



University of Colorado **Boulder**

EXPORT COMPLIANCE PROGRAM MANUAL

Updated 5/18/2016

Contents

Introduction	4
Export Control Laws at UCB	5
Department of State Regulations (ITAR)	6
Regulatory Authority and Scope	6
Important ITAR Definitions	6
The USML Categories	8
Exporting Under the ITAR	9
Commodity Jurisdiction	9
ITAR License Exemptions and Exclusions	9
Department of Commerce Regulations (EAR)	10
Regulatory Authority and Scope	10
Important EAR Definitions and Concepts	10
The Commerce Control List	12
License Exceptions	13
Commodity Classification	14
Anti-Boycott Restrictions	14
Department of Treasury Regulations – Office of Foreign Asset Controls (OFAC)	15
Regulatory Authority and Scope	15
OFAC Licensing for Country Based Programs	16
Additional Considerations	16
Records/Record Retention	16
Labeling of Export Controlled Material	17
Penalties for Export Violations	17
University of Colorado Boulder Export Control Procedures	19
Commitment to Export Control Compliance	19
Roles and Responsibilities for Export Controls at UCB	20
Empowered Official	20
Export Controls Office	20
Export Liaisons	21
Research Administrators	22
Business Administrators	22
Principal Investigators	22

Export Control Analysis	23
Policy	23
Procedure.....	23
Technology Control Plans (TCP)	23
Policy	23
Procedure.....	24
Licensing	24
Policy	24
Procedure.....	25
ITAR Licenses.....	25
EAR Licenses.....	25
OFAC Licenses	25
Training	26
Policy	26
Procedure.....	26
Recordkeeping	26
Policy	26
Procedure.....	27
Monitoring and Reporting Violations	27
Policy	27
Procedure.....	28
Appendix 1: University of Colorado Boulder Export Controls Organization Chart	29
Appendix 2: Export Control Agreement Review Forms	30
License Review Worksheet	30
Visiting Scholar Agreement.....	33
Export Control Checklist for Issues Involved in Sponsored Research	35
Appendix 3: Technology Control Plan Template	37
Appendix 4: Glossary and Abbreviations	40
Glossary.....	40
Abbreviations	41

Overview of Export Controls Regulations

Introduction

This manual is designed to assist you in complying with U.S. export controls. If you have any questions regarding the material contained in this Export Compliance Program Manual, please contact UCB's Office of Research Integrity and Compliance Export Controls Office:

Export Compliance Specialist: Linda.Morris@colorado.edu; 303-492-2889

Export Controls Analyst: Katherine.E.Mills@colorado.edu; 303-492-2427

Empowered Official: Joseph.Rosse@colorado.edu; 303-735-5089

University Counsel: Frank.Robison@cu.edu; 303-492-6532

Export Control laws are a complex set of federal regulations designed to protect United States (U.S.) national security; to prevent the proliferation of weapons of mass destruction; to further U.S. foreign policy including the support of international agreements, human rights and regional stability; and to maintain U.S. economic competitiveness. The export control regulations govern how information, technologies, and commodities can be transmitted overseas to anyone, including U.S. citizens, or to foreign nationals in the U.S. In addition to controlling exports to countries or individuals who are citizens of or located in those countries, the export control regulations ban exports to individuals and companies that have been involved in terrorist or drug trafficking activities as well as those who are barred from conducting exports because of previous violations of the export control laws.

Several federal agencies have jurisdiction over the control of exports, including the Department of Commerce, the Department of Energy, the Department of State, the Department of Treasury, the Nuclear Regulatory Commission, and the U.S. Department of Agriculture. The three principal agencies among these are the Department of State, which administers controls of defense exports through its Directorate of Defense Trade Controls (**DDTC**), the Department of Commerce, which administers export of commercial, 'dual-use' and less sensitive defense items and technologies through the Bureau of Industry and Security (**BIS**), and the Department of Treasury, which administers exports to embargoed countries and specially designated nationals through its Office of Foreign Asset Controls (**OFAC**).

Export Control Laws at UCB

The export control laws apply to many activities at UCB that you might not expect. For example, just entering into a contract with people listed on certain government lists, or sending money to certain countries, may require a license from the U.S. government. As another example shipping certain items, such as ancient artifacts from the UCB Museum of Natural History to foreign destinations, or robots for a competitions outside the U.S., or inert plasmids to a Ph.D. student writing her dissertation at a foreign university, might involve complying with the export control laws.

Universities in the United States, including UCB, have a long tradition of inventing and developing leading-edge technologies that are important for national security and economic competitiveness as well as for education and training scholars from around the world. In recognition of this role, both the Department of State and Department of Commerce export control laws carve out special provisions whereby unrestricted research and classroom teaching activities at university in the U.S. may be excluded from the regulations. Most research activities at UCB will be “fundamental research” as defined in the export control laws, and as a result, do not require an export “license” in most cases. Nonetheless, it is important to understand the limits on fundamental research in the context of the applicable export control regulations. Fundamental research is further discussed in on page 8 of this manual.

The U.S. export control agencies place the burden of understanding and complying with the regulations on the exporter.¹ Even though most research conducted on campus will not be subject to export control restrictions, it is important for the university community to be aware when activities potentially become controlled. The export control laws may apply to research activities on campus if controlled equipment, data, or information is used in the conduct of that research. It is incumbent upon UCB researchers to verify what, if any, information is export controlled, and to prevent the dissemination of such information to foreign parties in the US or abroad. This may be particularly challenging in the conduct of collaborative research with other institutions. The export control regulations apply to the export (even temporary) of controlled University owned equipment for field research and to the shipment of research materials or equipment to locations outside of the United States.

¹ See GAO Report “Export Controls: Agencies Should Assess Vulnerabilities and Improve Guidance for Protecting Export-Controlled Information at Universities:”, December 2006, available at <http://www.gao.gov/assets/260/254189.pdf>

The following brief descriptions of the export control laws are meant to provide an overview of the regulations as they impact activities at UCB. Determining which, if any, of the regulations apply to the particular project is complex; the Export Controls Office will work closely with researchers to make that determination and, when necessary, seek a determination from the relevant agencies.

Department of State Regulations (ITAR)

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. For example, military aircraft are on the USML, as are their engines, electronic controls, and inertial navigation systems, even though such components may have other applications. If a commodity contains a part or component that is controlled under the ITAR, such as a controlled inertial navigation system, then that commodity is also controlled under the ITAR, regardless of whether or not that commodity has an inherently military purpose. Thus, an autopilot system used in basic robotics research at UCB may be controlled under the ITAR.

Many items designed for military use are also used for research completely unrelated to that military use. These specific items are controlled under the ITAR even though they are not being used in any military activity. It is important to understand that the ITAR designation is unrelated to UCB's use of a controlled item.

Important ITAR Definitions

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. Additional definitions can be found in Appendix 4.

Defense article is defined in [22.C.F.R. § 120.6](#). It means any item or technical data that was or will be 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.

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 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. It also includes providing any foreign person any technical data as defined above. It is important to note that defense services may apply even if the information being furnished is in the public domain.

Public Domain is defined in [22 C.F.R. § 120.11](#). Public domain information is information that is published and generally accessible or available to the public. The ITAR describes means by which public domain information might be rightfully available, which in addition to libraries, subscriptions, newsstands and bookstores, include published patents and public release at conferences, meetings and trade shows in the United States where those venues are generally accessible to the public. Posting ITAR-controlled technical data to the Internet does not automatically make it public domain, and may represent an illegal export.

