Revision Table	
Date: 5/18/2022	By: Tina Bosworth
Date: 6/21/2022	By: Tina Bosworth
Date: 10/4/2022	By: Tina Bosworth
Date: 1/9/2023	By: Tina Bosworth

Table of Contents

Introduction

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). While the discussion below focuses on these three agencies, it is important to remember that meeting the export requirements of one of these agencies alone is not sufficient, and the applicability of all these regulations to a specific activity should be evaluated to ensure full compliance with the U.S. export control regulations.

In August 2009, President Barack Obama directed an interagency review of the U.S. export control system and its ability to protect national security and enhance U.S. economic competitiveness. This review concluded that the export control system was overly complicated, overly broad, and with too many redundancies. As a result, in August 2010, the Export Control Reform initiative was launched. In 2018, the Export Control Reform Act was introduced in House (02/15/2018) to authorize the President to control the export, re-export, and transfer of commodities, software, and technology to protect the national security, and to promote the foreign policy, of the United States, and for other purposes. As this initiative moves forward, the regulatory environment for export controls in the U.S. is in a state of flux. Thus, it is important to check the current regulations before engaging in any export controlled activities.

Acknowledgements

Thank you to the following universities for sharing their content, which has been adapted within this Export Compliance Manual, forms, guidance, and website content: The University of Miami, University of Central Florida, the University of Delaware, Caltech, and the University of Pennsylvania, and the additional guidance provided by the Association of University Export Control Officers (AUECO).

Export Control Laws at the University of Cincinnati (UC)

The export control laws apply to research and many other activities at UC. Such as international travel, shipments, conversations, payments, and publications (list not inclusive). There are many instances where export controls would apply to activities at UC. One example is travel to Iran to attend a medical conference, which requires a license. Another example is the attempt to apply the Fundamental Research Exclusion (FRE)[1] to equipment; FRE does not apply to physical items or shipments. Additional examples include student organizations traveling to Cuba[2], having a CubeSat project that involves foreign students or faculty importing items that are controlled and being held at U.S. Customs for proper paperwork and classification, and faculty collaborating with foreign institutions on publications that may contain sensitive information.

Universities in the U.S., including UC, have a long tradition of inventing and developing leading edge technologies that are important for national security and economic competitiveness as well as for educating 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 universities in the U.S. are excluded from the regulations. As a result, most research activities at UC are "fundamental research" as defined in the export control laws, which do not require a "license "or permission from the government. The University of Cincinnati has multiple Board Rules that are potentially relevant to export control restrictions[3]. Nonetheless, it is important to understand the limits on fundamental research in the context of the applicable export control regulations.

The U.S. export control agencies place the burden of understanding and complying with the regulations on the university,[4]although there is also personal liability. Even though most research conducted on campus will not be subject to export control restrictions[5], it is important for the university community to be aware of when activities potentially become controlled. Many universities accept restrictions on publication and participation in sponsored research, which can render the work and associated information and products under the export control regulations. It is incumbent upon UC researchers to verify what, if any, information is export controlled in the conduct of research, to get proper authorization to conduct such research, and to put appropriate safeguards in place. The export control regulations apply to the export (even temporary) of controlled university owned equipment, to the shipment of research materials or equipment to locations outside of the U.S., and to the sharing of controlled information with people who are not U.S. citizens or permanent residents.

The following brief descriptions of the export control laws are meant to be only an overview of the regulations as they impact activities at UC. The information should be used with caution, the UC

[1] See Appendix ZD

[2] See Appendix ZE

[3] *See* Appendix Y: "Board Rules: 10-30-02- 04" and "Draft Board Rule"

[4] 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

[5] See National Security Decision Directive 189 available at https://fas.org/irp/offdocs/nsdd/nsdd-189.htm

community is encouraged to consult with the Export Controls Office when contemplating activities that may be impacted by the export control regulations.

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 that commodity has an inherently military purpose. Thus, an autopilot system used in basic robotics research at UC may be controlled under the ITAR.

Many items designed for military use are also used for research completely unrelated to that military use. One example is use of Infrared (IR) Cameras in engineering and physics labs for research. Depending on which model of IR Camera, it may be ITAR controlled even though it is not being used in a military activity.

Important ITAR Definitions

Export in the ITAR includes the passing of information or technology to foreign nationals even in the United States. The following are examples of exports:

1. Exports of articles from the U.S. territory

    • Shipping or taking a defense article out of the United States.

    • Transferring title or ownership of a defense article to a foreign person (described as any person who is not a lawful permanent resident of the United States, also an agent working on behalf of a foreign company not incorporated in the US is considered a "foreign person(s)"), in or outside the United States.

2. Extra-territorial transfers

    • The re-export or re-transfer of defense articles from one foreign person to another, not previously authorized (i.e., transferring an article that has been exported to a foreign country from that country to a third country).

    • Transferring the registration, control, or ownership to a foreign person of any aircraft, vessel, or satellite covered by the USML, whether the transfer occurs in the United States or abroad.

3. Export of intangibles

    • Disclosing technical data to a foreign person, whether in the United States or abroad, through oral, visual, or other means.

    • Performing a defense service for a foreign person, whether in the United States or abroad.

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 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.

Fundamental Research Exclusion (FRE) is 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 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. (22 C.F.R. § 120.11).

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 in addition to libraries, subscriptions, newsstands, and bookstores, include published patents and public release at conferences, meetings, and trade shows ***in*** the U.S. where those venues are generally accessible to the public.

USML Categories

The USML is enumerated in 22 CFR Part 121 and specifies twenty-one (21) "Categories" of defense articles, with sub-itemization of "Significant Military Equipment" (SME) articles. SME is defined in 22 CFR § 120.7 as "articles for which special export controls are warranted because of their capacity for

substantial military use or capability. An electronic version of the USML is available on the Department of State website at:

https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-121

The twenty-one categories found on the USML are as follows:

Category I: Firearms, Close Assault Weapons and Combat Shotguns

Category II: Guns and Armament

Category III: Ammunition / Ordinance

Category IV: Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs and Mines

Category V: Explosives and Energetic Materials, Propellants, Incendiary Agents and Their Constituents

Category VI: Surface Vessels of War and Special Naval Equipment

Category VII: Ground Vehicles

Category VIII: Aircraft and Related Articles

Category IX: Military Training Equipment and Training Category X: Protective Personnel Equipment and Shelters Category XI: Military Electronics

Category XII: Fire Control, Range Finder, Optical and Guidance and Control Equipment

Category XIII: Materials and Miscellaneous Articles

Category XIV: Toxicological Agents, Including Chemical Agents, Biological Agents, and associated Equipment

Category XV: Spacecraft Systems and Associated Equipment

Category XVI: Nuclear Weapons, Design and Testing Related Items

Category XVII: Classified Articles, Technical Data and Defense Services Not Otherwise Enumerated

Category XVIII: Direct Energy Weapons

Category XIX: Gas Turbine Engines and Associated Equipment

Category XX: Submersible Vessels and Related Articles

Category XXI: Articles, Technical Data and Defense Services Not Otherwise Enumerated

Commodity Jurisdiction (CJ)

CJ is the process of determining if an item, article, service, or technical data is on the USML and subject to the requirements of the ITAR**.** Designations of defense articles and defense services are made by the Department of State with the concurrence of the Department of Defense.

