging and Guidance Equipment
XIII	Materials and Miscellaneous Articles
XIV	Toxicological Agents, Including Chemical Agents, Biological Agents and Associated Equipment
XV	Spacecraft and Related Articles
XVI	Nuclear Weapons, Related Articles
XVII	Classified Articles, Technical Data and Defense Services Not Otherwise Enumerated
XVIII	Directed Energy Weapons
XIX	Gas Turbine Engines and Associated Equipment
XX	Submersible Vessels and Related Articles

### **Exporting under the ITAR**

An export as defined under the ITAR includes sending or taking a defense article out of the U.S., disclosing (including oral or visual disclosure) technical data to a foreign person whether in the U.S. or abroad, transferring registration, control or ownership of any aircraft, vessel or satellite subject to the ITAR to a foreign person, releasing a defense article to an embassy (including agencies or subdivisions) in the U.S., or performing a defense service on behalf of or for the benefit of a foreign person whether in the U.S. or abroad. (See 22 C.F.R. § 120.17 for a complete definition of “export” under the ITAR). **This definition is broad and includes taking controlled technical data out of the U.S. on a laptop computer, regardless of whether or not that information is viewed or accessed while abroad. It also includes allowing a foreign person to view or use a defense article in the U.S. Most exports of defense articles and defense services must be licensed by DDTC.**

Any release 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.

Any person in the U.S. that either exports, temporarily imports, or manufactures defense articles or furnishes defense services must be registered with DDTC. Registration is required prior to applying for a license or taking advantage of some license exemptions. Registered entities may apply for licenses, or permission, to export defense articles and defense services. Cornell University is registered with the DDTC. Note that registration is *not* a license to export. License requests must be made through Cornell’s Export Control and Compliance Officer. DDTC reviews license requests on an individual basis, and consults with other agencies, such as the Department of Defense in consideration of the request.

### **Commodity Jurisdiction**

The DDTC has the responsibility to determine if an item or technology falls within the scope of the ITAR or if the item/technology is under the jurisdiction of the Department of Commerce for the purposes of export controls. While it is possible to self-classify an item, DDTC should be consulted if there is any doubt as to whether an article or service is subject to the ITAR. **The ECCO assists with the submission of commodity jurisdiction requests as well as with the determination of any export licensing requirements.**

## **3. OFAC (31 CFR 500-590)**

### **Regulatory Authority and Scope**

The Office of Foreign Asset Controls (OFAC) administers and enforces economic and trade sanctions based on U.S. foreign policy and national security interests. Many of the sanctions are based on United Nations and other international mandates. The OFAC sanctions vary in scope. Some broadly target entire countries, while others focus on specific entities. In addition to foreign countries and regimes, OFAC imposes sanctions on individuals, including those that the U.S. government deems to be a threat to the national security, foreign policy or economy of the U.S. The implementing regulations for the OFAC sanctions are found in 31 C.F.R. §§ 500-599, the Foreign Asset Control Regulations.

The OFAC sanctions broadly prohibit most transactions between a U.S. person and persons or entities in an embargoed country or who have been declared specially designated nationals (SDNs). The prohibition generally includes importation and exportation of goods and services as well as related financial transactions, and engaging in business activities. The current sanctions lists can be found at <https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx>.

### **OFAC Licensing for Country Based Programs**

It is important to review the specific sanctions program before conducting activities with an OFAC sanctioned entity or person, or in an OFAC-sanctioned country. The individual sanctions specifically describe what activities are exempt as well as what activities may be permitted under an applicable license. Activities which are permitted under a general license do not require specific permission from OFAC prior to engaging in the activity; however, the conditions of a general license must be carefully reviewed and the use of the general license documented. Activities that do not fall under an available general license may be eligible for a specific license from OFAC. Specific license requests must be submitted and approved by OFAC prior to engaging in the sanctioned activity. Activities conducted under both general and specific licenses are subject to OFAC audit, and records must be maintained for five years after the conclusion of the activity. The ECCO must be contacted when considering any OFAC sanctioned activities.

*Note: There are other restricted party lists maintained by government agencies including the Department of Commerce and the Department of State. Consultation with the ECCO or other appropriate offices within Cornell will ensure that the parties to any contemplated activity are appropriately screened.*

## **IV. ROLES AND RESPONSIBILITIES**

### **Vice President for Research and Innovation (VPRI)**

Overall responsibility for the export control management program at Cornell University is in the VPRI. The ECCO reports to the Chief Research Compliance Officer (CRCO) under the VPRI. The CRCO (or their delegate) shall be empowered with the ECCO authority, in instances where the ECCO is unavailable or unable to act.

### **Export Control Office**

The Export Control Office (ECO) is under the direction of the Export Control and Compliance Officer (ECCO) and includes the Export Control Associate (ECA). The ECCO is Cornell's "Empowered Official" for all export control issues and is responsible for overseeing and implementing Cornell's export control policies and procedures. It is important to understand that export compliance is ultimately the responsibility of all individuals. The Cornell community is urged to contact the ECO, who will provide direction, guidance and assistance to help ensure compliance.

Cornell's ECO is empowered with the following authority and responsibilities under Cornell's EICCP and this ECCM:

1. Serve as a resource to the Cornell community on export and import control matters.
2. Work with institutional partners, officials, and personnel ex. OGC, research compliance, OSP, OSRA. researchers, and deans, directors and chairs to identify



- export and import control related questions and resolve related issues proactively and prospectively to minimize or eliminate possible violations.
3. Create, update, implement, and maintain the Export Control Compliance Manual (ECCM) for Cornell's Ithaca-based locations, and assist with the ECCM for WCMC.
  4. Publish the ECCM on Cornell's Export Control Website and update the website with other compliance documentation as needed. Assist with the WCMC website.
  5. Complete, update and maintain appropriate registrations.
  6. Submit export license applications and, unless otherwise delegated, serve as the primary point of contact with government officials, related to such applications.
  7. Maintain export licenses and related records.
  8. Implement international shipping procedures and methods.
  9. Develop, conduct, and track appropriate training of University personnel.
  10. Report incidents of non-compliance to the Office of General Counsel (OGC) and make appropriate disclosures.
  11. Recommend resolution of export control matters in consultation with OGC and the Chief Research Compliance Officers of both Cornell's Ithaca-based locations and WCMC (hereinafter collectively referred to as CRCO).
  12. The ECCO shall serve as Cornell's Empowered Official<sup>1</sup>, and together with the ECA, Vice President for Research and Innovation, and the WCMC Senior Associate Dean for Research serve as Cornell's authorized signatory on export and import control documentation, including customs documents and license applications.
  13. Conduct regular and ad hoc risk assessments and implement corrective actions as needed or as required in consultation with OGC and the CRCO.
  14. Authorize shipping carriers and freight forwarders to make export and import control filings, if any, on Cornell's behalf.
  15. Halt exports or imports that violate (or are reasonably suspected of violating) U.S. Export or Import Control Regulations.
  16. Delegate some or all of the above authority to other export compliance professionals within the Cornell University community, in consultation with the CRCO.