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 where the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. The ITAR considers fundamental research in science and engineering at accredited institutions of higher learning in the U.S. to be in the [public domain](#), and, therefore, no export license would be needed to export the resulting information abroad, or share it with foreign nationals in the United States. However, 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 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. It is important to note that fundamental research applies only to the information generated, and not to any tangible technology created in the process.

The USML Categories

The USML defines twenty-one classes of defense articles. For detailed descriptions of what is included in each category, the ITAR may be accessed [online](#). ITAR-controlled research at UCB is typically included in Categories IV, VIII, XII, XIV, and XV (highlighted in bold below). Note that Category XXI (Miscellaneous Articles) is reserved for future use by the DDTC for controlling new technologies that will fall under the ITAR.

- I. Firearms, Close Assault Weapons and Combat Shotguns
- II. Guns and Armament
- III. Ammunition/Ordinance
- IV. Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs and Mines**
- V. Explosives, Propellants, Incendiary Agents, and their Constituents
- VI. Vessels of War and Special Naval Equipment
- VII. Tanks and Military Vehicles
- VIII. Aircraft and Associated Equipment**
- IX. Military Training Equipment
- X. Protective Personnel Equipment
- XI. Military Electronics
- XII. Fire Control, Range Finder, Optical and Guidance and Control Equipment**
- XIII. Auxiliary Military Equipment
- XIV. Toxicological Agents and Equipment and Radiological Equipment**
- XV. Spacecraft Systems and Associated Equipment**
- XVI. Nuclear Weapons, Design and Testing Related Items
- XVII. Classified Articles, Technical Data and Defense Services Not Otherwise Enumerated
- XVIII. Directed Energy Weapons
- XIX. [Reserved]
- XX. Submersible Vessels, Oceanographic and Associated Equipment
- XXI. Miscellaneous 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, or performing a defense service on behalf of a foreign person whether in the U.S. or abroad. (See [22 C.F.R. § 120.17](#) for a complete listing of export meaning under the ITAR).

This definition is extremely broad. It includes taking controlled technical data out of the U.S. on a laptop computer, smartphone or USB drive, 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. Exports of ITAR controlled items are prohibited to some countries and individuals, meaning that an export license WILL NOT be granted. The list of proscribed destinations may be found [online](#).

Commodity Jurisdiction

The DDTC has the authority 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, the DDTC must be consulted if there is any doubt as to whether an article or service is subject to the ITAR. At UCB, the Export Controls Office will work with researchers and the appropriate U.S. Government agencies to obtain correct classification for any UCB research project.

ITAR License Exemptions and Exclusions

While strict, the ITAR has specific license exemptions which permit the permanent or temporary export of defense articles and technical data by U.S. persons in lieu of obtaining an export license from the DDTC. These exemptions are authorizations that cover very specific situations and have specific requirements. An important exemption to universities such as UCB is the Bona fide, full-time employee exemption² (also known as the BFE). The BFE allows for disclosure of unclassified technical data in the United States by U.S. institutions of higher learning to foreign persons who are bona fide and full time regular employees of that institution. The exemption also requires that the foreign national has a permanent residence in the United States during the period of employment and is not a national of a country to which exports are prohibited. The term “bona fide and full time regular employee” does not

² Full text of [§125.4\(b\)10](#)

apply to student employees, and most universities find that only H-1B visa holders meet the criteria of the exemption.

As previously discussed, a license is not needed to export information that is already found in the public domain. Information released in connection with catalog-listed courses at a university is excluded from ITAR export controls. This includes information released during lectures, instruction in teaching laboratories and inclusion in course materials, as long as the information has already been rightfully published in the public domain. Additionally, information and technology is not controlled if it is part of fundamental research, defined to mean “basic and applied research” in science and engineering at accredited institutions of higher learning in the United States where the resulting information is ordinarily published and shared broadly within the scientific community.

Department of Commerce Regulations (EAR)

Regulatory Authority and Scope

The Export Administration Regulations (EAR) control 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 UCB include much of the space and aviation technology that is not included on the ITAR, laboratory equipment such as centrifuges, analyzers and fabrication equipment (such as milling machines and etching equipment for electronics) as well as certain chemicals, ceramics, microorganisms and toxins. These items are classified on the Commerce Control List (CCL). The CCL is a “positive list;” in other words, if an item is NOT listed on the CCL, then generally the EAR does not apply.

Like the ITAR, the EAR includes a number of exceptions that are important to UCB researchers. These include exclusions for 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; the Export Controls Office can assist in these interpretations.

Important EAR Definitions and Concepts

Export is defined in [15 C.F.R. § 732.2\(b\)](#) as an actual shipment or transmission of items subject to the EAR out of the U.S. as well as the release of technology or software subject to the EAR in a foreign country or to a foreign national either in the U.S. or abroad.

Deemed Export is defined in [15 C.F.R. § 732\(b\)\(ii\)](#). 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. For example, a research sample might be sent to collaborators in the UK, but then reexported to researchers in Israel, a country with more significant export restrictions. Analysis of export licensing requirements must consider the final end user, including any reexports. 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. § 732(b)(4).

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 interested public in any form.³ Publications may take the form of periodicals, books, print, electronic media, public web sites, or any other media available for general distribution. General distribution may be defined as available to an interested community, such as a technical journal available to scientists in a relevant field, so long as the price charged for the publication does not exceed the cost of reproduction and distribution. Articles submitted to journals for consideration for publication 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 technically qualified persons*, is considered to be publication of that information. Software is published when it is available for general distribution either free or at the cost of distribution. *However, strong encryption software remains controlled, regardless of general availability.*

³ Published information and software under the EAR differs from the ITAR in regarding most material subject to the EAR to be publically available once rightfully posted to a public website. Similarly, the ITAR requires that information already be published to be considered in the public domain, whereas for the EAR, information that has been, or is about to be, published is considered published information.

Fundamental Research is *basic and applied research in science and engineering, where the resulting information is ordinarily published and shared broadly within the scientific community. Such research can be distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary reasons or specific 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 scientific and technical information resulting from the research. Temporary delays in publication for the protection of sponsor proprietary information do not remove research from the fundamental domain. However, if that sponsor's proprietary information is subject to the EAR, then that information remains subject in the conduct of the research. **UCB researchers receiving proprietary information from corporate research sponsors should consult the export compliance office to ensure compliance with the EAR in the conduct of the related research.**

Educational Information is defined in [15 C.F.R. § 734.9](#). Educational Information 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. For example, participation by UCB international students in a university graduate course on design and manufacture of very high-speed integrated circuitry will not be subject to export controls, even though the technology is on the CCL. **The key factor is the fact that the information is provided by instruction in a catalog course.**

As long as the course material is subject only to the EAR (and not ITAR), foreign students from any country may enroll in a course. Course activities are exempt from the controls, even if the course contains recent and unpublished results from laboratory research, so long as that research qualifies as fundamental research.

The Commerce Control List

The Commerce Control List (CCL) may be accessed [online](#). 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 reason for

control. As an example, an Unmanned Aerial Vehicle (UAV) with the ability to maintain flight for 30 to 60 minutes has an ECCN of 9A012, where as an UAV with the capability of autonomous flight control has an ECCN of 9A120. In general, “###” with lower numbers are controlled to more destinations than those with higher numbers.

The categories and product groups are as follows:

Commerce Control List Categories	
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

Commerce Control List Product Groups	
A	Systems, equipment and components (finished or unfinished goods)
B	Test, inspection and production equipment (manufacturing equipment)
C	Material
D	Software
E	Technology

The EAR export licensing regime is much more complex 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.

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 UCB community should consult with the export compliance office 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 UCB community travelling abroad are BAG, which applies to personally-owned items taken abroad for personal use while abroad, and TMP, which applies to the temporary export of UCB-owned equipment, including laptop computers and other equipment listed on the CCL, for work-related activities. These activities include professional presentations, teaching, and field research. 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.