Proper CJ determination is essential to avoid violations. The ITAR only regulates items, defense articles, services and associated technical data of items specifically identified on the USML as opposed to other U.S. export regulations; however, other agencies regulate items that are not on the USML.

The first step for CJ is to self-classify items, articles, or services to determine if they are listed on the USML, or if they meet the qualifications of being considered "specially designed." "Specially designed" describes an item or service that meets the criteria of a defense article or defense service or provides the equivalent performance capabilities of a defense article on the USML. If an article is not on the USML, or if it is not "specially designed" it may still be export controlled but does not fall under the ITAR. The DDTC has a web-based interactive "Order of Review Decision Tool" to assist with this process:

https://www.pmddtc.state.gov/ddtc_public%3Fid=ddtc_public_portal_faq_detail&sys_id=8a8b2d9cdb3d5b4044f9ff621f961993?id=ddtc_public_portal_faq_detail&sys_id=1e8b2d9cdb3d5b4044f9ff621f9619ab

The effort to determine whether an activity or item is subject to the ITAR, i.e., on the USML, is known as a "Jurisdictional Analysis", other reviews are described, below.

The Jurisdictional Analysis process begins by reviewing the general characteristics of the item, technology, or proposed defense service. The general characteristics must fall within the proscribed requirements of "specially designed" to be subject to the ITAR. Commodities and software are "specially designed" if:

> (1) As a result of development, has properties peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions described in the relevant USML paragraph; or
>
> (2) Is a part (see § 121.8(d) of this subchapter), component (see § 121.8(b) of this subchapter), accessory (see § 121.8(c) of this subchapter), attachment (see § 121.8(c) of this subchapter), or software for use in or with a defense article.
>
> (b) A part, component, accessory, attachment, or software is not controlled by a USML ''catch-all'' or technical data control paragraph if it:
>
> (1) Is subject to the Department of Commerce Export Administration Regulations pursuant to a commodity jurisdiction determination.

(2) Is, regardless of form or fit, a fastener (e.g., screws, bolts, nuts, nut plates, studs, inserts, clips, rivets, pins), washer, spacer, insulator, grommet, bushing, spring, wire, or solder.

(3) Has the same function, performance capabilities, and the same or ‘‘equivalent’’ form and fit as a commodity or software used in or with a commodity that:

(i) Is or was in production (i.e., not in development); and

(ii) Is not enumerated on the U.S. Munitions List.

(4) Was or is being developed with knowledge that it is or would be for use in or with both defense articles enumerated on the U.S. Munitions List and also commodities not on the USML; or

(5) Was or is being developed as a general purpose commodity or software

If the technology meets the definitional requirements of qualifying as “specially designed” and is identified within a USML Category, the characteristics and functions of an article can be matched to a specific entry found on the USML.

Both the Departments of Commerce and State prefer for organizations to attempt to self-classify whenever possible; however, if a jurisdictional determination cannot be made, the U.S. Government will provide a definitive written determination in response to the submission of a “Commodity Jurisdiction Request.” The Export Controls Office (ECO) will work with researchers to review CJs and to submit Commodity Jurisdiction Requests when needed.

Requirements for ITAR Export Authorization

Any person or entity in the U.S. who engages in the business of manufacturing or exporting or temporarily importing defense articles or furnishing defense services is required to register with the Department of State. Registration is a mandatory prerequisite to process license applications or invoke other approvals for an activity regulated by the ITAR or invoke the use of an exemption to the license requirement. Once registered, licenses to export defense articles or perform defense services can be processed. License applications must go through the Export Controls Office (ECO). Certain licenses or exemptions or other government approvals are required to employ or allow foreign persons to participate in activities subject to export requirements (see “deemed exports”). License applications or other government approvals and exemptions contain additional certifications, transmittal letters, supporting documentation, and in some cases, non-transfer and use certification from the licensee and / or the foreign government of the licensee, end-user certifications. These documents are processed by the ECO.

University research is subject to the ITAR when the research involves defense articles or technical data. Activities that involve defense articles or export-controlled technical data that involve foreign persons require a license or other government approval before the foreign person is permitted access to the articles or data. Instruction or methods involved in the ITAR-controlled research constitute the

provisioning of “defense services”, which is also a licensable activity. A “defense service” is equivalent to a “deemed export” under the Department of Commerce regulations.

Proscribed Countries
Pursuant to U.S. policy related to arms embargoes, no ITAR exports, license requests, exemptions and other government approvals for export may be made to countries proscribed in 22 C.F.R. § 126.1, such as China, Cuba, Iran, North Korea, Sudan, and Syria. Additional restrictions apply to other countries; a complete list of U.S. arms embargoes is available online at:

https://www.state.gov/economic-sanctions-programs/

At UC, the Export Controls Office will submit commodity jurisdiction requests and determine any export licensing requirements.

Department of Commerce’ Export Administration Regulations (EAR)

Regulatory Authority and Scope
The EAR controls the export of “dual use” items, which are items that have civilian uses, but may also have military or other strategic applications. Examples include certain chemicals, microorganisms, some laboratory equipment (e.g., centrifuges, chromatographs, fabrication equipment, and etching equipment for electronics). 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. The EAR also controls the export of purely commercial commodities in support of U.S. trade and embargo policies. Purely commercial items are classified as EAR99 and have very few export restrictions. The current export reform initiative will also move some less sensitive military items from the ITAR to the EAR.

Many activities are not subject to the EAR. These include 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 also lists several exclusions from the regulations including published information, information resulting from fundamental research, educational information, and the export or re-export of items with less than *de minimis* U.S. content (where applicable; see definition, below). It is important to understand the definitions and limitations of each of these exclusions when making determinations.

Important EAR Definitions and Concepts
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.

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. It also includes the release of technology or software subject to the EAR to a foreign country or to a foreign national either in the U.S. or abroad.

