University of Missouri System

COLUMBIA | KANSAS CITY | ROLLA | ST.LOUIS

Export Compliance Management Program

February 8, 2023

I. Table of Contents

II. Introduction

U.S. export control and sanctions regulations are designed to accomplish various national purposes such as achieving foreign policy objectives, protecting national security, and enhancing economic competitiveness. The U.S. Government regulates the export of items and their associated parts, components, software, and "technology", including to foreign persons in the U.S. Technology includes both technical data, such as blueprints and manuals, and technical assistance that involves design, services (including the transfer of knowledge) and training. The U.S. export control system generally restricts the export of defense articles[1], defense services, and/or "dual-use" commodities and technologies that have both commercial and military applications. Export control regulations are broadly applicable. The regulations apply to U.S.-origin items, software, and technology located anywhere in the world including the reexport or retransfer abroad to third parties. The regulations also apply to any foreign-origin items, software and technology that are located within the U.S.

The U.S. Government also administers and enforces economic and trade sanctions against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and others engaged in activities contrary to U.S. interests. Sanctions laws apply to all persons located in the United States (regardless of citizenship) and to all U.S. persons (wherever located). These sanctions restrict services of value, including imports from and exports to comprehensively sanctioned locations and with entities and persons subject to list-based sanctions.

Three principal agencies regulate exports from the United States:

1) The U.S. Department of State, Directorate of Defense Trade Controls (DDTC)[2] regulates the export of defense articles and defense services through the International Traffic in Arms Regulations (ITAR);
2) The U.S. Department of Commerce, Bureau of Industry and Security (BIS) regulates the export of less-sensitive defense items and technology, "dual-use" items, and purely commercial goods under the Export Administration Regulations (EAR); and
3) The U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC) regulates sanctions against comprehensively sanctioned destinations and selective sanctions through restricted party lists under specialized regulatory actions or executive orders.

Other government agencies (i.e., the Department of Energy, Nuclear Regulatory Commission, etc.) also regulate exports. The U.S. Department of Commerce, Bureau of the Census regulates how and when exports are reported to the federal government through the Foreign Trade Regulations (FTR). While this Program focuses mainly on DDTC, BIS, and OFAC, all applicable regulations must be considered before engaging in any activity that may be subject to export control or sanctions regulations.

III. Export Controls, Sanctions, and Universities

While the responsibility for ensuring UM complies with export control and sanctions regulations is housed locally in each institution's Office of Research, these regulations apply to all University activities, even those that do not involve research. For example, entering into contracts with foreign entities or restricted parties, sending money to a party subject to comprehensive or targeted sanctions, presenting at a conference organized by parties subject to comprehensive or targeted sanctions, remotely employing people who live in places subject to comprehensive sanctions, international travel with University-issued equipment, or shipping items out of the United States all have export compliance implications for UM.

The majority of UM's export and sanctions compliance challenges are related to the University's research activities. Export controls and economic sanctions create a unique struggle in an academic research environment because compliance requires balancing concerns about economic development (through the safeguarding of proprietary business information) and national security against the traditional concepts of

[1] A glossary of common export compliance terms can be found at the end of this document.
[2] See "Commonly Used Acronyms" found at the end of this document.

academic freedom in research and the unrestricted publication and dissemination of research findings and results.

While U.S. policymakers recognize that "foreign students and scholars at U.S. universities provide support to university research efforts and to developing some of the nation's leading-edge civilian and defense-related technologies",[3] there is still concern over the potential transfer of controlled technologies to other countries and the consequences for U.S. national interests. Therefore, U.S. government agencies require that universities understand and comply with export control and sanctions regulations.[4] All UM personnel must be mindful of export control implications across all university activities, paying particular attention to their impact on research efforts, regardless of the funding source.

IV. U.S. Department of State

The U.S. Department of State, through the Directorate of Defense Trade Controls (DDTC), maintains the International Traffic in Arms Regulations (ITAR) which regulates the export and re-export of defense articles, defense services and related technical data (including software) from the United States to any foreign destination or to any foreign person located in the United States, i.e., a "deemed export". The ITAR contains the United States Munitions List (USML), which lists those commodities, related technical data, and defense services controlled for export purposes.