### **Vice President for Research & Innovation (VPRI)**

Makes the final determinations in consultation with ECCO, CRCO, and OGC on acceptance of any exceptions to an award with export control restrictions.

### **University Units**

Each Unit shall, upon request by the ECCO, designate a primary point of contact to serve as the ECO's liaison on export and import control related matters. The liaison will be responsible for coordinating notifications, trainings, maintaining local records, and ensuring the export and import control related activities are addressed in a timely manner.

### **Deans, Department Heads, and Chairs**

---

<sup>1</sup> *An empowered official is authorized by a business enterprise to sign and process license applications on behalf of the company. An empowered official understands the provisions of ITAR. This individual has the authority within the university to inquire into any aspect of a proposed export and to verify the legality and accuracy of the information submitted for a transaction. An empowered official also has the authority to refuse to sign any license application without retribution from his/her company since they are liable for ITAR violations.*

Responsible for taking offered training in export and import control regulations and for having knowledge of the information on the University's export controls website, as well as knowledge of the export and import controls relating to the area(s) of research that are under their purview.

### **Departmental Administrators**

The administrators are responsible for knowledge of policies and procedures related to export and import control regulations as they may pertain to the administrator's area. They shall consult the ECO and advise faculty as needed.

### **Principal Investigators (PIs)**

PIs have expert knowledge of the type of information and technology involved in a research project or other university activity, such as presenting at conferences and discussing research findings with fellow researchers or collaborators. PIs must ensure that they do not disclose controlled information, such as information that has been provided to them under a non-disclosure agreement or transfer controlled articles or services to a foreign national without prior authorization as required. Each PI shall:

1. Work with the ECO to understand their obligations under U.S. Export Control Regulations.
2. Assist the ECO in correctly classifying technology and items that are subject U.S. Export Control Regulations.
3. Assist in developing and maintaining the conditions of a technology control plan (TCP) for any activity, technology, data, or equipment where the need for such a plan is identified by the ECO.
4. Ensure that research staff and students have been trained on the technology control plan and on the U.S. Export Control Regulations should any apply.
5. Notify the ECO prior to or immediately upon the receipt of any information or technology that is either identified as or suspected to be export controlled.
6. Ensure that all international shipments sent from their lab are either approved by the ECO, or through a process set forth by the ECO.

A template TCP is in Appendix A.

### **Office of General Counsel (OGC)**

In conjunction with the CRCO and ECO, provide advice to University researchers and administrators regarding the laws, regulations, and University policies related to export and import controls.

### **Office of Sponsored Programs (OSP)**

OSP aids in export control compliance by working closely with the ECO in identifying export control contract issues, ensuring that the FRE is maintained, and negotiating solutions with the research sponsor. OSP shall:

1. Review the terms of a sponsored agreement, grant or other non-financial agreement and identify any restrictions on publication or dissemination of the research results, as well as restrictions for proprietary or national security reasons.
2. Consult with the ECO to understand any impermissible contractual restrictions, and work with the research sponsor to negotiate the impermissible terms out of the agreement.

3. Identify potential export control issues in agreements and bring them to the attention of the ECO.
4. Perform restricted party screenings on all collaborating entities in accordance with documented procedures.
5. Review non-disclosure agreements and other contractual terms for indications that information controlled under U.S. Export Control Regulations may be provided to Cornell. Alert the ECO and refrain from signing the agreement until a Technology Control Plan is executed and the ECO provides approval.
6. Act as liaisons between the PI, the sponsor, and the ECO.

### **Finance, Accounts Payable, and Business Service Centers**

Cornell Finance, Accounts Payable, and Business Service Centers (Payment Units) assist in ensuring compliance with export control regulations by identifying potential export issues in unit activities to the ECO, particularly those related to payments. The Payment Units shall:

1. Screen all payees and their country of location against U.S. sanctioned parties lists and elevate alerts to the ECO prior to submitting for payment.
2. Review contract and invoice terms where applicable and raise export control related issues to the ECO.

### **Procurement and Payment Services**

Procurement and Payment Services (PPS) monitors export and import control compliance as it relates to purchasing activities. PPS shall:

1. Screen all payees and their country of location against U.S. sanctioned parties lists and elevate alerts to the ECO prior to submitting for payment.
2. Review contract and invoice terms where applicable and raise export and import control related issues to the ECO.
3. Serve as the liaison between the ECO and the vendor, for resolution of export and import control related issues.
4. Update the Buying Manual as needed, to implement updated guidance from the ECO.

### **Center for Technology Licensing (CTL)**

Negotiates licenses to University intellectual property or material transfer agreements when a PI desires to transfer materials off-campus. CTL shall:

1. Review the terms of all outgoing MTAs and licensing agreements for export control issues.
2. Notify and assist the ECO in reviewing proposed transactions for export control issues.
3. Screen all licensees and material recipients against U.S. sanctioned parties lists and elevate alerts to the ECO prior to signing an agreement.

### **Human Resources**

The Division of Human Resources shall be responsible for providing names of new hires to the ECO for screening against sanctioned parties lists, as appropriate and in compliance with applicable U.S. laws and regulations.

### **Environmental Health and Safety**

Environmental Health and Safety (EHS) plays a key role in assisting the ECCO with technical issues related to biological and genetic materials. EH&S shall be responsible for technical assistance to the ECO and working with the ECO on import permits related to hazardous materials, genetic materials, radiation, and chemicals. EH&S shall work closely with the ECO in identifying licensable international shipments and obtaining the required paperwork

#### **Office of the Vice Provost for International Affairs (OVPIA)**

OVPIA shall be responsible for maintaining and administering the Cornell International Travel Registry, non-sponsored international collaborative agreements, requests for travel to Cuba, and other international support services. OVPIA shall work with the ECO to provide up-to-date guidance to travelers in accordance with U.S. Export Control Regulations. OVPIA shall refer matters and/or elevate export control related issues to the ECO, including but not limited to, engagements with sanctioned countries or entities. OVPIA shall provide travelers with resources and advice in accordance with Policy 8.5 Risk Management for International Travel and other institutional policies and procedures.