Re-export 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 re-export**). Re-export 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 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. Publications may take the form of periodicals, books, print, electronic, 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, if the price charged for the publication does not exceed the cost of reproduction and distribution. Articles submitted to journals for consideration for publication are 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. 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.*

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. Educational information is not subject to the EAR, even if the faculty member is teaching the class at an institution outside the U.S.

The Commerce Control List (CCL)

The CCL is found at 15 C.F.R. § 774, which may be accessed at: https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-774

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. 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 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.

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. 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 UC community who need assistance with classifying items should contact the Export Controls Office.

License Exceptions
While the CCL is much more extensive than the USML, given the available license exceptions fewer licenses are required for items controlled under the EAR than under the ITAR. There are limitations on the use of license exceptions (see 15 C.F.R. § 740.2), and the use of a license exception may have associated recordkeeping and notification requirements. If more than one license exception is available for a proposed activity, then use of the exception with the fewest restrictions minimizes compliance burden. Members of the UC community shall consult with the Export Controls 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 UC community travelling abroad are BAG (BAGGAGE), which applies to personally-owned items taken abroad for personal use while abroad, and TMP (Temporary imports, exports, re-exports, and in-country transfers), which applies to the temporary export of UC-owned equipment, including laptop computers and other equipment listed on the CCL, for work-related activities, including professional presentations, teaching, and research. 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.

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. Such companies are "blacklisted" under the 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. For example, UC 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 refusing 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.** If you encounter boycott language, promptly contact the Export Controls Office for assistance in determining whether an exception is applicable and if reporting to BIS is required.

Department of Treasury Regulations (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. 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 regulations are in31 C.F.R. §§ 500-599.

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 or engaging in business activities with SDNs. Currently OFAC sanctioned countries include the **Balkans, Belarus, Burma, 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**; this list could change. 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.

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 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. At UC, the Export Controls Office must be contacted when considering any proposed OFAC sanctioned activities.

Exemptions of General Applicability
As a general policy, UC will utilize exemptions only on a very limited basis. Use of exemptions must be documented. Classified transmissions, and offshore procurement arrangements (e.g., international collaborations) are not permitted.

Eligibility to use exemptions is conditional upon UC's continued registration with DDTC. Exemptions cannot be used to allow export, including the provisioning of defense services, to any foreign person who is a citizen of, or was born in, a Proscribed Destination:

https://www.govinfo.gov/app/details/CFR-2002-title22-vol1/CFR-2002-title22-vol1-sec125-4/summary

The applicability and use of all ITAR exemptions will only be made by the Empowered Official(s) or their designee. Use of exemptions must comply with all requirements specified in the ITAR, to include Sections 125.4.

22 CFR 125.4(b)(10) Exemption for Full-time Bona Fide Employees of U.S. Institutions of Higher Learning for Disclosures of Unclassified Technical Data

(10) Disclosures of unclassified technical data in the U.S. by U.S. institutions of higher learning to foreign persons who are their bona fide and full time regular employees. This exemption is available only if:

(i) The employee's permanent abode throughout the period of employment is in the United States.

(ii) The employee is not a national of a country to which exports are prohibited pursuant to § 126.1 of these subchapters; and

(iii) The institution informs the individual in writing that the technical data may not be transferred to other foreign persons without the prior written approval of the Directorate of Defense Trade Controls

Applicability of Exemption:

UC will only use the bona fide employee exemption under very specific conditions.

- This exemption is only available for university employees
- This exemption is not available for any of the following:
  - Students, including Graduate Research Assistants and Graduate Teaching Assistants,
  - Volunteers,
  - Part-time employees,
  - Other employees not receiving benefits, as these are not "regular" employees,
  - Appointed faculty that are not being paid, or
  - Any foreign person on a F-1 or J-1 visa, regardless of tax withholdings
- This exemption is specific to release/disclosure of unclassified technical data. It does not allow the transfer of defense services. Defense services require a separate license.
- The exemption does not allow for access to tangible defense articles.
- Supervisors of employees utilizing this exemption must be informed of the use. If necessary, the supervisor may be a signatory on the exemption certificate.

Use of Other ITAR Exemptions
The ITAR employs various other exemptions to the licensing requirements. Final determination with respect to the applicability of these exemptions must be made on a case-by case basis by the Empowered Official(s) or their designee.

Use of EAR Exceptions
The most common EAR exception used is the "Tool of Trade" exception, which is used for international travel or transmissions to destinations outside the U.S. of commodities required to conduct routine business, such as a laptop, certain software, cellphone, etc.

The exception requires:
- The destination cannot be to a sanctioned country (Cuba, Iran, Sudan, Syria, North Korea),
- Use of the "Tool of Trade" exception must be documented on a certificate,
- Equipment and data cannot be on the USML (e.g., DoD Sponsored project articles or data not in the public domain),
- Equipment and data must be in the "effective control" of the traveler for the duration of the trip and cannot be released, and
- Equipment and data cannot be out of the U.S. for longer than 12 months.

Equipment not Qualifying:
- Agents, toxins, microorganisms, pathogens, chemicals, or nuclear technologies,
- High end GPS units,
- Defense articles listed on the ITAR U.S. Munitions List (USML), and
- Non-standard cryptography technology and software, (non-mass market software), "open cryptographic interface" technology or "cryptanalytic (code-breaking)" technology

Data
Safeguard data and credentials while on travel[6]. Remove the following types of data from a laptop before departure as they do not qualify for the "Tool of Trade" exception:

- Proprietary technical data not intended for public distribution, such as sponsored research with access, publication, or participation restrictions,
- Technical data relating to the development, production, or use[7] of a commodity listed on the CCL, and
- Data relating to any military sponsored project or defense articles on the USML.

[6] See Appendix S, T, U
[7] See Appendix ZC

International Travel with Non-University Equipment
License Exception BAG allows US citizens to carry family-owned retail-level items including laptops, personal digital assistants (PDAs), and cell phones as personal baggage. The items and software must be for their personal use.

Record Retention Requirements
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.

Shipment of items controlled under the ITAR, or EAR should be clearly marked as controlled with the appropriate regulatory control cited. Any licensed export, 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 assists the UC community for the export of items being hand-carried or technical data being mailed or electronically transmitted. See Recordkeeping

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).