The State Department prohibits exports, imports, and sales to or from certain countries through statutory and administrative debarment lists. These lists include the Arms Export Control Act Debarred Parties, the Cuba Restricted List, the Cuba Prohibited Accommodations List, and the Terrorist Exclusion List. Additionally, there are a variety of Nonproliferation Orders that are implemented by the State Department, including but not limited to the Iran Freedom and Counter-Proliferation Act, Executive Orders 13949 and 13382, the Iran and Syria Nonproliferation Act, Missile Sanctions Laws, Chemical and Biological Weapons Sanctions Laws, and the Countering America's Adversaries Through Sanctions Act (CAATSA).

A. Items Controlled Under the ITAR

The ITAR regulates the export of defense articles, which are inherently military items and the associated information needed for the design, operation, repair, maintenance, etc. of defense articles. In other words, the ITAR covers not just physical items, but also the technical data, "know-how," and software required to operate those items. Because the "know-how" associated with a defense article is controlled, training another person on that "know-how" may also be a controlled activity known as a defense service.

The ITAR also controls the parts, components, and technology incorporated into an item, unless otherwise noted in the USML. If an item contains any components that are controlled under the ITAR, the entire item is thereby controlled under the ITAR, an unwritten DDTC policy commonly called the "see-through rule"[5]. "The 'see through' rule was most succinctly articulated in the State Department's Draft Charging Letter in the Boeing QRS-11' matter, as follows: 'The QRS-11 is covered by the U.S. Munitions List' and 'did not cease to be controlled by the ITAR simply by virtue of its inclusion into a non-USML flight instrument.'"[6] Some non-military items (such as commercial satellites with specific characteristics)[7] and certain chemical precursors, toxins, and

[3] GAO Report "Export Controls: Enforcement Agencies Should Better Leverage Information to Target Efforts Involving U.S. Universities," June 2022, available at https://www.gao.gov/assets/gao-22-105727.pdf

[4] GAO Report "Export Controls: Agencies Should Assess Vulnerabilities and Improve Guidance for Protecting Export-Controlled Information at Universities," December 2006, available at https://www.gao.gov/assets/gao-07-70.pdf

[5] ITAR / USML Updates FAQs: Where can I find the "see-through rule" in the ITAR and how does it work?, available at https://www.pmddtc.state.gov/ddtc_public?id=ddtc_public_portal_faq_detail&sys_id=e79535e31be7dc90d1f1ea02f54bcbf4

[6] Global Trade Law Blog, *Military Electronic Export Reform: Let the Chips Fall Where They May*, Scott Maberry and Reid Whitten, posted December 4, 2014 https://www.globaltradelawblog.com/2014/12/04/military-electronics-export-reform-let-the-chips-fall-where-they-may/

[7] "Spacecraft, including satellites and space vehicles, whether designated developmental, experimental, research, or scientific, or having a *commercial, civil*, or military end-use, that [meet one or more of thirteen listed characteristics]" are enumerated in Category XV-Spacecraft and Related Articles. (22 CFR §121.1, emphasis added.)

biological agents, are also controlled under the ITAR. In addition, there may be occasions where an ITAR item is used for research unrelated to that item's military purpose. It is important to understand that the ITAR designation applies to an item regardless of how it is being used.

B. The United States Munitions List

The United States Munitions List (USML) enumerates defense articles and defense services (including related technical data and software), as designated by the Arms Export Control Act of 1979, and groups them into 21 categories (see Exhibit A). An electronic version of the USML is available through the Electronic Code of Federal Regulations, and shall be, for purposes of this Export Compliance Management Program (ECMP), the appropriate authority for the contents of the USML.

C. Jurisdiction and Classification[8]

Determining the jurisdiction and classification of items is crucial for compliance with the U.S. export control system. Verifying whether an item is subject to the jurisdiction of the ITAR is the first step taken when establishing the applicable controls on the export, retransfer, or reexport of that item. DDTC has the ultimate responsibility over determining whether an item is subject to regulation under the ITAR. The item should be presumed to be ITAR controlled until it is determined not to be enumerated on the USML. Jurisdictional determinations are typically based on criteria that include whether it is predominantly used in civil or military applications.[9]

After the jurisdictional status of an item is resolved (e.g., whether it is subject to the ITAR) the next step is to determine its classification status (e.g., where on the ITAR's USML the item is described). This step must be completed before a determination can be made as to whether a license or other authorization is required to export, retransfer, or reexport the item to the proposed destination or end user or for the proposed end-use.