#### **Weill Cornell Medicine (WCM)**

WCM shall have its own Export Control Compliance Manual, setting forth roles and responsibilities specific to WCM. WCM's EH&S shall manage all aspects of export and import controls pertaining to physical shipments (including hand carried items) at all WCM locations. The foregoing sentence shall include applying for export licenses and import permits on WCM's behalf.

The ECCO authorizes the WCM CRCO to designate an official whose responsibility is to:

1. Submit export license applications and, unless otherwise delegated, serve as the primary point of contact with government officials, related to such applications.
2. Implement international shipping procedures and methods.
3. Serve as an authorized signatory on export and import control documentation, including customs documents and license applications.
4. Authorize shipping carriers and freight forwarders to make export and import control filings, if any, on WCM's behalf.
5. Halt exports or imports that violate (or are reasonably suspected of violating) U.S. Export or Import Control Regulations.

Such WCM official, must supply reports on WCM activities to ECCO on a regular basis and keep the ECCO informed as to all WCM activities.

#### **V. LICENSE APPLICATIONS**

If a license is required for a controlled activity, the ECO will be the primary point of contact for preparation and submission of the license application.

The license application will be developed with the cooperation of the concerned PI as the PI is accountable to Cornell University for complying with the terms of the issued license. It is worth noting that there is no guarantee that a license will be granted and, if granted, the terms can be less favorable than what was originally requested.

***NOTE: an OFAC license may be required in addition to an ITAR or EAR license.***

Sanctions programs for which implementation and administration are delegated to OFAC are set forth in the particular part of OFAC regulations dedicated to that sanctioned program. In the case of economic sanction programs not yet implemented in the regulations, OFAC controls can be found in the applicable executive order or other authority. License application procedures and reporting requirements are set forth in each sanctioned/embargoed part of the regulations and govern the transactions to be undertaken pursuant to either a “*general*” or “*specific*” license described below.

OFAC, therefore, has provisions for two types of licenses:

- (a) “*General License* - General licenses may be issued authorizing, under appropriate terms and conditions, certain types of transactions which are subject to the prohibitions contained in 31 CFR 501.801. General licenses also may be issued authorizing, under appropriate terms and conditions, certain types of transactions that are subject to prohibitions contained in economic sanctions programs the implementation and administration of which have been delegated to the Director of the Office of Foreign Assets Control (OFAC) but which are not yet codified in this chapter... It is the policy of OFAC not to grant applications for specific licenses authorizing transactions to which the provisions of a general license are applicable. Persons availing themselves of certain general licenses may be required to file reports and statements in accordance with the instructions specified in those licenses. Failure to file timely all required information in such reports or statements may nullify the authorization otherwise provided by the general license and result in apparent violations of the applicable prohibitions that may be subject to OFAC enforcement action.”
- (b) “*Specific Licenses* - Transactions subject to the prohibitions..., or to prohibitions the implementation and administration of which have been otherwise delegated to the Director of the Office of Foreign Assets Control, that are not authorized by general license may be effected only under specific licenses.”

### **Licensing Information**

The following general questions can be used to help determine whether an activity may require a license from the BIS, DDTC or OFAC:

- Is the person a U.S. Citizen or permanent resident (issued a green card)?
- Is the information already published (for example on the Internet or in public libraries)?
- Is it educational information covered in a course catalog?
- Is the technology disclosed in a published patent application or an issued patent?
- Is the research considered fundamental research that will be published?
- What is the export control classification of the product – is it EAR99, or other?
- Does a license exclusion or exemption apply?
- Does the proposed transaction involve a sanctioned country or an individual from a sanctioned country?
- What is the value of the shipment?
- Who is the end user?
- What is the purpose of the export?

If an activity is controlled under the export regulations, then a license or other approval is needed from the respective jurisdiction unless an exemption or exception applies. Examples of situations where a license may be required include:

- The conduct of research that is not fundamental.
- Shipping or taking a commodity or good outside of the U.S.
- Attending and presenting at a conference where registration is limited to U.S. citizens.
- Travel to a sanctioned country.
- Transfer of controlled technical data to a foreign person in or outside of the U.S.
- Providing anything of value, controlled items, or controlled technology to someone from a sanctioned country, on the entity list, denied persons list, debarred (or excluded) parties list or any other restricted list.

### **Technical Assistance Agreements**

If a Technical Assistance Agreement (TAA), [22 CFR 120.22, 124.1 and 124.12], is required for the performance of a defense service or the disclosure of “*technical data*” for a research project, the ECCO will review [22 CFR 120.25] and sign the TAA. The ECCO will evaluate the need for a Technology Control Plan and work with the PI to draft and implement the TAA, if necessary. For space systems and launches, the TAA application must be preceded by a Technology Transfer Control Plan (TTCP) as discussed under 15 CFR 124.15(a)(b) and will be developed by the ECCO with the full support and cooperation of the PI.

### **Technology Control Plan**

If it is necessary for export-controlled Technology or Technical Data to be transferred to Cornell University, a project specific TCP must be put into place by the ECCO with the full cooperation of the PI, department, and other pertinent units. The TCP will address the following informational needs:

- How will the persons working on the project be documented and controlled?
- How will citizenship status be verified?
- How will unauthorized persons be restricted from accessing research data and materials?
- What physical and informational security measures will be implemented to prevent access to the project by unauthorized persons?

The final document will be approved by the ECCO, the individuals involved, and the department chair. The department chair has the responsibility to ensure the compliance of the PI. All persons listed on the TCP are required to comply with the terms of the plan.

## **VI. TRAINING**

Training is a critical component of maintaining compliance with export control laws. The primary goal of training is to increase awareness and maintain compliance with U.S. export control laws and trade sanctions. Export control training is designed to educate the Cornell University community on its responsibilities under these laws and the procedures in place for ensuring compliance. It is especially critical that faculty and administrative staff that direct or participate in research projects involving export-controlled goods, technology, or software participate in training provided by the ECO.

The ECO provides education and training to Cornell University's administration, faculty, graduate students, postdocs, and staff on export control regulations and compliance.

The Cornell University export control website includes an overview of relevant information at <https://researchservices.cornell.edu/export-controls>. Individual and group training sessions can be arranged by contacting the ECCO. In addition, regular export control training is included in the Research Administration Certification Program (RACP) course offered on a semi-annual basis by the Office of Sponsored Programs. General export control training sessions are also offered periodically through the Research Division.

The export control training options include classroom training, department and center meetings, faculty staff meetings, and specialized group trainings for those interested in learning the basics. To schedule a presentation, contact the ECO via email at [exportcontrols@cornell.edu](mailto:exportcontrols@cornell.edu).