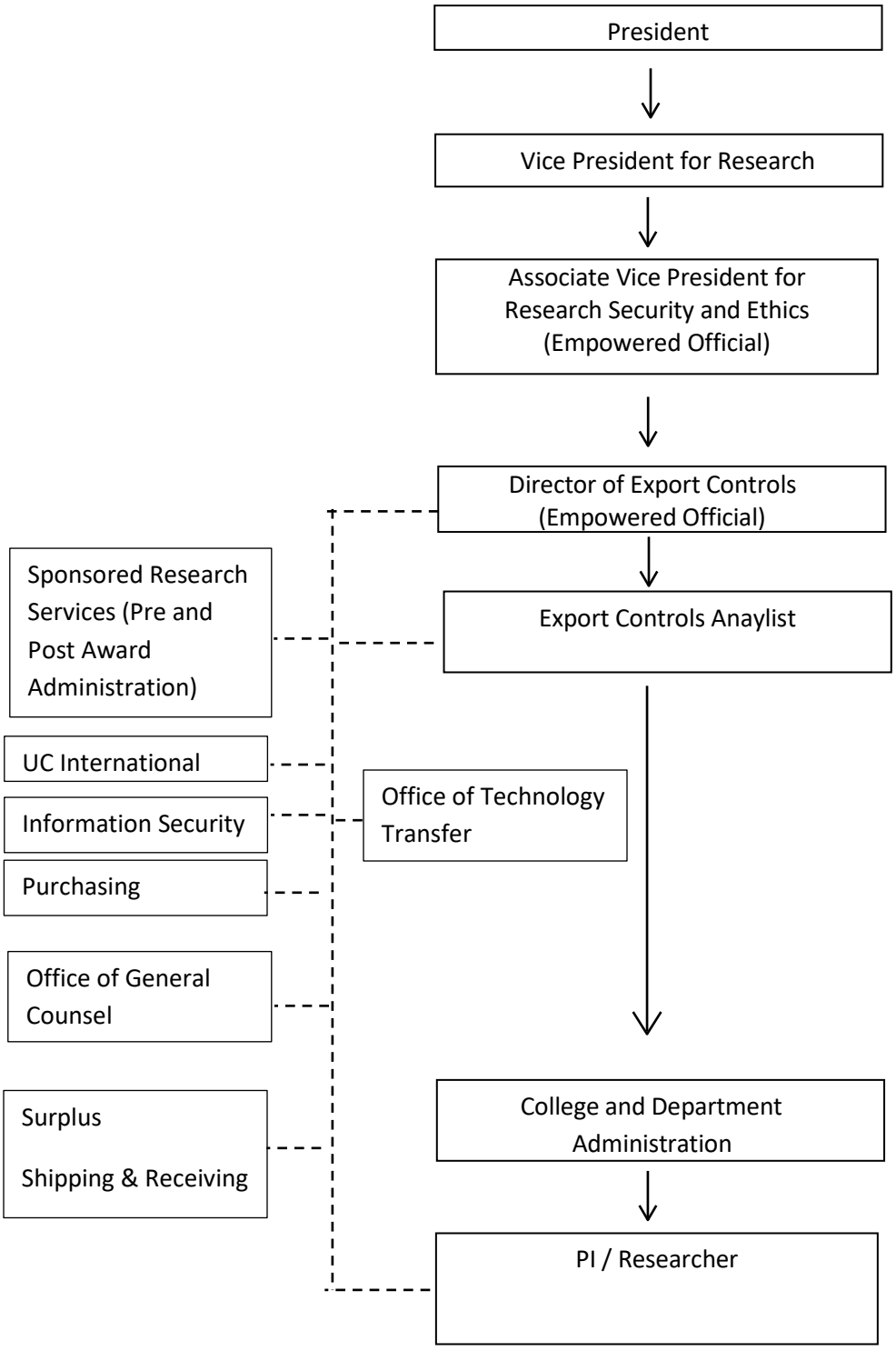
In assessing penalties, DDTC, BIS, and OFAC will consider mitigating factors. Mitigating factors include whether the disclosure of the violation was made voluntarily, whether the violation is an isolated incident or part of a pattern of continuing behavior, whether the company had a compliance program 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 inadvertence, mistake of fact, or a good faith misinterpretation of the laws. See Detecting and Reporting Violations

Commitment to Export Control Compliance

The University of Cincinnati must comply with all applicable U.S. Government export regulations. Most of the teaching and research activity at UC falls within one or more of several exemptions and exclusions from licensing requirements. However, it is important to understand how the laws apply and the corresponding compliance obligations.

The University of Cincinnati Export Controls Office (ECO) is responsible for helping the university community understand and comply with the export control laws, and for export license applications when necessary. Please see http://researchcompliance.uc.edu/exportControls/exportControls.aspx for additional information including guidance 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. Questions regarding export control laws or procedures for compliance please contact exportco@uc.edu.

UC Functional Organizational Chart for Export Controls



Roles and Responsibilities for Export Controls at UC

The Roles and Responsibilities for ensuring compliance with export control laws at UC are described below. While it is the responsibility of senior university management and 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 discussion below focuses on other key actors in export compliance at UC.

Empowered Officials

The Associate Vice President for the Office of Research Security and Ethics and the Export Controls Director are the University of Cincinnati's Empowered Officials. In this capacity, the Empowered Officials have 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 export control responsibilities.

The President designated the following university officers as Empowered Officials pursuant to 22 CFR 120.25:

- Dr. Holly Bante, Associate Vice President for Research Security and Ethics
- Tina Bosworth, Director, Export Controls, Empowered Official

In this capacity, designated Empowered Officials:

(1) Are directly employed by UC in a position having authority for policy or management; and

(2) Are legally empowered in writing by the applicant to sign license applications or other requests for approval on behalf of UC with the U.S. State Department; and

(3) Understand the provisions and requirements of the various export control statutes and regulations, and the criminal liability, civil liability, and administrative penalties for violating the Arms Export Control Act and the International Traffic in Arms Regulations; and

(4) Have the independent authority to:
- (i) Enquire into any aspect of a proposed export or temporary import by UC, and
- (ii) Verify the legality of the transaction and the accuracy of the information to be submitted; and
- (iii) Refuse to sign any license application or other request for approval without prejudice or other adverse recourse.

Export Controls Office

The functional administrative unit at the UC charged with the responsibility for oversight of compliance and recordkeeping of all applicable exports and regulated transactions with sanctioned individuals, entities, and countries is the Export Controls Office, under the Office of Research Security and Ethics within the Office of Research.