Commodity Classification

BIS encourages exporters to use the detailed descriptions in the CCL to identify the potential ECCN of 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 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. Members of the UCB community who need assistance with classifying items should contact the Export Controls Office. When unsure about a self-classification, the university may submit the item/technology to BIS for a formal classification.

Anti-Boycott Restrictions

The Anti-Boycott provisions of the EAR were designed to address foreign governments' boycotts of countries friendly to the U.S. The provisions were first implemented in response to the Arab League Boycott of Israel. Arab countries including Kuwait, Lebanon, Libya, Qatar, Saudi Arabia, Syria, the United Arab Emirates and Yemen have been known to impose boycott restrictions on Israel and companies that do business with Israel. Companies, as well as individuals, are "blacklisted" under boycott.

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 and specifically prohibit the following activities:

- Agreement to refuse or actual refusing to do business with a boycotted country or with blacklisted persons
- 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 very limited. Additionally, U.S. persons asked to engage in the prohibited activities are required to report the request to BIS. If you encounter any boycott language in a UCB activity or contract, please contact the Export Controls Office or University Counsel for assistance in determining whether an exception is applicable and if reporting to BIS is required.

[Department of Treasury Regulations – Office of Foreign Asset Controls \(OFAC\)](#) [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. Sanctions are country/program specific, and are subject to frequent change based on the changing geo-political landscape. In addition to foreign countries and regimes, OFAC imposes sanctions on individuals, such as people the U.S. government deems to be terrorists and narcotics traffickers. 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). They prohibit importation and exportation of goods and services as well as related financial transactions or engaging in business activities with SDNs. As of early 2016, OFAC sanctioned countries include the Balkans, Belarus, Burma/Myanmar, Cote d'Ivoire, Cuba, the Democratic Republic of Congo, Iran, Iraq, Lebanon, the Former Liberian Regime of Charles Taylor, Libya, North Korea, Somalia, Sudan, Syria, and Zimbabwe. Additional activity-based sanctions programs include Counter Narcotics Trafficking, Counter Terrorism, Non-Proliferation, and Transnational Criminal Organizations sanctions as well as the Rough Diamond Trade Controls. The activity-based sanctions programs are implemented through the designation of individuals engaging in the banned activities as SDNs. Updated lists of sanctioned countries are available online.

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 from the embargo (for instance personal communications, exchange of informational materials, etc.) as well as what activities may be permitted under either a general or specific license. Activities which that 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. At UCB, the Export Controls Office should be contacted when considering any proposed OFAC sanctioned activities. Note that license applications to OFAC require substantial advance planning, often taking 6 months or more to be adjudicated by OFAC once submitted.

Additional Considerations

Records/Record Retention

The ITAR, EAR and OFAC regulations all stipulate record keeping requirements for regulated export activities. Under each of these sets of regulations, records must be retained for five years after the completion of the activity and made available to the regulating authority upon request. Records that should be retained include all memoranda, notes, correspondence (including email), financial

records, shipping documentation, as well as any other information related to the export activities. Additionally, when a license exception (EAR) or license exemption (ITAR) is used, additional records documenting the applicability of the exception/exemption may be required and in some cases there may be additional reporting requirements.

Labeling of Export Controlled Material

Export of items controlled under the ITAR or EAR should be clearly marked as controlled, with the appropriate regulatory control cited. Any export requiring a license, as well as exports with a dollar value greater than \$2500, must be entered into the Department of Census Automated Export System (AES) prior to the export of the item or information. While commercial freight forwarders will usually handle the AES entry, the Export Controls Office is able to assist the UCB community for the export of items being hand-carried or technical data being mailed or electronically transmitted.

Penalties for Export Violations

Violation of the export control laws can result in both civil and criminal penalties including fines and imprisonment. Although there is a maximum amount for a civil or criminal penalty, the actual penalty is often multiplied. For instance, if multiple unauthorized shipments of the same item to the same end user were completed, each individual shipment could potentially incur the maximum penalty. Even a single unauthorized export may result in multiple violations (e.g. export without a license, false representation on shipping documents, acting with knowledge of a violation, etc.). Maximum penalties for violations under the OFAC, ITAR and EAR are \$1,000,000 and criminal prison sentences can be up to 20 years for individuals engaging in the violations. Violation of the export control laws may result in the loss of future export privileges (EAR) or even from debarment from participation in future federal contracts (ITAR).

In assessing penalties, regulatory agencies will consider mitigating factors. Mitigating factors include whether the disclosure of the violation was made voluntarily, whether the violation is an isolated incident or part of a pattern of continuing behavior, whether there was a compliance program in place at the time of the violations, whether steps were taken to improve the compliance program after the discovery of the violation and whether the violation was due to inadvertent action, mistake of fact, or a good faith misinterpretation of the laws.

Possible violations of export control laws discovered at UCB should be brought to the attention of the Export Controls Office. Most importantly, if there is a question as to whether an activity would be

a violation of the export control laws, it is important to consult with the Export Controls Office prior to engaging in the activity.

University of Colorado Boulder Export Control Procedures

Commitment to Export Control Compliance

The University of Colorado is committed both to the preservation of academic freedom and to compliance with all applicable U.S. Government export regulations. The vast majority of teaching and research activity at UCB falls within one or more exemptions and exclusions from licensing requirements. However, it is important to understand how the laws described in the first section of this manual apply to UCB practices and procedures, as well as the corresponding compliance obligations.

The U.S. government defines exports to include not only tangible or “physical” items such as biological materials, chemicals, and equipment, but also intangible information that may include research data, formulae, engineering designs and ideas. Furthermore, an export is defined not only as an actual physical shipment, but also includes electronic and voice transmissions out of the United States (e.g. email or a phone call to a colleague at a foreign institution or remotely accessing controlled documents while travelling internationally). Exports also include the release of technology to foreign nationals within the U.S., the provision of training or services involving controlled equipment to foreign nationals in the U.S. or abroad, and engaging in transactions or providing services to entities and individuals who are on embargo or specially designated nationals lists.

Exports are controlled by multiple federal agencies including: the Department of State through the International Traffic in Arms Regulations (ITAR), the Department of Commerce through the Export Administration Regulations (EAR), and the Department of Treasury through the Office of Foreign Assets Control (OFAC). Each agency has its own procedures for enforcement, but violations of any of these regulations can result in significant institutional and personal penalties including fines of up to \$1,000,000 per violation, incarceration for up to 20 years, and the loss of future exporting privileges.

As stated, the University of Colorado is committed to the preservation of academic freedom. However, the University recognizes its obligation to comply with the U.S. export control regulations. Fortunately most, but not all, research activities on campus fall under the “fundamental research exemption”, which provides that basic and applied research activities NOT subject to publication or access restrictions will not be subject to export controls. Other exemptions apply to information shared in the conduct of teaching activities on campus IN the U.S. as well as to information that is already

publicly available. The export regulations are complex and continually changing, so it is important to consider each activity on an individual basis.

The UCB Office of Research Integrity (ORI) is responsible for helping the community understand and comply with the export control laws, and apply for an export license when necessary. Please see the [UCB Export Control website](#) for additional information including analytical tools to assist you in determining if and how the regulations apply to an activity, as well as points of contact for assistance with export control matters.

Roles and Responsibilities for Export Controls at UCB

While it is the responsibility of senior university administrators to ensure the existence of adequate resources and management support to comply with the export control regulations and to resolve identified export control issues, the following roles focuses on other key actors in export compliance at UCB (see also Appendix I).