The U.S. government encourages exporters to self-classify items wherever possible. Self-classification of items under the jurisdiction of the ITAR will be performed by Research Security and Compliance, in conjunction with the PI, sponsor, manufacturer, and other parties as appropriate to identify the accurate USML Category. If self-classification is not possible, a Commodity Jurisdiction (CJ) request can be submitted to DDTC to determine the appropriate classification under the ITAR. University employees must contact Research Security and Compliance prior to attempting to classify an item. If a CJ determination is necessary, Research Security and Compliance will file the request on behalf of the University.

D. Embargoed Countries Under the ITAR

DDTC maintains a list of countries under U.S. or United Nations arms embargoes that are subject to more stringent export restrictions under the ITAR. License exemptions are not available for ITAR exports to these countries. The State Department has a policy of denying license applications to export, or otherwise engage in transactions involving, ITAR-controlled defense articles and/or defense services to certain countries;[10] license applications for other countries are reviewed and approved on a case-by-case basis. A complete list of U.S. arms embargoes is available at 22 CFR § 126.1: Prohibited export, imports, and sales to or from certain countries.

E. Authorization to Export Under the ITAR

With very few exceptions, the export of defense articles and defense services is restricted to all non-U.S. destinations and to all foreign persons in the U.S. Through their research activities, UM personnel are typically

[8] "Classification" here refers to the analysis and selection of a USML category for a defense article., It is not a reference to information that, for national security purposes, has been classified pursuant to Executive Order 13526 and is subject to the National Industrial Security Program (NISP).

[9] More information about the criteria used by DDTC in providing a commodity jurisdiction determination can be found in 22 CFR § 120.4 (Commodity Jurisdiction)

[10] At the time this document is published, arms embargoes with strict policies of denial are in place against Belarus, Burma (Myanmar), China, Cuba, Iran, North Korea, Syria, and Venezuela, see 22 CFR § 126.1.

engaged in the creation of data that is not subject to the ITAR or are engaged primarily in the fabrication of non-defense articles for experimental or scientific purposes. No license is needed if only U.S. Persons are involved or have access to defense articles or defense technology in the United States.

If UM researchers desire to involve foreign persons in an ITAR-controlled, restricted research project, it is likely that it will be necessary to obtain a license from DDTC. The University must apply for and receive permission from DDTC in the form of an export license before any export of a USML item, release of ITAR-controlled technical data, or provision of a defense service can occur.

F. Registration with the Directorate of Defense Trade Controls (DDTC)

Any U.S. person or entity that manufactures, brokers, or exports defense articles or services must be registered with DDTC, and registration is required prior to applying for a license or utilizing some license exemptions. The Curators of the University of Missouri is registered with DDTC and renews its registration annually. UM regularly reviews research projects and available license exemptions to determine if a license is required to complete that project. Assistance from the faculty involved in such projects is critical and expected in order to accept restricted research. Any request for licensing must be routed to the Empowered Official in Research Security and Compliance for review, processing, and submission to DDTC. University employees may not independently submit license applications or register with DDTC for any University-related activity.

V. U.S. Department of Commerce

The Bureau of Industry and Security (BIS), within the U.S. Department of Commerce, regulates the export of commercial and dual-use products and technology under the Export Administration Regulations (EAR). The EAR covers a wide range of products and technologies, which are enumerated on the Commerce Control List (CCL). The EAR also regulates the export of all other items, software, and technology not specifically enumerated on the USML or the CCL. The product classification process is highly technical and licensing requirements are dependent upon the type of product, the final destination (country and recipient), and the intended end use.

The EAR also implements “Lists of Parties of Concern” which include, but are not limited to, the Denied Persons List, the Entity List, the Unverified List, and the Military End User List. If a company, entity, or person is found on one of these lists, the University must take on additional due-diligence activities. The list a party is found on will identify whether exports to that party are strictly prohibited, whether there are specific licensing requirements, or whether there are other red flags that need to be resolved.