The Export Controls Office is the point of contact for all export control related activities throughout UC. The Export Controls Director is the primary responsible official for the institutional-wide development, implementation, maintenance, management, and improvement of the Export Controls Office to ensure overall university compliance with export control laws and regulations related to international trade and technology transfer. The Export Controls Director is the designated senior Empowered Official charged to oversee, administer, and coordinate all export compliance functions in concert with other departments and units as necessary, including:

• Direct the day-to-day operational, administrative, communication, database, and record-keeping functions of the Export Controls Office and all export control and related activities throughout the university, including all staff assigned to the office. Perform risk assessments of the export compliance program.[8]

• Manage the support functions the Export Controls Office provides to other university departments and units, including: performing agreement reviews and analysis; conducting export assessments of international shipping, transfers and travel; preparing, reviewing, approving and submitting license applications for international exports and deemed-exports, and other requests for government agency export approval; determining the applicability of licensing exceptions or licensing requirements and exception/exemption certificates as applicable; and researching, preparing, approving and submitting advisory opinion requests or other government guidance requests.

• Lead, manage and approve the overall university approach to implementing institutional- wide export control policies, procedures, and protocol by working directly with university administration, management, and technical personnel. These documents provide consistency and compliance for all departments and units involved in exports and travel matters, such as: screening end users, end use and countries for exported technology; subcontractors and visitors to controlled facilities; determining international travel requirements including those for embargoed and sanctioned countries.

• Provide subject matter expertise on university policy and procedures related to export controls.

• Develop and maintain the university security approach for controlling technology. Such measures include Technology Control Plan (TCP)/ Sensitive But Unclassified plans, and other security protocols that document controls for: the secure handling, use, storage, and transmission of sensitive information; physical security controls for sensitive work and material storage areas; research activities

[8] See Appendix ZA

subject to export control and activities with contractual security requirements. Provide institutional oversight of TCP implementation and monitor compliance with such plans.

• Maintain and update institutional registrations with necessary federal agencies as they relate to export controls.

• Develop and deliver export control training, guidance, and support to the university community, including, ITAR, EAR, OFAC, DEAR, FAR, international travel and related issues, including embargoed and sanctioned countries.

• Provide strategic consultation and guidance to faculty, staff and administration on decisions impacted by export control regulations.

• Identify project-specific sensitive material concerns. Collaborate with Principal Investigators and research staff to identify sensitive information and equipment. Determine commodity jurisdiction and self-classify equipment and technologies pursuant to ECCN or USML classifications and implement and maintain automated self-classification decision tools (Visual Compliance).

• Identify, implement, and maintain an information management system for tracking and managing export controlled hardware, software, information, and deliverables in accordance with applicable federal and state statutes and policies as well as university policies. Develop and implement automated tools for the screening of research project personnel and external recipients to determine federal export control status (Visual Compliance).

• Make immigration related export certifications and conduct technology alert investigations, as required by the U.S. Consulate. Review H-1B and other foreign national beneficiary information as it relates to deemed export and licensing needs. Work with other units to acquire and review associated agreements and technology/data or software associated with foreign national activity at the university. Review and approve deemed export control attestations on behalf of the university. Manage federal background investigations, personnel security clearances and visit authorizations for employees, consultants, and cleared visitors as it relates to export controls.

• Liaise with federal regulatory and investigatory agencies (Commerce, State, Treasury, Energy, Defense, DSS, FBI) regarding export control matters. Assist federal agencies in the identification and neutralization of foreign interdiction of sensitive U.S. technology, articles, and data identified as export controlled and act as liaison and coordinator for export-related matters between the various research and regulatory offices within UC.

UC International

International Services
The Office of International Services processes all visa requests on behalf of the University of Cincinnati. International Services reviews visa requests and submits all visa applications related to activities to the Export Controls Office for compliance assessment[9]. Sponsoring units are required to submit a Visiting

[9] See Appendix V

Scholar Questionnaire[10] for assessment. International Services relies upon the Export Controls Office for I-129 (Petition for Nonimmigrant Worker) attestations[11]. International Services coordinates with the Export Controls Office to ensure review of employee, visiting scholar and business visitor activity. No one in this department is required to take the Export Control training; however, additional in person or virtual training can be given.

International Planning
The International Planning unit within UC International works jointly with the Export Controls Office and Office of General Counsel (OGC) to review certain international collaborations and exchanges for export compliance. Some agreements are reviewed by International Planning while others are elevated to OGC to ensure that Restricted Party Screenings are conducted and the insertion of an export control clause. No one in this department is required to take the Export Control training; however, additional in person or virtual training can be given.

International Programs
The International Program office works closely with the Export Controls Office to ensure that study abroad programs and activities are compliant with the export controls regulations. The ECO ensures that the travel is approved for the use of a general license under OFAC and that if hand-carried items comply with the EAR/ITAR. No one in this department is required to take the Export Control training; however, additional in person or virtual training can be given.

Office of General Counsel (OGC)

The Office of General Counsel employs multiple attorneys, who provide legal advice to the university, including the Office of Research and the Export Controls. No one in OGC is required to take the Export Control training; however, additional in person or virtual training can be given upon request.

Purchasing

Purchasing assists, the Export Control program by conducting Restricted Party Screens on all vendors. No one in this department is required to take the Export Control training; however, additional in person or virtual training can be given upon request.

Asset Management and Surplus

The Asset Management Office assists the Export Controls Office by ensuring that assets within the electronic system have their export classification (ECCN/USML Category) identified in the system. Then based on the classification, they mark those items that are identified as requiring appropriate destruction or repurposing, so Surplus Management will properly dispose. Surplus Management has policies for sales to the public that include an export controls clause within the terms and conditions to protect the university. No one in this department is required to take the Export Control training; however, additional in person or virtual training can be given upon request.

[10] See Appendix X
[11] See Appendix ZB

UC Information Security (Info Sec)

Info Sec is instrumental in data security and provides incident tracking and reporting of data breaches involving unclassified data, including export controlled data. Info Sec conducts university-wide training concerning threats, methods to counter-threats and other data security methods and guidance on classification and safeguarding of data, storage, and travel[12]. No one in this department is required to take the Export Control training; however, additional in person or virtual training can be given upon request.

UC Office of Technology Transfer

In addition, to being responsible for the licensing of intellectual property, UTAC also reviews, negotiates, and executes, intellectual property related confidentiality agreements, and material transfer agreements. UCTAC works closely with the ECO to ensure proper review and classification of technology when applicable.[13] Everyone in this department is required to take the Export Control training in person, or virtual training can be given upon request.