## **VII. RECORDKEEPING**

Cornell University is subject to several regulatory recordkeeping requirements related to its export activities. The ITAR [22 CFR 122.5], the EAR [15 CFR 762.2] and OFAC [31 CFR 501.601] all require that records be kept reflecting the export, reexport and temporary import of defense articles, defense services, dual use commodities and related technologies. Types of records to be maintained will be based on the individual controlled items or activities.

The storage of the appropriate records either originals or back-ups, must be maintained by the individual unit. Records must be kept in a manner which facilitates the ability to retrieve them for any purpose, especially during an internal or U.S. Government audit.

### **Maintenance of Records**

Unless specified otherwise, all records shall be retained for no less than five (5) years after the date of export, reexport, the project's TCP or license termination date, or any other aspect of the transaction, whichever is later.

If ITAR controlled technical data is exported under an exemption, certain records of the transaction must be kept even beyond the standard five year period. The records must include:

- A description of the unclassified technical data;
- The name of the recipients and end-user;
- The date and time of the export;
- The method of transmission (e.g., email, fax, telephone, FedEx, etc.); and
- The exemption under which the export qualified.

Information which meets the criteria of being in the public domain, i.e., educational information or results from fundamental research is not subject to export controls under the ITAR and qualifies for an exception; however, it is required that all documentation for these analyses be maintained for five years or more after the overall analysis is completed.

The EAR has specific recordkeeping requirements. Generally, required records must be kept for a period of five years from the project's end date. However, if BIS or any other government

jurisdiction makes a request for such records, for example, a request following a voluntary self-disclosure (VSD), the records must be maintained until the requesting jurisdiction concerned provides a written authorization to release the records.

## **VIII. INTERNAL AUDITS/REVIEWS**

An internal review of export records may be randomly and periodically conducted in order to maintain Cornell's export compliance program and to ensure consistent adherence to U.S. export laws. The purpose of the reviews is:

- To identify possible violations; and
- To identify deficiencies in training, procedures, etc. that can be rectified.

## **IX. VIOLATIONS AND REPORTING**

### **General Overview**

Generally, any person or entity that brokers, exports, or attempts to export a controlled item or controlled technology without prior authorization, or in violation of the terms of a license, is subject to penalties. Violators may incur both criminal and civil penalties. Although there is a maximum amount for a civil or criminal penalty, the actual penalty imposed is often multiplied.

### **Detecting and Reporting Violations**

Any individual who suspects a violation has occurred must immediately notify the Export Control and Compliance Officer. The ECO will work with OGC to determine the appropriate follow-up to the notification, which may include a voluntary self-disclosure to the government. The ECO will conduct an internal review of the suspected violation by gathering information about the circumstances, personnel, items, and communications involved. The ECO may provide the government agency with a thorough narrative account of:

1. The project's description and background.
2. A description of the suspected violation.
3. Items and controlled categories involved.
4. Dates the violations occurred on.
5. Countries involved.
6. Name and citizenship status of individuals involved.
7. An explanation of why the alleged violation occurred.
8. Any corrective actions taken.
9. Cornell's commitment to export control compliance.

Once the initial notification has been sent, Cornell will follow the government agency's instructions.

There are civil and criminal penalties, including fines and imprisonment, for violating the export control laws and trade sanctions, and both the organization and the individual(s) involved are subject to these penalties. Cornell University and the individual(s) involved may also lose their ability to export, and/or be suspended or debarred from government contracting. A voluntary self-disclosure may serve as a mitigating factor and a representation of Cornell's commitment to maintaining compliance.



# **APPENDICES**

## **APPENDIX A**

### **Template - Technology Control Plan**

#### **Technology / Export Control Plan (T/ECP)**

In accordance with Export Control Regulations (EAR and ITAR), a Technology / Export Control Plan (T/ECP) is required in order to prevent unauthorized exportation of protected items / products, information, or technology deemed to be sensitive to national security or economic interests.

Violations can result in both civil and criminal penalties for the individual and for the University. In addition to a civil penalty for each violation of the export regulation, there are criminal penalties that may be imposed, including significant fines against Cornell University, and a fine, or

imprisonment, or both against the individual. Voluntary self-disclosures, if made appropriately, can mitigate the seriousness of the penalty. Penalties apply to each individual violation, which means that if a violation relates to more than one controlled material or item or occurs on more than one occasion, each item or incident may trigger a penalty. Contact the Export Control and Compliance Officer immediately if you think you have made a mistake and violated export controls; they can help assess how best to remedy the situation.

**Date:**

**Title of Sponsored Project/Activity:**

**Technical Description of Item/Technology/Equipment/Software To Be Transferred:**

**Responsible Individual (Project Manager / Principal Investigator {PI})**

**Work Address:**

**Phone:**

**E-mail:**

1. **Physical Security Plan:** (Project data and/or materials must be physically shielded from observation by unauthorized individuals by operating in secured laboratory spaces, or during secure time blocks when observation by unauthorized persons is prevented. This would pertain to laboratory management of “work-in-progress”)
  - a. **Location** (describe the physical location of each sensitive technology / item to include building and room numbers. A schematic of the immediate location is highly recommended):
  - b. **Physical Security** (provide a detailed description of your physical security plan designed to protect your item/technology from unauthorized access, i.e., secure doors, limited access, security badges, CCTV, etc.):
  - c. **Perimeter Security Provisions** (describe perimeter security features of the location of the protected technology / item):

2. **Information Security Plan** (Appropriate measures must be taken to secure controlled electronic information, including User ID's, password control, SSL or other approved encryption technology. Database access must be managed via a Virtual Private Network (VPN), allowing only authorized persons to access and transmit data over the internet, using 128-bit Secure Sockets Layer (SSL) or other advanced, federally approved encryption technology).
- a. **Structure of IT security** (describe the information technology (IT) setup / system at each technology / item location:
  - b. **IT Security Plan** (describe in detail your security plan, i.e., password access, firewall protection plans, encryption, etc.):
  - c. **Verification of Technology/Item Authorization** (describe how you are going to manage security on export controlled materials in the case of terminated employees, individuals working on new projects, etc.):
  - d. **Conversation Security** (Discussions about the project or work product are limited to the identified contributing investigators and are held only in areas where unauthorized personnel are not present. Discussions with third party subcontractors are only to be conducted under signed agreements that fully respect the non-U.S. citizen limitations for such disclosures. Describe your plan for protecting export controlled information in conversations):
  - e. **Graduate Thesis:** Any graduate student fulfilling their thesis research requirement with results from projects that are ITAR controlled must be a U.S. Person (or, alternatively, the University must have obtained an export license for his/her participation and access to ITAR controlled technical data). In addition, the thesis advisory committee and the participants to thesis defense must be U.S. Persons and/or an export license must have been granted for their participation and access to ITAR controlled data. Publication of the thesis and research results must be approved by the sponsor and might be delayed to meet the requirements of the research contract. Similar restrictions on access to technology/technical data apply to thesis research involving EAR controlled technology/technical data except that the restricted access by non-U.S. Persons is technology and citizenship specific.
  - f. **End-of-Project security measures:**
  - g. **Departure from the University:** The procedures outlined above in 2.c. will be used when a PI or other project member of an ITAR controlled project is departing from the University.