Empowered Official

The Associate Vice Chancellor for Research Integrity and Compliance is the University of Colorado Boulder's Export Controls Officer and Empowered Official. The Empowered Official has the authority to represent the university before the export control regulators in matters related to registration, licensing, commodity jurisdiction and classification requests, and voluntary or directed disclosures. While certain oversight functions may be delegated, only Empowered Officials may sign paperwork and bind the university in any proceeding before DDTC, BIS, OFAC, or any other government agency with regard to export control responsibilities.

The Empowered Official will also work with the Export Control Advisory Group to review and provide feedback on the UCB export controls compliance program. The body reviews relevant university policies and procedures and makes recommendations to facilitate research in adherence with federal regulations and best practices among peers. The Export Control Advisory Group is comprised of representatives from the University of Colorado Boulder research community and administration affected by export control regulations.

Export Controls Office

The Export Controls Office (ECO), a unit of the Office of Research Integrity and Compliance, is the primary campus organization charged with ensuring that research activities comply with export

control requirements. The office collaborates with other Export Liaisons and senior management in order to accomplish the following tasks:

1. Identify areas at UCB that are impacted by export control regulations;
2. Develop procedures and other guidance to assist the university in remaining in compliance with export control regulations;
3. Educate inventors, principal investigators, research centers and academic units about export control regulations and procedures at UCB;
4. Coordinate with other UCB units such as Business Services, Purchasing, Travel, International Programs, International Student and Scholar Services (ISSS), Human Resources and the Technology Transfer Office (TTO) regarding export control regulations and procedures at UCB;
5. Monitor and interprets export control legislation;
6. Apply for export licenses, commodity jurisdiction and classification requests, and advisory opinions from the U.S. Government;
7. Investigate and report export control noncompliance as required;
8. Work with others such as Export Liaisons to facilitate understanding and compliance with export controls;
9. Assist investigators, researchers and offices at UCB when research involves export controlled equipment or information;
10. Seek advice from the Office of University Counsel in analyzing and handling export control compliance issues;
11. Assist PIs in developing technology control plans for research involving export controlled items or information to ensure compliance with export control regulations;
12. Advise and assist with record keeping for export controlled activities at UCB;
13. Maintain the campus export control website

Export Liaisons

The export liaisons are individuals appointed from academic and business units across campus to assist the Export Controls Office in identifying training needs, identifying potential export control issues, and to serve as local points of contact for questions related to export controls. The export liaisons are trained and have access to software to perform restricted party screening. The export liaisons meet with the Office of Export Compliance on a regular basis to promote the export compliance program at UCB.

Research Administrators

The school and department research administrators work closely with Export Controls Office, the Office of Contracts and Grants (OCG) and the PI. Together with Export Controls Office, they:

1. Provide assistance to PIs in reviewing terms of sponsored program agreements, material transfer agreements (MTA) and other non-monetary agreements to identify restrictions on publication and dissemination of research results and flag such restrictions in agency requests for proposals;
2. Provide assistance to PIs in identifying international components of sponsored program agreements, identifying potential export control issues in the proposed international component;
3. Communicate identified potential export control issues to the PI and the Export Controls Office;
4. Communicate with the Export Controls Office and OCG about any changes in awards that necessitate a re-review of the project for export controls.

Business Administrators

The school and department business administrators assist in ensuring compliance with export control regulations by identifying potential export issues in unit activities. Such issues may include reviewing invoices for statements that items may not be exported, ensuring international shipping is compliant with export laws, ensuring that payments do not go to, or contracts are not entered into, anyone on the then-current Specially Designated Nationals (SDN) list, ensuring that international travel is compliant with applicable export control regulations, and ensuring that visa export certification information has been completed.

Principal Investigators

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 corporate non-disclosure agreement, or transfer export-controlled articles or services to a foreign national without prior authorization as required. Each PI must:

1. Understand his/her obligations under the export control laws;
2. Assist the Export Controls Office in correctly classifying technology and items that are subject to export control laws;

3. Assist in developing and maintaining the conditions of a Technology Control Plan for any activity, data or equipment where the need for such a plan is identified;
4. Ensure that research staff and students have been trained on the Technology Control Plan and on the export control regulations should any apply.

Export Control Analysis

Policy

An export control analysis will be performed when a PI submits a proposal, receives an award, or changes the scope of an existing project. The Office of Contracts and Grants will send to the Export Controls Office any proposal or award that is subject to export regulations for review.

Procedure

The Office of Contracts and Grants staff are trained to identify red flags in proposals and awards which indicate the possible presence of export control issues:

1. References U.S. export control regulations (beyond a mere statement to comply with the law);
2. Restricts access or participation based on country of origin;
3. Restricts the use of proprietary or confidential information;
4. Grants the sponsor pre-publication review and approval for matters other than the inclusion of patent or sponsor proprietary/confidential information;
5. Allows the sponsor to claim the results or data generated in the agreement as proprietary or trade secret;
6. Involves export controlled technology;
7. Includes foreign sponsors or collaborators;
8. Travel, shipping, or work outside of the United States;
9. Military applications of project results.

If any export control concerns are identified, the Office of Export Controls is notified. During review, all non-U.S. persons are screened against U.S. and restricted party lists. Export controlled equipment, data, or technology is identified and the appropriate compliance procedures are implemented.

Technology Control Plans (TCP)

Policy

Any UCB research project that involves export controlled equipment or information, or has restrictions on access, requires a Technology Control Plan. The Export Controls Office will work with the

PI to develop and implement a TCP to appropriately secure the equipment, data, or technology from access by unlicensed non-U.S. persons.

Procedure

Technology Control Plans will include:

1. A commitment to export control compliance;
2. Identification of the applicable export controls and items or technologies subject to said controls;
3. A description of the agreed upon security measures to control the item/technology including as appropriate:
 - a. Laboratory compartmentalization
 - b. Time blocking, which is the compartmentalization of lab areas by scheduling blocks of time when restricted or non-restricted work can be conducted
 - c. Appropriate marking for export controls, to include document marking
 - d. Physical security, to include locked storage
 - e. Electronic security, to include online transfer software and email
 - f. Confidential communications;
4. Identification and nationality of each individual who will have access to the controlled item or technology;
5. Personnel screening measures for granting access to the controlled item/technology;
6. Appropriate security measures for disposal of the item/technology when use is complete.

Before any individual may have access to export controlled items or technology, he or she must be informed of the conditions of the TCP and agree to comply with the security measures outlined in the TCP.

Licensing

Policy

The UCB Export Controls Office is responsible for coordinating, drafting, submitting and managing any authorizing license for export controlled activities. The PI must work with the Export Controls Office and the Empowered Official to ensure that the scope of the project is covered in any license. The University's Empowered Official is the individual authorized by the University to apply for licenses or other government authorization. Any UCB personnel who is unsure about licensing requirements for proposed international activities or the use of controlled equipment by foreign

nationals should consult the Export Controls Office prior to engaging in the activity. Once a license is obtained, all provisos, conditions and recordkeeping requirements must be met and maintained.

Procedure

ITAR Licenses

Following an export control analysis of the project, the Export Controls Office advises the PI, University Empowered Official, and the Office of Contracts and Grants that an ITAR license is needed. The Export Controls Office drafts a transmittal letter outlining the scope of the project. This letter is intended to explain the export controlled aspects of the project to the licensing offices of the Department of State. This letter includes (but is not limited to) statement of work, proposed timeline of research, technology to be exported, and projected foreign involvement or collaboration. The Office then reviews the document with the PI to ensure all export controlled portions of the statement of work are included. With authorization from the Empowered Official, the Export Controls Office will submit the appropriate DSP-5 form, transmittal letter, and any other relevant supplemental information to the Department of State's Directorate of Defense Trade Controls (DDTC). Upon DDTC approval, the Export Controls Office will review and advise the PI on the license provisos and will advise on implementation of a TCP and any recordkeeping requirements.