Office of Sponsored Research Services (SRS)

The Office of Sponsored Research Services (SRS) has the sole authority to bind UC to research related agreements. SRS:

1. Reviews terms of sponsored program agreements and other non-monetary agreements to identify restrictions on publication and dissemination of research results and to negotiate out such restrictions page
2. Provides assistance to PI in identifying international components of sponsored program agreements, identifying potential export control issues in the proposed international component, and verifying that the international entities and individuals are not restricted parties or specially designated nationals.
3. Communicates identified potential export control issues to the PI and the Export Controls Office.
4. Communicates with the Export Controls Office about any changes in awards that necessitate another review of the project for export controls.

No one in this department is required to take the Export Control training; however, grant administrators may request training and complete it accordingly. In person or virtual training can be given upon request for this department.

Research Administrators

The college and department research administrators work closely with SRS and the PI. Together with SRS, they:

[12] See Appendix I, J, K, S, T, U
[13] *See* Appendix Q

1. Provide assistance to PIs in reviewing terms of sponsored program agreements, material transfer agreements 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 PI 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 SRS about any changes in awards that necessitate a re-review of the project for export controls.
5. Research Administrators are required to take Export Control training. They are notified of this requirement upon award.

Business Administrators

The college 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 control laws, ensuring that payments do not go to, or contracts are not entered, 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. Business Administrators are required to take Export Control training. They are notified of this requirement upon award.

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 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[14] 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 plan and on the export control regulations should any apply.

[14] See Appendix F

5. Review all provided guidance by administration to ensure compliance[15]
6. Principal Investigators are required to take Export Control training. They are notified of this requirement upon award.

Export Control Analysis

An export control analysis shall be performed when a PI submits a proposal, receives an award, or changes the scope of an existing project.

SRS performs an initial review of the request for proposal, broad agency announcement or award. A checklist is used to identify potential export control issues[16]. The SRS staff are trained to identify the following red flags 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 equipment(if known).
7. Includes foreign sponsors or collaborators.
8. Travel, shipping, or work outside of the United States;
9. Military applications of project results.

All non-U.S. persons are screened against the specially designated and restricted party lists. Export controlled equipment, data, or technology is identified and referred to the Export Controls Office.

Export Control Classification of Technology

The ECO works with faculty, staff, and students to provide export control classification of technology that is developed on campus as well as received commodities (includes information, designs, products, equipment, etc.). Business Administrators work with ECO to ensure that the export control classification is received from the vendor, or we self-classify the software or items or services contract. The UC Office of Technology Transfer works closely with the ECO to ensure that technology or information is self-classified, utilizing the Internal Classification Form[17] or received from the vendor or provider which sometimes uses the Product Classification Form[18] for internal developed technology as well as proprietary information received through an NDA. The ECO also works with (SRS) to ensure that the sponsor provides the export control classification for commodities or proprietary information that is

[15] See Appendix A, B, and G
[16] See Appendix C, D, and E
[17] See Appendix W
[18] See Appendix H

being provided to the PI, see SRS procedure[19]. The ECO assists faculty and staff with obtaining the export control classification of commodities that are purchased, when requested. The ECO works with Asset Management and Surplus in obtaining the export control classification of commodities listed in the electronic system and providing the classification for identification within the system for tracking and disposal.

The ECO may also consult with an expert, independent of the university, who is under contract by the Office of Research for advice/guidance on classifying technology on an ad hoc basis.

Technology Control Plans (TCP)

When export controlled equipment, data, or technology is identified for a project, the Export Controls Office will work with the PI to develop and implement a TCP[20] to appropriately secure the equipment, data, or technology from access by unlicensed non-U.S. persons. The TCP will include:

1. A commitment to export control compliance;
2. Identification of the applicable export controls and items or technologies subject to the controls;
3. A description of the agreed upon security measures to control the item/technology including as appropriate:
    a. Laboratory compartmentalization
    b. Time blocking
    c. Marking
    d. Locked storage
    e. Electronic security
    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;
7. If any circumstances or changes that would cause a TCP to be amended (i.e., new student/researcher added) *occur during the project outside of annual review*, it is the PI's responsibility to notify the Export Controls Office. Notification by the PI must occur **immediately** in order to minimize any impact to the research.
    a. The ECO will prepare an addendum describing the changes which will be added to the end of the TCP.
    b. Both the TCP and addendum will be reviewed at annual review and updated, if applicable. Any new student/researcher added will undergo mandatory training in order to access the controlled item/technology. The ECO will authorize access upon receipt of training verification.
    c. The addendum will be signed by the PI and the student/researcher.
    d. The form will be returned to the Export Control office for filing with the original TCP;
8. Export control training will be required of all individuals listed on the TCP (in Appendix A).; and

[19] See Appendix E
[20] See Appendix F

9. TCPs will be reviewed and updated annually, based on when the initial TCP was approved, using the TCP Audit form. The audit form identifies critical information pertaining to the TCP as well as any information that requires updating.
    a. The ECO will review the audit document and discuss with the PI any changes to personnel which may require reviewing physical access and/or ECO training.
    b. Multiple discussions between PI and ECO may be required to fully understand any changes needed.
    c. If there was an addendum made earlier in the year, this information will be verified by the PI and will continue to reside coupled to the TCP.
    d. Once all information is updated accordingly and confirmed, the PI will attest to the best of his/her knowledge that the audit form is accurate. As of June 1, 2022, a time/date signature will be required. This will be documented in writing and saved in the TCP folder on the Shared Drive.
    e. The PI will be reminded of his/her responsibility to secure ITAR research data and materials for five years in accordance with Department of State, university records retention policies and the Office of Research once the ITAR research has concluded.

Before any individual may have access to export controlled items or technology, they must be informed of the conditions of the TCP, have a clean restricted party screening result, and agree to comply with the security measures outlined in the TCP.

If a license or exemption/exception is necessary for the involvement of a foreign person, then the Export Controls Office will notify the PI and all parties involved in the activity. The TCP will not be endorsed and the project or access to the controlled technology will not be permitted until authorization from a UC Empowered Official is received. The authorization will list the exemption/exception, if a license is necessary the ECO will request from the cognizant US government agency. Then the authorization will be stated in the TCP and endorsed by all parties to ensure understanding and compliance.

Safeguarding Export Controlled Data

UC provides guidance for how to identify[21] and safeguard export controlled technical data on the UC website in addition to this manual[22]. The electronic and physical storage of export controlled data must be managed appropriately. The following guidelines are drawn from regulations issued by the Department of Defense, mandating "enhanced safeguarding" measures for certain types of data. Note that breaches of systems containing Unclassified Controlled Technical Information must be reported to the Department of Defense within 72 hours of discovery. UC offers a service for storing export controlled research data that adheres to the guidelines below.