### 3. Item Security

- a. **Item Marking** (Export controlled information must be clearly identified and marked as such):
- b. **Item Storage**

### 4. Project Personnel (clearly identify every person (including their national citizenship) who is determined to have authorized access to the controlled technology / item).

- a. **Name:**
- b. **Name:**
- c. **Name:**
- d. **Name:**

\*\*It is the responsibility of the PI to inform the Export Control and Compliance Officer of any new addition to the project personnel. The T/ECP will be updated accordingly.

### 5. Personnel Screening Procedures

- a. At a minimum, all individuals receiving access to the controlled items/information must be screened in Visual Compliance.
- b. **Background Checks** (describe types of background checks performed on persons with access to technologies / items, i.e., criminal, driver's license, etc.):
- c. **Third Party Contractors** (describe security screening procedures for temporary employment agencies, contractors, etc.):

### 6. Training / Awareness Program

- a. **Foreign Nationals** (describe schedules and training for informing foreign national employees of technology access limits):
- b. **U.S. Employees** (describe training for U.S. employees with access to controlled technology areas.)
  - i. This is completed by the ECCO. Upon completion of the export-control training, records will be maintained documenting training in export-control regulations and familiarity with Cornell's Export Compliance requirements.

## 7. Self-Evaluation Program

- a. **Self-Evaluation Schedule** (describe how often you plan to review / evaluate your T/ECP):
  - b. **Audit Checklist** (provide a checklist for items reviewed during self-evaluation audits):
    - i. **Update employee training policy, if required**
    - ii. **Check Visual Compliance for all individuals accessing.**
    - iii. **Proper identification and labeling of stored software**
    - iv. **Verify all physical security measures (locks, etc.) are in place with no breach**
    - v. **Verify IT and network security (no unauthorized access outside of course teaching)**
    - vi. **Verify physical layouts of rooms within classroom are compliant with ensuring security from external users.**
  - c. **Action Item and Corrective Procedures** (describe your process to address findings in yourself evaluation audits):
8. **Special notes** (this paragraph will include all other requirements specific to the project such as publication restrictions, etc.):

## EXPORT CONTROL PLAN CERTIFICATION

Project Director:

Department:

Sponsor Name:

Project Title:

Proposal/Agreement Number:

It has been determined that a Technology / Export Control Plan (T/ECP) is necessary for this project / activity. This is to acknowledge I have read and understand the Export-Controlled Information Overview, and that I agree to comply with the requirements of the T/ECP, which is attached herewith.

Name, Title, Signature, Date

---

Name, Title, Signature, Date

---

Name, Title, Signature, Date

Acknowledgement of Department Chair:

---

Name, Title, Signature, Date

Approval of IT Representative:

---

Name, Title, Signature, Date

## **Appendix B**

### **OSP Pre- and Post- Award Review Criteria**

#### **During Proposal Preparation**

If your project includes foreign activities, including travel, collaboration with consultants or subcontractors (here or abroad), or overseas shipments, contact your GCO or the Export Controls Officer as early as possible. They will help determine if additional steps need to be taken to ensure that the project is carried out as seamlessly as possible. The GCO may advise that consultation with other Cornell offices (i.e., Global Cornell, the Office of the Vice Provost for International Affairs, or the Export Controls Office) is necessary or helpful to the success of the project.

#### **Post-Award Activities**

During the term of the award, foreign activities may arise that must be vetted for export control concerns. For example, international shipments and foreign travel should be processed in accordance with the direction found on the [Export Control Page](#).

In addition, access to proprietary or controlled information by a foreign national, must be reviewed and approved by the [Export Control Office](#), **prior** to such access occurring.

#### **Sample Contract Language:**

Each Party acknowledges that they are subject to U.S. export control laws and regulations (collectively, “Export Control Laws”), which include (without limitation) the International Traffic in Arms Regulations (ITAR), the Export Administration Regulations (EAR), and regulations and orders administered by the Treasury Department’s Office of Foreign Assets Control (“OFAC Regulations”). Each Party agrees to comply with all Export Control Laws. Neither Party shall disclose any technology or technical data subject to Export Control Laws unless and until a plan for the transfer, use, dissemination, and control of the information has been approved by each Party’s Export Control Officer. Sponsor expressly acknowledges and agrees that University shall conduct the Project as “fundamental research” under Export Control Laws, such that the Project results qualify as “public domain” under ITAR Parts 120.10(a)(5) and 120.11 or as “publicly available” under EAR Parts 734.3(b)(3) and 734.8(a) and (b).

## APPENDIX C

[National Security Decision Directive 189 \(NSDD 189\)](#)



### [\[National Security Decision Directives \(NSDDs\)\]](#)

---

[stamped:] UNCLASSIFIED

September 21, 1985 (re-affirmed May24, 2010)

### **NATIONAL POLICY ON THE TRANSFER OF SCIENTIFIC, TECHNICAL AND ENGINEERING INFORMATION**

#### **I. PURPOSE**

This directive establishes national policy for controlling the flow of science, technology, and engineering information produced in federally-funded fundamental research at colleges, universities, and laboratories. Fundamental research is defined as follows:

"Fundamental research' means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons."

#### **II. BACKGROUND**

The acquisition of advanced technology from the United States by Eastern Bloc nations for the purpose of enhancing their military capabilities poses a significant threat to our national security. Intelligence studies indicate a small but significant target of the Eastern Bloc intelligence gathering effort is science and engineering research performed at universities and federal laboratories. At the same time, our leadership position in science and technology is an essential element in our economic and physical security. The strength of American science requires a research environment conducive to creativity, an environment in which the free exchange of ideas is a vital component.

In 1982, the Department of Defense and National Science Foundation sponsored a National Academy of Sciences study of the need for controls on scientific information. This study was chaired by Dr. Dale Corson, President Emeritus of Cornell University. It concluded that, while there has been a significant transfer of U.S. technology to the Soviet Union, the transfer has occurred through many routes with universities and open scientific communication of fundamental research being a minor contributor. Yet as the emerging government-university-industry partnership in research activities continues to grow, a more significant problem may well develop.