A. Items Controlled Under the EAR

Generally, all non-ITAR items of U.S.-origin, wherever located, are subject to the EAR. Foreign-made items that incorporate a defined amount of controlled U.S.-origin technology or software may also be subject to the EAR.

The EAR requires a license for the export of a wide range of commercial items that have potential military use (commonly called “dual-use” items) or that otherwise have non-military strategic value to the U.S. In addition, under the process of “Export Control Reform,” many items previously under regulation by the ITAR have been transferred to control by the EAR. Thus, the EAR now also regulates certain lower-level military products. Unlike the ITAR’s ‘see through’ through rule, the EAR typically, though not always, considers the complete product being exported rather than each subcomponent of the item (i.e., a ‘black box’ approach). Purely commercial items generally have fewer export restrictions.

B. The Commerce Control List

Items subject to control under the EAR are enumerated on the Commerce Control List (CCL). If an item (including the technology and/or software associated with that item) is listed on the CCL, it may require a license prior to export, depending on the country to which it will be exported and other factors.

Items listed on the CCL are assigned an Export Control Classification Number (ECCN) based on a category and a product group. The first digit of an ECCN represents the category, and each of the ten categories is divided further into five product groups, represented by the second digit of an ECCN (see Exhibit B). The last three digits establish the stringency of the controls. Numbers beginning with a 'zero' or 'one' (e.g., 4A**0**01), indicate highly rigorous controls while those beginning with a 'nine' (e.g., 4A**9**94), are subject to lower levels of control.

Many commercial goods are not listed on the CCL and do not have an associated ECCN. These goods are designated as EAR99 and generally consist of low-level technology and consumer goods. Although they are not specifically enumerated on the CCL, EAR99 items are still subject to the EAR. They generally can be exported without a license to any destination other than to a sanctioned destination, to a restricted party, or for use in certain prohibited end-uses.

An electronic version of the CCL is available through the Electronic Code of Federal Regulations, and shall be, for purposes of this ECMP, the appropriate authority for the contents of the CCL.

C. Jurisdiction and Classification[11]

As discussed above, DDTC is the ultimate authority on whether an item is under the jurisdiction of the ITAR or the EAR. DDTC encourages exporters to self-classify. If doubt exists, a CJ request may be submitted to DDTC to determine whether an item is ITAR or EAR controlled. (See Part III(C))above for the process to request a CJ). Items that do not fall under ITAR jurisdiction are generally controlled by the Department of Commerce Bureau of Industry and Security (BIS) under the EAR.

Once jurisdiction under the EAR is established, the next step is to classify the item on the CCL. As with jurisdiction, the regulatory agencies encourage exporters to self-classify. Self-classifications of items that are under the jurisdiction of the EAR will be performed by Research Security and Compliance, in conjunction with the PI, sponsor, manufacturer, and other parties as appropriate to identify the accurate Export Control Classification Number (ECCN) on the CCL or EAR99 designation. However, if Research Security and Compliance is unable to determine the ECCN, the next step will be to submit a "Classification Request" to BIS.[12] Additionally, Research Security and Compliance can file a request for a non-binding "Advisory Opinion" to ask for guidance in regard to interpretations of the EAR or to determine whether a license is required or would be granted for a particular transaction.

If an item is improperly exported because of an erroneous self-classification, the University is liable for any violation. University employees must contact Research Security and Compliance prior to attempting to classify an item. If a classification request or advisory opinion is necessary, Research Security and Compliance will file the request on behalf of the University.

D. Authorization to Export Under the EAR

An item's export classification dictates the need for an export license. For each ECCN, the CCL will provide the "Reason for Control" (license requirements), available license exceptions, a list of items or technology controlled by that ECCN, and other valuable information. The "Reason for Control" applicable to the ECCN are

[11] 'Classification' here refers to the analysis and identification of a USML Category, an ECCN or EAR99 designation or USML Category. It is not a reference to information that, for national security purposes, has been classified pursuant to Executive Order 13526 and is subject to the National Industrial Security Program (NISP).

[12] BIS assists with determining the specific ECCN of a dual-use item listed on the CCL. However, if doubt exists as to whether an item is ITAR or EAR controlled, BIS may forward the issue to DDTC for jurisdiction determination before proceeding with the classification.

cross-referenced against the country of ultimate destination in the EAR's "Country Chart"[13] to determine whether an export license is required for a transaction.