EAR Licenses

Following an export control analysis of the project, the Export Controls Office advises the PI, University Empowered Official, and the Office of Contracts and Grants that an EAR license is required. The Export Controls Office drafts a letter of explanation that describes the scope of the project for the licensing officials of the Department of Commerce. The letter includes (but is not limited to) a statement of work, proposed timeline of project, list of export controlled materials, and foreign national involvement or collaboration. The letter, appropriate BIS 748 form and any additional supplementary information is submitted to the Department of Commerce's Bureau of Industry Security (BIS). Upon BIS approval, the Export Controls Office will review and advise the PI of any license conditions and will advise on the implementation of a TCP and any recordkeeping requirements.

OFAC Licenses

The Department of the Treasury's Office of Foreign Asset Controls is unique in that while most activities with sanctioned countries may require licenses, some activities are authorized under OFAC "general" licenses and do not require prior approval by the United States government. As the name suggests, these general licenses apply to general activities with sanctioned countries. These activities include general travel (not tourism), general education and research activities, and other non-specific

actions. However, any activity outside the scope of the available general license, such as activities that provide a service or any financial transaction, require a more specific license that can take 6 to 12 months to obtain. If the PI anticipates any collaboration or activity with a sanctioned country, he or she will need to work closely with the Export Controls Office to obtain a specific OFAC license.

Training Policy

UCB understands that training is the foundation of a successful export compliance program, and is committed to providing and increasing awareness across the University. The Export Controls Office will prepare up-to-date training materials so that employees or students engaged in export controls receive the appropriate briefing. UCB policy requires export control compliance training for all research staff working on projects requiring an export license or government authorization to export. Such training is highly recommended for all researchers working with potentially export-controlled technology.

Procedure

The Export Controls Office strives to provide up-to-date guidance and training materials. The Office also provides face-to-face training when requested or necessary. The Office also maintains records of training or briefings provided. In addition to in-person training sessions, training on export controls is available online via the University's SkillSoft system. Additional resources addressing special topics are available on the export control web page found at the University's Export Control [website](#).

The Export Liaisons will assist the Export Controls Office in implementing the export control training sessions or briefings relative to their respective schools, departments, centers, or institutes and business units. Export Liaisons will work with senior management as necessary to implement export training to fit the individual department needs.

Recordkeeping Policy

UCB's policy is to maintain export-related records based on controlled items or activities. Unless otherwise provided for or instructed by the Office of the University Counsel, all records shall be maintained consistent with the UCB record retention policy, and shall be retained no less than five years after the TCP termination date or license termination date, whichever is later.

Procedure

If ITAR-controlled technical data are exported under an exemption, certain records of the transaction must be kept beyond UCB's five year retention⁴ period. Those records include:

- a description of the unclassified technical data;
- the name of the recipient /end-user;
- the date / time of export;
- the method of transmission (e.g., e-mail, fax, telephone, FedEx); and
- the exemption under which the export took place.

Note that information which meets the criteria of being in the public domain, being educational information, or resulting from Fundamental Research is not subject to export controls under the ITAR. Therefore, the special requirement for recordkeeping when using an exclusion, exception, or exemption may not apply. However, it is a good practice to provide such description for each export to establish a record of compliance.

BIS has specific record-keeping requirements.⁵ Generally, records required to be kept by EAR must be kept for a period of five years from the last export date. However, if BIS or any other government agency makes a request for such records following a voluntary self-disclosure, the records must be maintained until the agency concerned provides written authorization otherwise.

Monitoring and Reporting Violations

Policy

In order to maintain University of Colorado Boulder's export compliance program and ensure consistent adherence to U.S. export laws, the ECO may conduct internal reviews of Technology Control Plans and certain projects. The purpose of the reviews are to identify possible violations and to identify any deficiencies in training or procedures that can be rectified.

It is the policy of the University of Colorado Boulder to voluntarily self-disclose export control violations as required. Since 11 September 2001, government agencies have dramatically increased the investigation in, and the successful prosecution of, export regulations violations. The penalties for these violations can be severe, including personal liability, monetary fines and imprisonment. However, government agencies assign great weight to voluntary self-disclosures as a mitigating factor. It is

⁴ See 22 C.F.R. §§ 122.5 and 123.26.

⁵ See 15 C.F.R. § 762.6

University policy for any individual who suspects that a violation has occurred to immediately notify the Export Controls Office, the Office of University Counsel and the university's Empowered Official. These violations require disclosure and review by the U.S. Government. All university employees who act in good faith in reporting known or suspected violations of law or university policy are protected from retaliation. However, any UCB employee will be subject to disciplinary action if the employee knowingly fabricated , knowingly distorted, or knowingly exaggerated the report.

Procedure

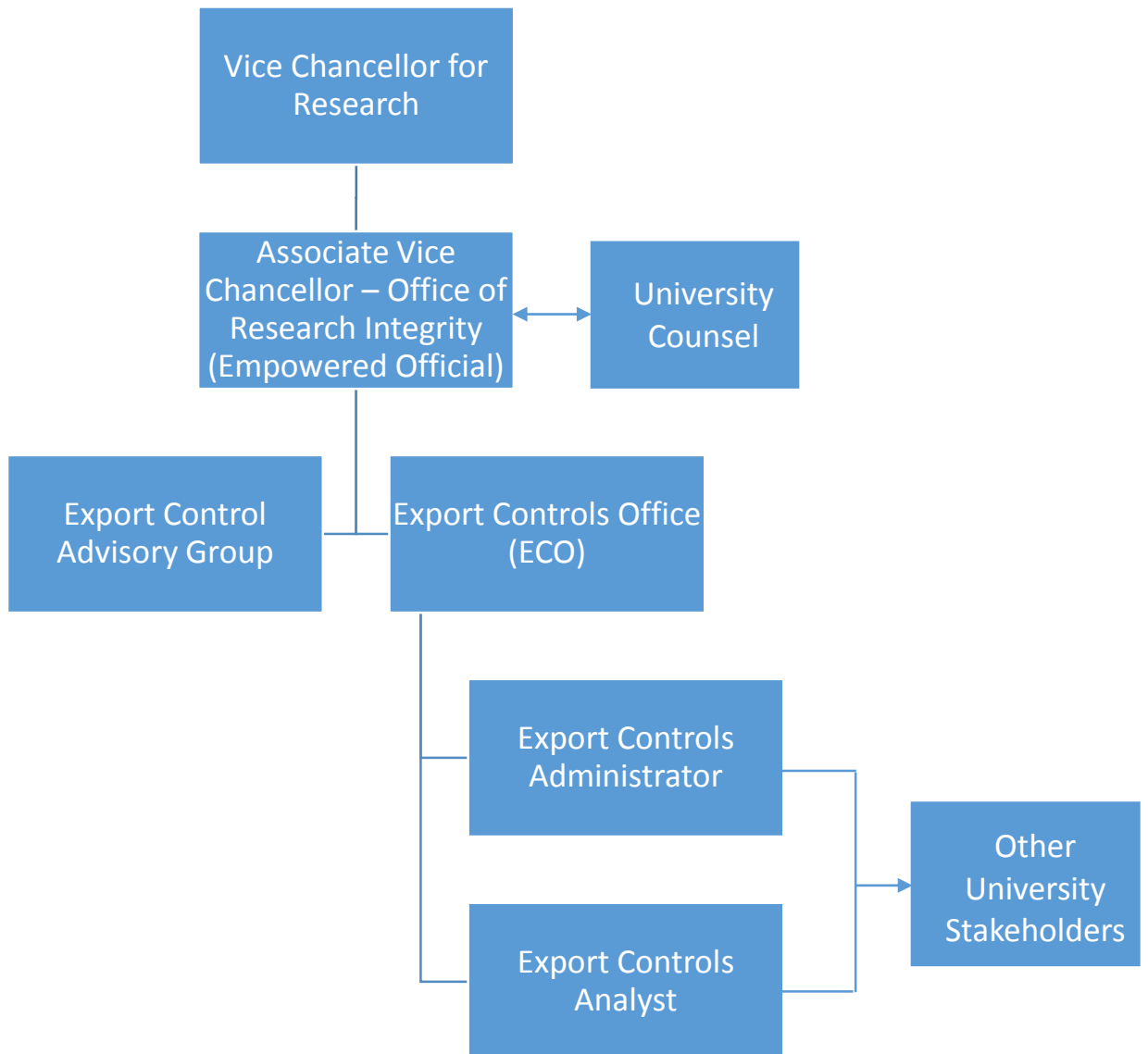
Any individual who suspects a violation has occurred must immediately notify the Export Controls Officer and/or the Office of University Counsel. The Export Controls Office and Empowered Official will work with University Counsel to determine the appropriate follow-up to the notification, which may include a voluntary self-disclosure to the government. The Empowered Official may send an initial notification about the suspected violation to the appropriate government agency.⁶ The Empowered Official, assisted by University Counsel and the Export Controls Office, will conduct an internal review of the suspected violation by gathering information about the circumstances, personnel, items, and communications involved. Once the review is complete, the Empowered Official and Export Controls Officer may provide the government agency with a supplementary letter with a thorough narrative account of:

1. the project's description and background;
2. a description of the suspected violation;
3. which items and controlled categories were involved;
4. which dates the violations occurred on;
5. which countries were involved;
6. who was involved and their citizenships;
7. an explanation of why the alleged violation occurred;
8. any corrective actions taken; and
9. UCB's commitment to export controls compliance.

Once the initial notification and supplementary letter have been sent, UCB will follow the government agency's instructions.

⁶ For EAR violations, see [15 C.F.R. § 764.5](#). For ITAR violations, see [22 C.F.R. § 127.12\(c\)](#).

Appendix 1: University of Colorado Boulder Export Controls Organization Chart



Appendix 2: Export Control Agreement Review Forms

License Review Worksheet

Office of Research Integrity
<http://www.colorado.edu/VCResearch/integrity>

Export License Review Worksheet

Laboratory Collaboration – your Name: _____

Export control regulations prohibit the unlicensed export of specific technologies for reasons of national security or protection of trade. If University research involves such specified technologies, the University may be required to obtain prior approval from the Departments of State, Commerce, or Treasury before allowing a) foreign nationals to participate in the research, b) partnering with a foreign company or c) sharing research information—verbally or in writing—with people who are not U.S. citizens or permanent residents.

However, if you are doing “fundamental research” and the results will be in the public domain (see definitions below), you probably will not have any export control issues unless you have a foreign national working with controlled (found on the Commerce Control List [CCL] or the U.S. Munitions List) proprietary technology in conjunction with your research project.

In order to determine if an export license, Technical Assistance Agreement, or other formal agreement will be required for your activity⁷, please provide the following information. The information will be used to classify your item and or activity to determine what restrictions may apply and to ensure that your collaborators, vendors or end-users are not on any of the denied entities list maintained by the U.S. government.

1. Provide the name of the funding source and title of this research project. Provide a Statement of Work and copy of the agreement (draft form is ok).
2. Will any non-disclosure agreements be signed in furtherance of this research? If so, provide copies or sample copies.
3. Provide names and affiliations of the parties involved in this activity (students, post docs, visiting scholars, collaborating organizations—list key principals from those organizations).
- 3b. Provide CV’s and identify the country of citizenship and visa status for the project personnel.
4. Research results. State what the item is, what it is a component of, what it does, how it works, and any other information that explains the item that will be developed or tested in the course of the research project.
5. State what the item is originally designed for and why the item is being developed. State whether the item is being developed, designed or modified specifically for military use, for commercial use, or both

⁷ “Exports” include both physical exports of commodities, technical data, or software out of the United States as well as disclosure or transfer of technical data to a foreign person, whether in the U.S. or abroad.

military and commercial use. Give examples of the uses for which it is being developed, designed or modified. A brief product history is helpful.

6. Special Characteristics. State any military standards or military specification that the item is designed to meet. Describe any special characteristics of the item e.g., radiation-hardening, thermal or infrared signature reduction capability, and surveillance or intelligence gathering capability. If the item uses image intensification tubes, give the level of technology (Gen II, Gen III, etc.).

7. Provide any other relevant information that would be helpful in making a commodity classification assessment. Include any brochure, specification sheet, marketing literature, technical data, IP disclosures, Patents or any other document that will assist in the determination.

8. In the course of the research activity, what are the item(s) (equipment, software, technology, processes) that will be used or developed to conduct this research?⁸

9. What are the processes involved?

- ❖ Fabrication, i.e., briefly explain
- ❖ What external facilities or vendors are involved?
- ❖ What testing and/or simulation devices are you using?
- ❖ What modeling software are you using? Is this proprietary software?
- ❖ What and whose proprietary designs will you have access to? Who on the project team will have access to this proprietary information?

10. What equipment will be used or purchased in support of the research? Have you factored that into your budget?

11. How will the items (equipment, software, technology, processes) be used by the principles (see item 7 below)?

12. Will any non-U.S. person (1) do ALL SIX of the following activities with respect to the items (equipment)? — operation, installation (including on-site), maintenance, repair, overhaul, *and* refurbishing: OR (2) will s/he have access to its underlying manuals, blueprints, or technology?

13. Is the information to be used or generated in this research publically available OR is it being released to UCB students enrolled in a catalog-listed course or teaching lab?

14. Are the results of the research expected to be published?

15. If applicable, provide a short bibliography of publications related to this technology.

Please send the completed form to Linda Morris in the Office of Research Integrity - Export Controls at Linda.Morris@colorado.edu and Katherine.E.Mills@colorado.edu.

Definitions “Fundamental Research” includes basic or applied research in science and/or engineering at an accredited institution of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community. Fundamental research is distinguished from

⁸ An item can be equipment, commodities, software, and technology.

research that results in information which is restricted either for proprietary reasons or pursuant to specific federal government access and dissemination controls. University research does not qualify as Fundamental Research if: (1) the University accepts any restrictions on the publication of the information resulting from the research, other than limited prepublication reviews by research sponsors to prevent inadvertent divulging of proprietary information provided to the researcher by the sponsor or to insure that publication will not compromise patent rights of the sponsor; or (2) the research is federally-funded and specific access and dissemination controls regarding the resulting information have been accepted by the University or the researcher. The citation for the official definition of “Fundamental Research” under the EAR is 15 CFR § 734.8. The ITAR citation is 22 CFR § 120.11.

“Public Domain” (22 CFR 120.11) means information that is published and that is generally accessible or available to the public: (1) through sales at newsstands and bookstores; (2) through subscriptions that 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 U.S.; (7) through public release (i.e., unlimited distribution) in any form (e.g., not necessarily in published form) after approval by the cognizant U.S. government department or agency; and (8) through fundamental research. The citation for the official definition of “Public Domain” is 22 CFR § 120.11.