Export-controlled information housed at the University of Cincinnati must be managed in accordance with these guidelines. Export-controlled information that is received by or brought to UC must be

[21] See Appendix !, J
[22] See Appendix M

housed on the Isilon server designated for this purpose. Any exceptions must be explicitly approved by the Export Controls Office.

Guidelines

Data subject to ITAR or EAR export control restrictions is referred to collectively below as Controlled Information and must comply with the following access controls

Access Controls

Do not access Controlled Information from shared, public computers such as kiosk computers in libraries, hotels, and business centers, or from computers that have no local access control.

Do not post Controlled Information on public websites or websites that rely solely on IP addresses for access control. Secure access using individually-assigned accounts requiring username/password, user certificates, or other user-specific authentication methods.

Protect Controlled Information by at least one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.

System Management

Use regularly-updated malware protection software.

Keep computers hosting Controlled Information up to date on security patches and updates

All Controlled Information must be encrypted if stored on mobile computing devices such as laptops, PDA's and removable media such as thumb drives or CD/DVD (see additional notes below).

Wipe electronic media in accordance with NIST 800–88, Guidelines for Media Sanitization.

Transmission of Data

Do not transmit or email Controlled Information unencrypted. If encryption is not available, data must be individually encrypted using at least application-provided mechanisms such as the password-based encryption provided in Microsoft Office 2007 and above.

Transmit Controlled Information via voice or fax only where there is reasonable assurance that access is limited to authorized persons.

Wireless network access to Controlled Information must be encrypted using, e.g., WPA2 Enterprise wireless network encryption or VPN.

Provide monitoring and control over inbound and outbound network traffic. Include blocking unauthorized ingress and egress.

Detect exfiltration of data using firewalls, router policies, intrusion prevention/detection systems, or host-based security services.

Transfer controlled information only to subcontractors with a need to know. Subcontractors must adhere to these same data protection requirements. - These data protection requirements, including this requirement, must be included in all subcontracts if access to or generation of controlled data will take place.

Shared Systems

In such cases where the Controlled Information is a software executable that will be run on a shared (multi-user) system such as a compute cluster, the following additional guidelines apply:

The directories containing the software shall be access controlled so that only the designated user(s) as approved by the PI will have read, write and execute permissions. No others shall have access.

The shared system shall have audit logging enabled, and the audit logs shall be backed up.

The shared system shall be managed solely by U.S. Persons, as defined in the export regulations. All users with root or pseudo privileges must be U.S. Persons.

Only U.S. Persons shall have unescorted physical access to the shared system.

Mobile Computing Systems

In such cases where data must be stored locally on a mobile device, as determined by the PI, the following guidelines apply:

The data must be stored on a single-user portable device in a volume using strong encryption (e.g., AES-256) with a unique decryption passphrase known only to the device's authorized primary user.

Where feasible (e.g., if the mobile device is a laptop computer), the mobile device must be protected by a software firewall.

Where feasible (e.g., if the mobile device is a laptop computer), the mobile device must have audit logging enabled and audit logs backed up.

Where feasible (e.g., if the mobile device is a laptop computer), the mobile device must be accessed using a login account with a password of no less than 8 characters in length, a mixture of upper -and lower-case letters, numbers and symbols, subject to change no less frequently than annually, or when any possibility of password exposure is suspected.

Inbound remote login to any mobile device containing export-controlled data is prohibited by policy.

If data backup is required, the encrypted volume must be backed up intact, with encryption preserved.

In all cases, export-controlled data must be housed on Institute-owned devices.

Requirements for Safeguarding DoD Unclassified Controlled Technical Information

There are additional requirements for safeguarding Department of Defense (DoD) unclassified controlled technical information that resides on or transits through UC's information technology systems.

Please contact the Export Controls Office for guidance if you plan to receive DoD Unclassified Technical Information on behalf of UC.

Goal

The goal of your security measures is to be able to answer the following questions in the affirmative:

> Can you trace with precision who is working on the project?
>
> How do you know with whom they can share the work? How do you track/ensure this?
>
> Do you have appropriate physical and electronic precautions in place to prevent unauthorized access?
>
> Do you have the appropriate physical and electronic precautions in place to restrict access to project data to only authorized individuals?

Managed Hosting for Export Controlled Data

The University of Cincinnati (UC) offers a service for storing export controlled research data. This service adheres to the guidelines described in Safeguarding Export Controlled Data.

Access Control

The server is housed in a climate-controlled, locked data center with physical access controlled via individually-issued electronic card keys using a card-key system that logs all entry events. Physical access to the server is limited to authorized staff employed by UC.

A local software firewall and an external hardware firewall provides monitoring and control over inbound and outbound network traffic. Only authorized network traffic will be permitted. Firewall permit and deny events are logged.

Access is restricted to a limited number of authorized users only, as determined and requested by the PI. Access requests and approvals will be logged. No access will be granted to non-U.S. Persons without an export license, exemption, or other government authorization. U.S. Person status will be confirmed with UC's Human Resources department before access requests are granted. Exception status will be confirmed with UC's Export Controls Office.

All remote access to the server will be controlled via unique username and password credentials. All authentication events, including username, date/time and source IP address, will be logged to a central server monitored by UC's Information Security Office (InfoSec).

Maintenance and configuration

The server utilizes up-to-date malware detection software. The operating system and software will be kept current on security patches by authorized US Person staff employed by UC InfoSec.

Data will be backed up via an encrypted network connection to a remote site leased by UC and staffed by U.S. Persons. Access to backups will be limited to authorized U.S. Persons employed by UC.

Decommissioning

Decommissioned drives will be destroyed by shredding through UC Surplus. All other media sanitization will follow UC's Electronic Media Sanitization Standard[23].

Remote access

All remote access to the data will be conducted via encrypted network connections. Wireless network access to the data is disallowed except from UC remote connections or where UC VPN is used.

Remote access from shared, public computers or from computers with no local access control is prohibited by policy.

Copying of data from the server is prohibited by policy unless:

1) The data is transmitted via a local, private network to an access-controlled authorized backup device, or

2) The data is transmitted via an encrypted network connection to an encrypted volume by an authorized user with prior approval from the PI, or

3) The data is transmitted via an encrypted network connection in the form of an encrypted file or volume from an authorized user, to an authorized recipient as determined by and with prior approval from the PI.

International Travel Recommendations

It is recommended if you are traveling internationally with UC owned equipment, items, samples, etc. that you use the International Travel Certificate[24] and implement the recommended IT Security protocols[25]. All employees are encouraged to use Concur prior to traveling. Concur provides travelers with any relevant advisory and/or security risks/concerns for the traveler for both domestic and international travel.