Registration with the BIS electronic licensing system is required prior to applying for a license. As such, The Curators of the University of Missouri is registered with BIS. Any request for licensing must be routed to Research Security and Compliance for review, processing, and submission to BIS. University employees may not submit license applications or register with BIS independently for any University-related activity.

E. Anti-Boycott Restrictions

Anti-boycott regulations, administered by BIS under the EAR, were first implemented to prevent U.S. businesses from participating directly or indirectly in the Arab League Boycott of Israel. The Arab League's boycott has lessened over the years, yet it remains in effect in some countries. The regulations were broadly written to apply to any boycott not endorsed by the U.S. government.

U.S. law prohibits U.S. businesses and their employees from agreeing to participate in, further, or support an international boycott of any country that is a United States ally or that is not sanctioned by the United States. Under Missouri law, the University cannot enter certain kinds of contracts without first obtaining written certification that the other party and/or its affiliates do not and will not boycott Israel.

Anti-boycott restrictions prevent the University from agreeing to actions that include:

1) Refusing to do business in or with a boycotted country or person;
2) Discriminating against persons based on race, religion, sex, national origin, or nationality;
3) Furnishing information about business relationships in or with a boycotted country; or
4) Providing information about the race, religion, sex, national origin, or nationality of another person.

The U.S. Department of the Treasury publishes a list of countries that "require or may require participation in, or cooperation with, an international boycott." As of Dec. 23, 2022, that list includes Iraq, Kuwait, Lebanon, Libya, Qatar, Saudi Arabia, Syria, and Yemen[14]. University personnel must take care when reviewing and negotiating contracts or other agreements with entities from these countries.

Boycott requests can take many forms and may not always be obvious. One example is a request for certification that goods are not coming from a specific country, such as, "In the case of overseas suppliers, this order is placed subject to the suppliers being not on the Israel boycott list published by the central Arab League."[15] A request for information about a business relationship with a specific country or about a person's race, religion, or national origin may also signal a boycott request.

University employees may not agree to contractual terms requiring participation in a boycott under any circumstances. Contact Research Security and Compliance for assistance concerning such requests. U.S. Persons asked to engage in these types of activities are mandated by law to report the request to BIS or the Internal Revenue Service. Research Security and Compliance in conjunction with the Office of General Counsel will submit such reports on behalf of the University.

VI. U.S. Department of the Treasury

The U.S. Department of the Treasury, through the Office of Foreign Assets Control (OFAC), administers several different sanctions programs. The sanctions can be either comprehensive or targeted and are used to

[13] Export Administration Regulations. 15 CFR § 738, Supplement No. 1 Commerce Country Chart. Retrieved November 28, 2022, from https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-738/appendix-Supplement%20No.%201%20to%20Part%20738. See Exhibit B for additional information about using the Country Chart.
[14] List of Countries Requiring Cooperation With an International Boycott, FR Doc. 2022-27923 (December 23, 2022). *Federal Register: The Daily Journal of the United States.*
[15] BIS, Examples of Boycott Requests, at https://www.bis.doc.gov/index.php/enforcement/oac/7-enforcement/578-examplesof-boycott-requests.

achieve foreign policy and national security goals by isolating the targets of the sanctions and depriving them of resources. Other goals of sanctions programs are to compel the targets to change their practices, to penalize the targets for their practices, and to make a political statement of opposition to those practices. Sanctions help prevent U.S. persons and organizations from doing business with terrorist organizations, embargoed countries, nationals of some targeted countries, international narcotics traffickers, and other specified entities engaged in activities related to the proliferation of weapons of mass destruction or other threats. The regulations apply not only to U.S. persons, wherever located, but also foreign persons located in the U.S.

OFAC implements most of the active sanctions programs under the umbrella of the Foreign Assets Control Regulations (FACR). OFAC acts under Presidential wartime and national emergency powers and through the authority granted by specific legislation such as the International Emergency Economic Powers Act (Russia, Sudan, Iran, Syria, Burma/Myanmar, terrorism, narcotics, and nonproliferation) and the Trading with the Enemy Act (Cuba and North Korea).[16] OFAC has the authority to prohibit U.S. persons and corporations from making payments, providing services, or exporting/providing anything of value[17] to sanctioned countries, governments, businesses, organizations, or individuals. OFAC can impose controls on business transactions of all kinds and freeze any assets that are under U.S. jurisdiction. OFAC also prohibits travel to[18], and certain other dealings with some sanctioned countries.