University of Colorado at Boulder
Visiting Scholar/Scientist Export Compliance Agreement

The University of Colorado at Boulder (“CU-Boulder” or “University”) is committed to full compliance with all applicable U.S. laws and regulations, including those related to export control. Research and scholarly activities that are subject to U.S. export controls include the physical shipment or transmission of export-controlled items, software, materials or technical data out of the U.S.; certain activities involving defense articles¹ or the provision of defense services²; release of controlled technical data, software or source code to a foreign national or foreign government in the U.S. or abroad; involvement with restricted parties; and any activity involving a sanctioned country. Any activity, including informal discussion, directly related to the development, modification, manufacture, repair, testing, assessment or deployment of military or defense equipment, systems, items, processes, software or code is a defense service and may not be conducted at CU-Boulder without explicit authorization of the CU-Boulder Office of Export Controls.

The University expects and requires all visiting scholars/scientists to abide by U.S. laws and regulations, including those related to export control. In order to prevent inadvertent violation of U.S. export controls, visiting scholars/scientists are not permitted to participate in export controlled, proprietary or confidential research programs without explicit authorization from the CU-Boulder Office of Export Controls. Further, no CU-Boulder employees or students may engage in any activity supporting, formally or informally, such defense services without explicit prior authorization from the CU-Boulder Office of Export Controls.

The University is committed to the free and open exchange of ideas outside of the scope of U.S. export control regulations. Export controls do not apply to the conduct and reporting of basic and applied research, the results of which are typically published and shared broadly within the research community (often referred to as the fundamental research exclusion or exemption, or FRE). However, research results associated with research that does not qualify for the FRE must be protected as export controlled until they are authorized for unlimited public release or dissemination.

Footnotes:

(1) *Defense article* means any item or technical data designated in 22 CFR 121.1 (the U.S. Munitions List or “USML”); this includes most space-qualified hardware. The policy described in 22 CFR 120.3 is applicable to the designation of additional items. This term includes technical data recorded or stored in any physical form, models, mockups or other items that reveal technical data directly relating to items designated on the USML. It does not include basic marketing information on function or purpose or general system descriptions.

(2) *Defense service* means (a) the furnishing of assistance (including training) to foreign persons, whether in the U.S. or abroad in the design, development, engineering, manufacturer, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles; (b) the furnishing to foreign persons of any technical data controlled under 22 CFR 120.10 whether in the U.S. or abroad; or (c) military training of foreign units and forces, regular or irregular, including formal or informal instruction of foreign persons in the U.S. or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercises, and military advice.

Visiting Scholar/Scientist Statement

I have read and understand the information provided on page one of this agreement. I understand that should I have questions related to the U.S. export control regulations at any point during my time at CU-Boulder, they should be directed to the CU-Boulder Office of Export Controls (Linda Morris, 303-492-2889; Linda.Morris@colorado.edu)

By my signature below, I agree that I will not engage in export controlled, proprietary, or confidential work during my tenure at CU-Boulder without explicit authorization from the CU-Boulder Office of Export Controls.

Printed Name

Signature

Date

Sponsoring Faculty Acknowledgement

I have read and understand the information provided on page one of this agreement. I understand that it is my responsibility to instruct the other members of my research or project team as necessary to prevent inadvertent violation of U.S. export control laws and regulations. I understand that should I have any questions related to U.S. export control regulations they should be directed to the CU-Boulder Office of Export Controls.

Printed Name

Signature

Date

Department or School Acknowledgement

Printed Name

Title

Signature

Date

Export Control Checklist for Issues Involved in Sponsored Research

EXPORT CONTROL CHECKLIST

Use this checklist to assist in determining whether or not Export Control regulations apply to your project.

Does this project or agreement:	YES	NO
Restrict researcher participation (faculty, student, others) based on country of origin or citizenship?		
Require research participation in US-citizen-only meetings?		
Grant the sponsor a right of prepublication review for matters other than the inclusion of patent and/or proprietary sponsor information?		
Provide that any part of the sponsoring, granting, or establishing documents may not be disclosed?		
Limit access to confidential data and involve a controlled technology (see below)?		
Involve research containing source code for encrypted software (other than publicly available software distributed at no charge)?		
Involve research, information or software that could be used in the development of weapons of mass destruction (nuclear, biological, chemical), or their delivery systems?		
Involve equipment, software, services or technology that is on the United States Munitions List ("USML") under the International Traffic in Arms Regulations ("ITAR"; see http://pmdtc.org/)?		
Involve equipment, software, services or technology that is on the Commerce Control List ("CCL") under the Export Administration Regulations ("EAR"; see http://www.access.gpo.gov/bis/)?		
Involve technical information or instructions concerning equipment, software or technology on the USML or the CCL?		
Provide data, services or conduct any transaction with an embargoed country as defined by the Office of Foreign Assets Control ("OFAC"; see http://www.treas.gov/offices/enforcement/ofac/)?		

If the answer to any of these questions is “yes,” or if you have any other questions related to export controls, please contact Linda Morris, Export Control Administrator, at linda.morris@colorado.edu or Katherine Mills, Export Control Analyst at katherine.e.mills@colorado.edu

If accepting proprietary information as part of a project:	YES	NO
Is the information clearly identified?		
Can the information be appropriately protected?		
Can proprietary information be removed from research results, so that results may be freely published?		

If the answer to any of these questions is “no,” please contact the Export Controls Office at the contact information listed above.

Appendix 3: Technology Control Plan Template

ITAR Project Technology Control Plan

PIs:

Program:

Materials:

Date:

Personnel

1. The PI (_____) is responsible for identifying all persons who may have access to the ITAR/EAR restricted documentation and software, and that such controlled technical data will not be further disclosed, exported, or transferred in any manner not authorized under ITAR except with the prior written approval of the U.S. Department of State.
2. AES I9 Partner, Patti Gassaway or CU Human Resources is responsible for confirming the citizenship status of each individual granted access to the materials by the PI(s) above.

Training

3. Each participant is required to complete the University of Colorado online export control training.
4. Each participant is required to attend a 30-minute workshop offered by the Office of Research Integrity Export Control (short, as a follow up to any questions arising out of the online training)

*Individuals successfully completing the steps above are considered **approved personnel**. Individuals may not receive restricted data or hardware until they are approved.*

Facilities

5. An AES approved ITAR designated room is used for storage of all ITAR controlled physical materials (hardware, software, files, printed documentation).
6. The ITAR room is clearly marked on the exterior door (ITAR/EAR Restricted Area – U.S. Persons only) and this approved technology control plan is posted clearly inside the room.
7. The ITAR room is access controlled. The access process (room key or card) is managed by the AES department and all access requests are made in writing by the project PI. Only approved personnel will be granted access.
8. Regular custodial, recycling and maintenance services are **NOT** to be provided in the ITAR room and facilities management is given instructions that staff are not to access the room unaccompanied. Project personnel are responsible for cleaning and/or escorting staff as visitors (as described below) for occasional cleaning and maintenance services.
9. The ITAR room must have a shredder or disposal container for export controlled printed matter.

Marking Documents and Hardware

10. All ITAR restricted documents and hardware are to be clearly marked with *“This document contains Technical Data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.). Violations of these export laws are subject to severe criminal penalties.”*

Visitor and Guest Access

11. All parties entering the access-controlled room who are not approved personnel must sign in and be accompanied by an approved person. It is recommended that all visitors be approved by the PI prior to entering the facility. Foreign persons will not be allowed to enter the access-controlled room unless all ITAR controlled materials are secured in a locked cabinet or covered.
12. Sign in sheets must include the name of the guest/visitor, a confirmation of all parties' citizenship, a record of the responsible approved person chaperoning the visit, as well as the date of the visit.