[23] See Appendix K
[24] See Appendix P
[25] See Appendix S and T

Licensing

Licenses from OFAC may be required in support of international university activities in embargoed countries. Licenses from the Department of State or the Department of Commerce may be required for the export of UC owned equipment in support of international activities. Additionally, export licenses may be required in order for foreign nationals to access controlled items or technology at UC. The Empowered Officials are the individuals at UC authorized to apply for licenses. In the event that a license is required, the Empowered Official with the advice of the Office of General Counsel as required will prepare and sign the necessary documentation for preparing the license request. The Export Controls Office will be responsible for maintaining records associated with license requests.

UC personnel who are unsure about licensing requirements for proposed international activities or the use of controlled equipment by foreign nationals should consult with the Export Controls Office prior to engaging in the activity.

Restricted Party Screening (RPS)

RPS[26] ensures UC does not engage in an unlawful transaction or restrictive trade practice with a debarred or restricted entity (e.g., person, institution, company) prior to and for the duration of any type of business transaction, including providing services or collaboration. U.S. exporters are prohibited from conducting export related business with parties subject to denial orders (i.e., parties listed on the Department of Commerce, Denied Persons List ("DPL"), parties specified on the Department of Treasury, Specially Designated Nationals List ("SDN") or Specially Designated Terrorists List ("SDT"), or parties subject to Department of State proscription, suspensions or debarments). This prohibition includes intra-country transfers abroad of U.S. origin goods and technology and the servicing of a denied party's U.S. origin items. In order to prevent business with such denied parties, UC uses a current list of these parties against which it screens customers, suppliers, consultants, and other business partners. An auditable record indicating that the DPL screening has been performed is maintained by the ECO on any document, database or list that is screened.

Various U.S. Government agencies maintain a number of lists of individuals, parties, corporations, entities institutions, governments, etc. that are debarred, suspended, blocked, declared ineligible or otherwise restricted from entering into certain types of transactions with U.S. Persons, including universities. A party or entity designated on a federal list may be subject to a variety of federal prohibitions or other regulatory requirements of which UC is obligated to comply.

UC utilizes the e-Customs "Visual Compliance" system to conduct mandatory RPS of over 50+ US government restricted party lists. These lists include export-related restricted, denied and blocked persons and munitions export-related restricted, denied and blocked persons, and sanctioned countries. Screening involves database searches for key words, specifically, names, organizations, vendors, suppliers, etc. to ensure that no foreign nationals on any government "watch" lists, sanctioned or embargoed country are associated with a UC research contract.

[26] See Appendix ZF

All potential RPS alerts are investigated, research, analyzed and concluded by the ECO.

These screenings are being conducted by various units throughout UC either by manual entry or an automated bulk upload of names. All companies, entities, affiliates or persons are required to be screened before the commencement or continuation of the business relationship. Parties are added to and removed from various restriction lists daily. Should an entity with whom the university has an existing relationship be added to a federal list, UC is required to comply with the regulatory requirements imposed on the entity regardless of the type, value or duration of the relationship.

Training

Training is the foundation of a successful export compliance program. Well-informed employees minimize the likelihood that inadvertent violations of the law will occur. The greatest risk of non-compliance of export laws and regulations occurs during casual conversations in person, on the telephone, or via e-mail. The way to prevent these types of violations is through awareness and training.

Outreach is provided by the Export Controls Office through in-person meetings, presentations, training, website, and Compliance Matters email newsletter.

The Export Controls Office provides training materials and will ensure that UC personnel engaged in export controlled activities receive the appropriate briefing. The Export Controls Office maintains records of training provided. In addition to in person training sessions, training on export controls is available through CITI found on the following website: http://researchcompliance.uc.edu/ExportControls/Training.aspx .

Recordkeeping

UC's policy is to maintain export-related records based on individual controlled items or activities. Unless otherwise provided for or instructed by the Office of the General Counsel, all records shall be maintained consistent with the UC Export Controls record retention policy[27], and shall be retained no less than five years after the TCP termination date or license termination date, or date of last export (e.g., shipment, hand-carry, deemed, etc.), whichever is later. Any document destruction will be recorded in accordance with University policy and a copy of the disposal form will be sent to the UC Records Manager.

If ITAR-controlled technical data is exported under an exemption, certain records of the transaction must be kept even beyond UC's five year retention period.[28] Those records include:

A description of the unclassified technical data;

The name of the recipient /end-user;

[27] *See* Appendix N
[28] *See* 22 C.F.R. §§ 122.5 and 123.26.

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.[29] 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 Auditing

In order to maintain UC's export compliance program and to ensure consistent adherence to U.S. export laws, the Export Controls Office shall conduct annual internal reviews of TCPs using the TCP Audit form and export records. The purpose of the reviews is: (i) to identify possible violations; and (ii) to update/confirm active personnel; (iii) maintain accurate physical access records as well as procedures, etc. that require updating.

Detecting and Reporting Violations

Any individual who suspects a violation has occurred must immediately[30] notify the ECO, the OGC, the Compliance Hotline at (800) 889-1547 or EthicsPoint, UC's anonymous reporting system. The Export Controls Director and Empowered Official will work with OGC to determine the appropriate follow-up to the notification, which may include a voluntary self-disclosure to the U.S. Government. An Empowered Official may send an initial notification about the suspected violation to the appropriate government agency.[31] The ECO, 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 and OGC is consulted, the ECO may provide the U.S. 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;

[29] *See* 15 C.F.R. § 762.6.

[30] Appendix Y: http://www.uc.edu/content/dam/uc/trustees/docs/rules_10/10-17-02.pdf and http://www.uc.edu/content/dam/uc/trustees/docs/rules_10/10-17-03.pdf

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

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. UC's commitment to export controls compliance.

Once the initial notification and supplementary letter have been sent, UC will follow the U.S. Government agency's instructions.

Glossary of abbreviations

AECA	Arms Export Control Act
AES	Automated Export System
BAG	Baggage
BIS	Bureau of Industry and Security
CCL	Commerce Control List
DDTC	Directorate of Defense Trade Controls
EAR	Export Administration Regulations
ECCN	Export Control Classification Number
ECO	Export Controls Office
ITAR	International Traffic in Arms Regulations
OFAC	Office of Foreign Asset Controls
OGC	Office of General Counsel
SRS	Office of Sponsored Research Services
SDN	Specially Designated National
TCP	Technology Control Plan
TMP	Temporary imports, exports, re-exports, and transfers (in-country)
USML	United States Munitions List
USMIL	United States Munitions Import List