#### **III. POLICY**

It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted. It is also the policy of this Administration that, where the national security requires control, the mechanism for control of information generated during federally-funded fundamental research in science, technology and engineering at colleges, universities and laboratories is classification. Each federal government agency is responsible for: a) determining whether classification is appropriate



prior to the award of a research grant, contract, or cooperative agreement and, if so, controlling the research results through standard classification procedures; b) periodically reviewing all research grants, contracts, or cooperative agreements for potential classification. No restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification, except as provided in applicable U.S. Statutes.

[stamped:] UNCLASSIFIED

[Ashton B. Carter, Under Secretary of Defense for Acquisition, 5/24/10 Directive: No restrictions on DOD Contracted Fundamental Research](#)

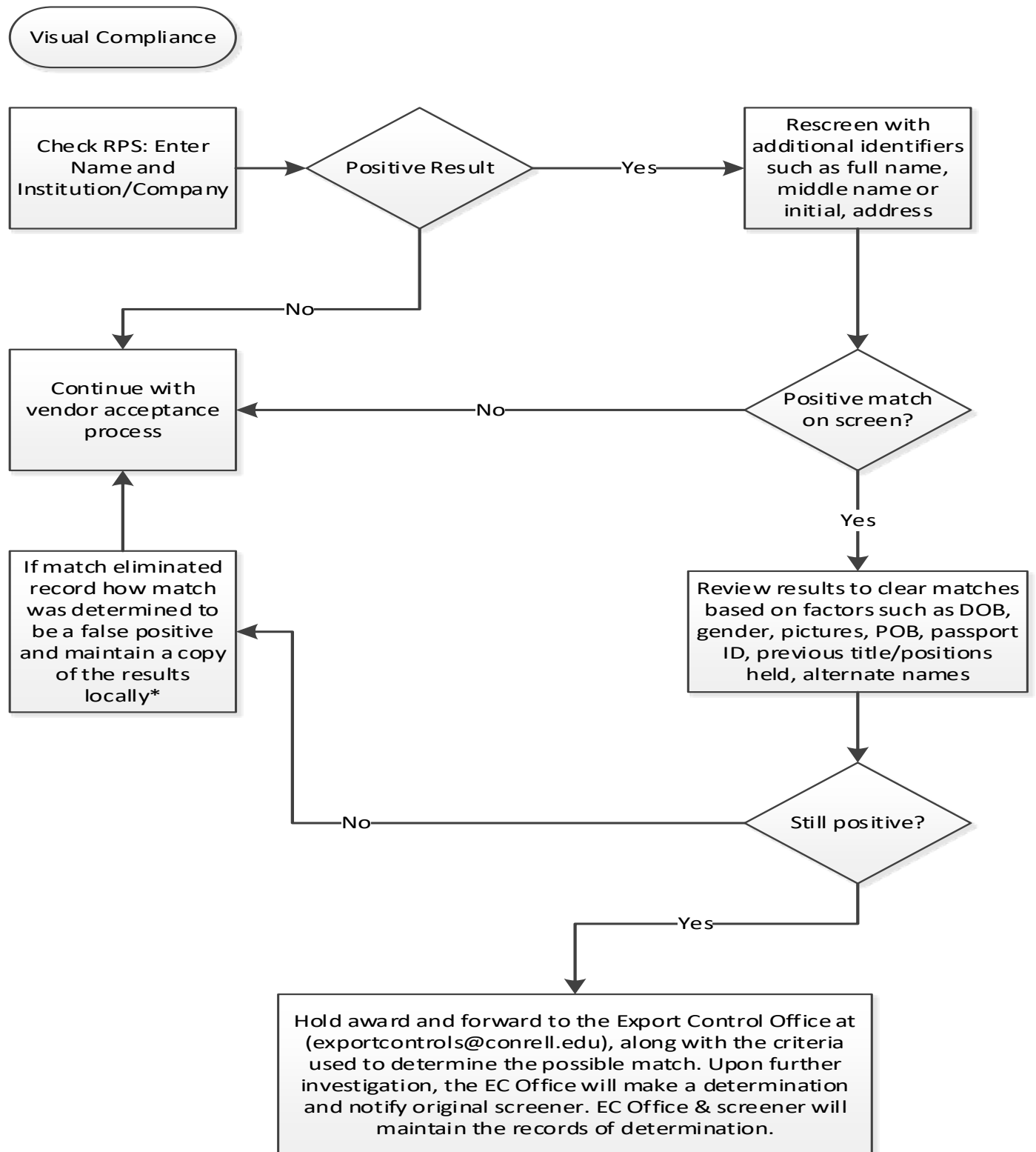
## APPENDIX D

### Restricted Party Screening Procedure

It is the responsibility of the applicable administrative offices on campus to comply with U.S. Government-imposed restrictions on doing business with certain entities. The Government has published various lists of names and entities for which these restrictions exist. These lists must be reviewed to ensure that a proposed transaction does not violate export regulations.

Cornell University has a subscription to the [Visual Compliance](#) tool which enables efficient screening. Access can be obtained by contacting the Export Control Office at [exportcontrols@cornell.edu](mailto:exportcontrols@cornell.edu).

Individual users will perform screenings in accordance with the procedure below. Individual users are also responsible for monitoring the daily “alerts” from Visual Compliance to ensure that a previously cleared entity or individual does not subsequently become prohibited. Users will conduct a Restricted Party Screening (RPS) by entering the name of the individual or potential sponsor, and ascertain the risk following this procedure:



## APPENDIX E

### TMP Self Certification Letter

#### License Exception for Foreign Travel

##### **Export License Exception (TMP) for Temporary Exports/Reexports**

This exception (TMP) can be used for travel outside the U.S. when you are taking items or technology that would normally require a license from the State Department of Commerce.

##### **What the exception covers:**

The export of items, technology, commercial software, and encryption code is subject to export control regulations (this includes laptops, PDA's and digital storage devices). The Department of Commerce's Export Administration Regulations (EAR) makes an exception to licensing requirements for the temporary export or re-export of certain items, technology, or software for professional use as long as the criteria in the **Export License Exception (TMP) Certification** are met.

The following items are controlled by the EAR with Export Control Classification Numbers listed:

- Laptops, iPhones, Blackberries: 5A992
- Mass market software (Windows, OS X, Office, Adobe products, Visual Studio): 5D992
- Open source software (Linux, Apache): 5D002

The Commerce Control Listings for these ECCNs are in <https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl>

The TMP exception is documented in §740.9 of the EAR.