OFAC, as well as the U.S. Department of State and the U.S. Department of Commerce, administer and enforce U.S. sanctions, principally through three types of programs:

1) Country/Region Based: These prohibit nearly all activities and transactions involving certain countries or regions (currently those are Cuba, Iran, North Korea, Syria, the Crimea Region of Ukraine, and the so-called Donetsk People's Republic and Luhansk People's Republic in Ukraine);
2) List Based: These prohibit or restrict activities and transactions with certain targeted individuals and entities including, for example, those listed on, or owned, directly or indirectly, 50% or more in aggregate by those listed on OFAC's Specially Designated Nationals and Blocked Persons List ("Blocked Persons"); and
3) Government/Industry Sector Focused: Prohibits or restricts activities and transactions with certain governments (currently the Government of Venezuela), entities in certain industry sectors in certain countries (currently Russia and Venezuela) and, in relevant part, activities and transactions related to certain credit, debt, or equity.

A. Comprehensive Sanctions

Comprehensive U.S. sanctions prohibit most transactions with (1) persons or entities in a sanctioned country or region; or (2) the government of a sanctioned country or region. This prohibition includes importing and exporting goods and services (directly or indirectly), as well as "facilitation" of transactions between foreign parties and a sanctioned location. More limited sanctions programs may block specific transactions or require licenses under certain circumstances for exports to certain countries.

There are a handful of locations commonly referred to as "OFAC countries" or "embargoed destinations" to whom comprehensive sanctions, administered by OFAC, have been applied. These are Cuba, Iran, North

[16] Other major sanctions laws include the Countering America's Adversaries Through Sanctions Act (Iran, North Korea, Russia) ; the United Nations Participation Act (Iraq and diamond trading); International Security and Development Cooperation Act (Iran); The Cuban Democracy Act (Cuba); the Cuban Liberty and Democratic Solidarity Act (Cuba); The Antiterrorism and Effective Death Penalty Act (Cuba, North Korea, Iran, Syria and Sudan); the Foreign Narcotic Kingpin Designation Act; the Syria Accountability and Lebanese Sovereignty Act; and more.

[17] Under OFAC regulations, providing a service may be construed as providing something of value even if no payment is made. This potentially includes many activities that occur in a university environment, such as the exchange of unpublished data or research results or testing/analysis of samples with colleagues in certain sanctioned countries.

[18] As of January 2023, OFAC only limits travel to Cuba. Travel restrictions were eased significantly under the Obama administration but were not removed entirely, and the Trump administration made additional changes to some travel restrictions and tightened recordkeeping requirements. Research Security and Compliance must be consulted prior to any University travel to Cuba to ensure compliance with the most current regulations.

Korea, and Syria. In more recent years, OFAC has also begun to apply sanctions to specific regions of countries. These are the Crimea, Donetsk, and Luhansk regions of Ukraine. While U.S. policy is normally to deny export licenses for exports to geographies under comprehensive sanctions, exceptions do exist that permit exports or the provision of services in specific circumstances through the usage of general licenses.

The electronic version of OFAC sanctions programs shall be, for the purposes of this manual, the appropriate authority for the contents of the sanctions. This is available through the Electronic Code of Federal Regulations. Additional guidance is available on the OFAC website.

B. Targeted Sanctions

As part of its enforcement efforts, OFAC publishes lists of individuals and companies owned by, controlled by, acting for, or acting on behalf of targeted countries. OFAC also lists individuals, groups, and entities, such as terrorists and narcotics traffickers, designated under selective sanctions programs that may not be tied to specific countries. OFAC publishes the names of selected parties in lists, such as the "Specially Designated Nationals and Blocked Persons List (SDN List)" and the "Non-Specially Designated Nationals and Blocked Persons List (Non-SDN List). OFAC lists can be searched online through the Sanctions List Search; however, there are additional lists that need to be reviewed prior to engaging in a transaction with a foreign party (see VII below.