Computer Access and Electronic Data

13. All computers that store ITAR materials must meet the minimum campus security standards (<http://www.colorado.edu/avcit/sites/default/files/attached-files/minimum-security.pdf>). The campus minimum security standards require that the operating system is currently supported and patched, the computer is password protected and runs current virus protection software when available for the operating system, and host-based firewall is enabled to block inbound traffic. The OIT Security Office will validate the security of systems storing ITAR data annually. A security review can typically be conducted within one business day.
14. A secure ITAR designated system is used as the primary storage for all ITAR materials. The AES IT manager is responsible for ensuring that the system is secure. The OIT Security Office (security@colorado.edu or 303.735.6637) shall be notified of the IP address and name of any ITAR designated system. OIT will arrange additional monitoring for the server.
15. Storage and backup of the ITAR system data is maintained in a secure facility on campus or stored on a password protected device that is clearly marked. No open remote storage of such documents is permitted (i.e. Dropbox or Google drive)
16. It is required that all ITAR data and documents be password protected. Supported data protection methods include PGP (for Windows and Mac) and TrueCrypt (for Linux). If it is not feasible to use PGP or Truecrypt, Microsoft Excel and Word 2010 or later may be used if the machine is physically secured and the password is not stored in publically accessible location.
17. Access to CU computers used for projects with ITAR material is controlled by the AES IT manager. Only approved personnel will be granted access.
18. Remote access to these computers must use a secure connection (VPN, SSH or similar).
19. Remotely working on ITAR restricted materials in public locations (eg. coffee shops, airports, computer labs, etc.) is forbidden because the citizenship of onlookers cannot be verified.
20. Transfer of ITAR restricted materials to remote storage like Dropbox or Google Drive is forbidden.
21. Transfer of ITAR controlled materials to a laptop, personal computer, or portable drive (USB drive) by students is highly discouraged. Where necessary, the transfer of ITAR data to such devices by students must be clearly justified, approved by the PI and will only be granted for a specific period of time.

22. Electronic transfer of ITAR data and documents to the sponsor or approved project personnel shall use the campus file transfer service (filetransfer.colorado.edu) or a sponsor preferred system of delivery. All files and communication must include a statement notifying the recipient that the data is ITAR controlled. The Office of Research Integrity and Regulatory Compliance will provide the necessary language. A record / log of each transfer of technical data and date of transfer will be maintained.

Travel

23. Computers containing ITAR/EAR data cannot leave the United States without prior approval of the University of Colorado Export Controls Office. It may be necessary to obtain an export license for such cases, which can take 90 days or more.
24. Project participants travelling outside the United States with a laptop which may contain export controlled materials are required to receive additional training. The University of Colorado Export Controls Office must be contacted 90 days in advance of any anticipated international travel.

This TCP does not cover any materials classified higher than "sensitive but unclassified".

Read and acknowledged by:

[PI] Date

[Co-Investigator] Date

[Co-Investigator] Date

Appendix 4: Glossary and Abbreviations

Glossary

Commerce Control List (CCL): The CCL identifies specific item subject to the list-based controls of the Export Administration Regulations, under the export control jurisdiction of the Bureau of Industry and Security in the United States Department of Commerce (10 CFR §774)

Deemed Export: Release of technology or source code subject to the EAR to a foreign national in the United States is considered or “deemed” an export to the home country of the foreign national. The ITAR considers any transfer or disclosure of technical data to a foreign national (in the United States or abroad) to be an export.

Defense Article: In the ITAR, a defense article means any item or technical data designated on the United States Munitions List (USML). The term includes technical data recorded or stored in any physical form, models, mockups or other items that reveal technical data directly relating to items designated on the USML. It does not include basic marketing information on function or purpose or general system descriptions. A defense article includes a wide array of objects, and is not limited to traditional “weapon” or “military” items.

Defense Service: In the ITAR, a defense service means the furnishing of assistance (including training) to foreign persons, whether in the United States or abroad, in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing, or use of a defense article. The term also includes the furnishing to foreign persons of any technical data controlled under the ITAR, in either the United States or abroad. Finally, defense services include military training of foreign units and forces, regular or irregular, including formal or informal instruction of a foreign person in the United States or abroad by either correspondence course, technical, educational, or information publications and media of all kinds.

End-use, End-user: The EAR controls the export of all items subject to the EAR if they will be received by certain entities or used for certain purposes. Many EAR licenses and exemptions require certified “end use” statements from the receiver of the EAR data or hardware.

Export Control Classification Number (ECCN): A five-character alphanumeric classification used under the EAR to identify items on the Commerce Control List.

Foreign Person: The regulations define foreign person as anyone who is not a U.S. person. The EAR bases this on person's most recent citizenship or permanent residence. The ITAR bases this on the person's country of origin (i.e., country of birth) and all current citizenships.

International Traffic In Arms Regulations (ITAR): The ITAR (22 CFR §120 – 130), under the jurisdiction of the United States Department of State, controls the export of articles, services, and related technical data whose most predominant application is that of defense. The defense articles, services, and technical data are listed on the United States Munitions List (USML).

Office of Foreign Assets Control (OFAC): An office within the United States Department of Treasury that administers and enforces economic embargoes and trade sanctions based on US foreign policy and national security goals.

Reexport: An actual shipment or transmission of an item subject to the EAR from one foreign country to another. Reexports of EAR controlled items typically require a license or other form of government authorization

Restricted Parties: Individuals or entities with whom the university and its employees are prohibited by law, or require a license, to engage in export controlled activities. Lists include Denied Parties List (OFAC), Debarred Parties List (ITAR) and Denied Persons List and Denied Entities List (EAR).

Restricted Research: University research, development, or testing subject to: publication restrictions, access or dissemination controls, or contract-specific national security restrictions (usually federally-funded). Restricted research projects are subject to approval by the University of Colorado Boulder's [Restricted Research committee](#) and may be subject to EAR and ITAR controls.

Sanctioned and Embargoed Countries: Countries designated by OFAC, ITAR, and EAR as having limited or comprehensive trade and arms sanctions imposed by the United States for reasons of anti-terrorism, non-proliferation, drug and human trafficking, human rights violations, and other reasons.

Technical Data: Refers to information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of controlled articles. This information can be in the form of blueprints, instructions, diagrams, photographs, etc.

Technology: In the EAR, technology is specific information necessary for the development, production, or use of a product.

United States Munitions List (USML): The USML includes articles, services, and related technical data designated as defense articles and services pursuant to the ITAR.

US Person: For purposes of defense and dual-use exports, a U.S. person is defined as a U.S. entity or a U.S. citizen, or a person lawfully admitted for permanent residence in the United States (i.e., green card holder) A U.S. person may be engaged in activities that are export controlled, unless there are some additional restrictions that limit participation to U.S. citizens.

Abbreviations

AECA	Arms Export Control Act
AES	Automated Export System
BIS	Department of Commerce Bureau of Industry and Security
CCL	Commerce Control List
CFR	Code of Federal Regulations
CJ	Commodity Jurisdiction
DDTC	Department of State Directorate of Defense Trade Controls
EAR	Export Administration Regulations

ECCN	Export Control Classification Number
EO	Empowered Official
ECO	Export Controls Office
ITAR	International Traffic in Arms Regulations
OFAC	Department of the Treasury Office of Foreign Assets Control
OCG	Office of Contracts and Grants / Sponsored Programs
ORI	Office of Research Integrity
PI	Principal Investigator
SDN List	Specially Designated Nationals and Blocked Persons List
TAA	Technical Assistance Agreement
TCP	Technology Control Plan
UCB	The University of Colorado at Boulder
USML	United States Munitions List
VPN	Virtual Private Network