##### **What the exception does NOT cover:**

The exception does not apply to any EAR satellite or space-related equipment, components, or software, or to any technology associated with high-level encryption products and cannot be used for travel to Cuba, Iran, North Korea, Syria or the Crimea region of Ukraine.

##### **Record-keeping:**

Fill out the exception form prior to travel (keep a copy for your files) and return to the Export Control Office via e-mail @ [exportcontrols@cornell.edu](mailto:exportcontrols@cornell.edu). Contact the Export Control Office at 607.255.5284 if you have questions regarding the exception and procedures.

**EXPORT LICENSE EXCEPTION (TMP) CERTIFICATION**  
**Export Administration Regulations (EAR) controlled Items, Technology, and Software**

**To:** University Export Compliance Officer **From:** [Insert Name of CU PI or Employee]

**Date:** [Insert Date]

**Re:** **Export License Exception for Temporary Exports/Reexports\***

The export of items, technology, commercial software, and encryption code is subject to export control regulations (this includes laptops, PDAs and digital storage devices). The Department of Commerce's Export Administration Regulations (EAR) makes an exception to licensing requirements for the temporary export or reexport of certain items, technology, or software for professional use as long as the criteria to which you are certifying below are met. The exception does not apply to any EAR satellite or space-related equipment, components, or software, or to any technology associated with high-level encryption products. In addition, this exception does not apply to items, technology, data, or software regulated by the Department of State's International Traffic in Arms Regulations (ITAR).

Detailed Description of Items, Technology or Software to which this Certification applies:

[Insert description here]

By my signature below, I certify that:

1. I will ship or hand-carry the items, technology, or software to [insert country(s) traveling to] as a "tool of the trade" to conduct Cornell University business only;
2. **I will return the items, technology, or software to the US on [insert return date] which is no later than 12 months from the date of leaving the US** unless the items, technology, or software are certified by me to have been consumed or destroyed abroad during this 12 month period;
3. I will keep the items, technology, or software under my "effective control" while abroad (defined as retaining physical possession of item or keeping it secured in a place such as a hotel safe, a bonded warehouse, or a locked or guarded exhibition facility);
4. I will take security precautions to protect against unauthorized release of the technology while the technology is being shipped or transmitted and used abroad such as:
  - a. use of secure connections when accessing e-mail and other business activities that involve the transmission and use of the technology,
  - b. use of password systems on electronic devices that store technology, and
  - c. use of personal firewalls on electronic devices that store the technology;
5. **I will not ship or hand-carry the items, technology or software to Iran, Syria, Cuba, North Korea, or the Crimea region of Ukraine without consulting with Cornell University's Export Control Office.** If I am planning to travel to these countries, I will consult Cornell University's Export Control Office.

Signed:

[Name of PI/Employee]

OSP #:  
[If applicable]

***\*Keep a signed copy with you when traveling abroad***

## APPENDIX F

### Definitions - Export Control Terms

**Bureau of Industry and Security (BIS)** – The bureau at the U.S. Department of Commerce responsible for enforcing the Export Administration Regulations (EAR). [15 CFR 730-774]

**Code of Federal Regulations (CFR)** – The codification of the general and permanent rules and regulations published in the *Federal Register* by the executive departments and agencies of the U.S. Government.

**Commerce Control List (CCL)** – A list of Items under the export control jurisdiction of the BIS. The CCL is at 15 CFR 774, Supplement 1.

**Commodity Jurisdiction (CJ)** – A determination of whether a particular Item or service is covered by the U.S. Munitions List (USML). The determination entails applying to the DDTC as to whether an article or service is currently covered by the USML. [22 CFR 120.4; 15 CFR 734.6]

**Commodity Classification** – A classification of Items on the Commerce Control List that are subject to the export licensing authority of the Bureau of Industry and Security [15 CFR 738.2]. The classification is represented by an Export Control Classification Number (ECCN).

**Deemed Export** – The release of any Item (information, data, technology, or source code) or service subject to export controls to any foreign national in the United States or abroad. Deemed exports may occur through such means as a demonstration, email, computer access, oral exchanges, or visual inspection of equipment and facilities, as well as the electronic transmission of controlled information or technology. This exchange is “deemed” to be an export to the country of the Foreign National. [15 CFR 734.13]

**Deemed Reexport** – The release of any Item (information, data, technology, or source code) or service subject to export controls by a foreign national who has been licensed to receive it to the national of another foreign country who has not been licensed to receive it. [15 CFR 734.14(b)]

**Defense Article** – Any Item or Technical Data designated in the United States Munitions List (USML). Includes Technical Data recorded or stored in any physical form, models, and mock-ups, or other Items that reveal Technical Data directly relating to the Defense Article listed in the USML. Defense articles also include forgings, castings, and other unfinished products that have reached a stage in manufacturing where they are clearly identifiable by mechanical properties, material composition, geometry, or function as defense articles. Basic marketing information on function, purpose, or general system description does not constitute a Defense Article [22 CFR 120.6].

**Defense Service** – Means the furnishing of assistance (including training), whether in the United States or abroad, to a foreign person in connection with the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing, or use of Defense Articles; or the furnishing of any controlled Technical Data to a foreign national anywhere; or military training of foreign units and forces in the U.S. or abroad. [22 CFR 120.9]

**Directorate of Defense Trade Controls (DDTC)** – The directorate at the Department of State responsible for the administration and enforcement of the International Traffic in Arms Regulations (ITAR). [22 CFR 120-130]

**Dual Use Item** – A term used for EAR-controlled Items that can be used both in commercial applications and in military and other strategic uses. [15 CFR 772.1]

**Employment Exclusion:** No license is required to export an export controlled Item to a foreign national who is a fulltime regular Cornell University employee if the individual meets all of the following criteria: 1) has a permanent address in the U.S. for their entire period of employment; 2) is not a national of a sanctioned country; and 3) agrees in writing not to share the export controlled item with any foreign national. For export control purposes, graduate students working as research assistants on research projects are considered to be students and *not* employees. Generally applicable only to H-1B visa holders. No technology controlled or EI (encryption) reasons or technology or source code controlled for MT (Missile Technology) reasons may be released under this exclusion. [22 CFR 125.4(b)10 and 15 CFR 740.13(f)]

**Export Administration Regulations (EAR)** – Department of Commerce Bureau of Industries and Security (BIS) regulations [15 CFR Parts 730-774] implementing the Export Administration Act of 1979 (EAA), as amended, and the International Emergency Economic Powers Act, as amended.

**Export Control Classification Number (ECCN)** – A five character alphanumeric classification [15 CFR 738.2(d)] used to identify Items on the Commerce Control List that are subject to the export licensing authority of the Bureau of Industry and Security. [15 CFR 738.2]

**Educational Information** – Information released by instruction in catalog courses and associated with teaching laboratories of academic institutions; this educational information is not subject to export controls. [15 CFR 734.3(b)(3)(iii)]

**Export** – Any release of export controlled Items, information, or services outside the U.S. to anyone (including a U.S. citizen). “*Release*” includes shipment as well as oral, written, electronic (fax, e-mail, Internet, etc.), or visual disclosure [15 CFR 734.15; 22 CFR 120.17] as well as the export of encryption source code or object code software. Any release of export-controlled Items, information, or services to a foreign national or foreign person in the U.S. is a Deemed Export.

**Export controlled** – Any Item, information, assistance, Technology, Technical Data, or service which can be considered an export or reexport under the export control regulations such as EAR, ITAR, and OFAC.

**Export License** – A written authorization provided by the appropriate governing regulatory authority (such as BIS, OFAC or DDTC) detailing the specific terms and conditions under which the export, deemed export, reexport, or deemed reexport of export-controlled items, information, technology, services, or other regulated activities are allowed. [15 CFR 772.1; 22 CFR 120.20 and 123]

**Foreign National** – Any person who is not: a U.S. citizen (native or national); an alien who is a “lawful permanent resident” (Green Card) as defined by 8 U.S.C. 1101(a)(20); or a “protected individual” as defined by 8 U.S.C. 1324b(a)(3) designated as an asylee, refugee, or a temporary resident under amnesty provisions. Any foreign corporation, business association, partnership,

trust, society, or any other foreign entity or group, as well as any international organization or foreign government, is considered to be a foreign national under the EAR. [15 CFR 772.1]

**Foreign Person** – 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 U.S., as well as international organizations, foreign governments and any agency or subdivision of foreign governments. [22 CFR 120.16]

**Fundamental Research** – Under the EAR, Fundamental Research is defined as research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons. [15 CFR 734.8]. Under the ITAR, Fundamental Research is similarly defined, with the added requirement that it be conducted at accredited institutions of higher learning in the U.S. in order to be exempt from the controls. [22 CFR 120.11(8)]

**International Traffic in Arms Regulation (ITAR)** – Department of State Directorate of Defense Trade Controls (DDTC) regulations [22 CFR 120-130] implementing the Arms Export Control Act [22 USC 2778] and Executive Order 11958, as amended.

**Item** – A commodity, software or Technology. [15 CFR 772.1]

**License Exception** – An authorization, described at 15 CFR 740, that allows Cornell University exporters (facility, researchers, administrators, students, etc.) to export or reexport, under stated conditions, items subject to the EAR that otherwise would require a license. Unless otherwise indicated, these license exceptions are not applicable to exports under the licensing jurisdiction of agencies other than the Department of Commerce.

**License Exclusion** – An export license is not required if one of these exclusions applies: fundamental research (ITAR, EAR); education information (ITAR, EAR); publicly available information (EAR), or information in the public domain (ITAR).

**Office of Foreign Assets Control (OFAC)** – The office at the Department of the Treasury responsible for blocking assets of foreign countries subject to economic sanctions; controlling participation by U.S. persons, including foreign subsidiaries, in transactions with specific countries or nationals of such countries; and administering embargoes on certain countries or areas of countries. [31 CFR 500 -599]

**Public Domain** – ITAR defines public domain as information which is published and which is generally accessible or available to the public. [22 CFR 120.11(a)(1-8)]

**Published** – Information that is generally accessible to the public without restrictions and, therefore, not subject to the EAR. [15 CFR 734.7 (a)]

**Red Flags** – Possible indicators of an unlawful diversion or an abnormal or suspicious circumstance. [15 CFR 732 Supplement 3]



**Reexport** – A shipment or transmission of export controlled items, information, and services from one foreign country to another foreign country. ITAR [22 CFR 120.19] and EAR [15 CFR 734.14] impose restrictions on shipments and transfers to a third country of goods or technology originally exported from the United States, without proper authorization.

**Technical Assistance Agreement (TAA)** – An agreement for the performance of defense service(s) or the disclosure of *technical data* as opposed to an agreement granting a right or license to manufacture defense articles. [22 CFR 120.22]

**Technical Data** – For purpose of ITAR control, this means information regarded as required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles. Technical Data includes information in the form of blueprints, drawings, photographs, plans, instructions, or documentation. It further includes classified information, information covered by an invention secrecy order and software directly related to defense articles [22 CFR 120.10(a)].

**Technology** – Information necessary for the “development,” “production,” “use,” operation, installation, maintenance, repair, overhaul, or refurbishing of an Item. Technology may be in any tangible or intangible form, such as written or oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, electronic media or information revealed through visual inspection. [15 CFR 772.1]

**Tools of Trade** – Usual and reasonable kinds and quantities of tools of trade (commodities, software, and technology) for use in a lawful enterprise or undertaking of the exporter. For the exporter or reexporter of commodities or software, the transaction must meet the requirements of 15 CFR 740.9 paragraph (a)(1). For export or reexport by U.S. persons of authorized *technology*, the transaction must meet the requirements of 15 CFR 740.9 paragraph (a)(3).

**Travel Registry** - A system for recording international Cornell travel found at <https://travelregistry.cornell.edu/>

**U.S. Export Control Regulations** - Comprised of the EAR, ITAR, and OFAC regulations. Control the release of certain items, technology, information, services, and software both in the U.S. and abroad. Also include sanctions and embargoes against specific entities, individuals and countries, as well as anti-boycott laws.

**U.S. Import Control Regulations** - Laws and regulations that dictate how and if certain items can enter the U.S. and impose duties as applicable. Regulator agencies include the CBP, USDA, CDC, USFWS, FDA, etc.

**U.S. Person** – Any individual who is a citizen of the United States, an individual who is a lawful permanent resident as defined by 8 U.S.C. 1101(a)(20), or an individual 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. [22 CFR 120.15].

**Unit** - A Cornell college, department, program, research center, institute, business center, or other operating unit.

**United States Munitions List (USML)** – A list of articles, services, and related Technical Data designated as Defense Articles and Defense Services pursuant to sections 38 and 47(7) of the Arms Export Control Act, 22 U.S.C. 2778. [22 CFR 121.1(a)]

Additional EAR and ITAR definitions are available at 15 CFR 772.1 and 22 CFR 120, respectively.

## **APPENDIX G**

Policy 4.22 Export and Import Control Compliance:

<https://policy.cornell.edu/policy-library/export-and-import-control-compliance>