While most sanctions are administered by OFAC, other government agencies have additional embargos and jurisdiction over certain export prohibitions. BIS maintains lists of designated persons and entities to whom exports may require a license or be otherwise restricted. BIS also has implemented comprehensive embargoes against certain countries and limited embargoes for specific categories of items to countries subject to United Nations Security Council arms embargoes. DDTC also maintains a list of embargoed countries (see III.D above).

C. Authorization to Export, Provide Services, or Conduct Other University Business Under OFAC Sanctions

There are many OFAC sanctions programs, based on a unique set of foreign policy priorities and each program is distinct and different. Some programs are comprehensive in scope, prohibiting most unlicensed activities. Other programs may be more focused and target a specific activity or activities. Additionally, because sanctions are political in nature and utilized to bring about changes in behavior, OFAC regulations are constantly being revised. University employees must contact Research Security and Compliance prior to attempting to apply the sanctions regulations.

Each sanctions program specifies the activities that are exempt from prohibition and the activities that are permissible under a general license (without requiring government approval). Activities that are not exempt or do not fall under a general license may be allowed under a specific license upon application by the University and approval by OFAC or the appropriate agency. If clarification by OFAC or another agency or a license to conduct the activity is necessary, Research Security and Compliance will file the request on behalf of the University. University personnel may not independently file a license application to conduct University-related business.

VII. Restricted Parties and Parties of Concerns

As referenced in prior sections, the U.S. Departments of State, Commerce, and the Treasury maintain lists of people, companies, universities, organizations etc., with which University activities must be limited. U.S. persons (wherever located) and foreign persons located in the U.S. may be restricted from entering certain types of transactions with persons or entities on those lists.

To ensure compliance with regulations and laws, and to protect the integrity and reputation of the University, as a matter of general policy the University will not engage in exports or transactions with parties found on these lists and subject to these restrictions. The University reserves the right to restrict activities with additional

parties based on emerging U.S. Government legislative/administrative guidance or when it is otherwise in the best interests of the University.

All lists must be screened to ensure that the University does not engage in a transaction with a listed entity. The University has purchased software for Research Security and Compliance to expedite screening of all government lists of restricted parties. University employees must contact Research Security and Compliance prior to attempting to search these lists. University personnel outside Research Security and Compliance may be granted access to this software on a case-by-case basis and shall follow all policies and procedures implemented with its use.

VIII. Penalties for Violations

A. General Overview

Any person or entity that:

1) Brokers, exports, or attempts to export a controlled item without prior authorization or in violation of the terms of a license; or
2) Exports goods or services, engages in financial transactions, or otherwise acts contrary to or in violation of sanctions regulations, may be subject to criminal or civil penalties, or both. Typically, one unauthorized export can result in multiple violations; therefore, a series of violations occurring over a period of time could result in exorbitant fines, criminal prosecution and jail time, or both. Additionally, organizations facing export control violations risk having their export privileges revoked and being debarred from receiving federal funding, in addition to the reputational damage they will incur.

B. Defense Export Violations

The Arms Export Control Act (AECA), the implementing legislation for the ITAR, provides that willful (criminal) violations can incur fines of up to $1,000,000 per violation, twenty years of imprisonment, or both. In addition, the Secretary of State may assess civil penalties, which can exceed $1,000,000 per violation,[19] in addition to, or instead of, any other penalty. The articles exported or imported as a result of a violation, and any vessel, vehicle or aircraft involved in such violation, are subject to seizure. DDTC may also order that the violator be debarred, or prohibited from exporting defense items, for a period of time. The U.S. Department of State will also publish a press release regarding the violation, leading to negative publicity for the offender.

C. Dual-Use/Commercial Item Exports and Anti-Boycott Violations Under the EAR

The Export Control Reform Act of 2018, the primary statutory authority for the EAR,[20] establishes fines for export violations for items subject to the EAR and anti-boycott violations, which can be up to $1,000,000 per violation in criminal cases, and exceed $300,000 per violation or twice the value of the transaction (whichever is greater) in most administrative (civil) cases.[21] In addition, criminal violators may be sentenced to prison time to up 20 years. Administrative penalties may include the denial of export privileges that would prohibit an individual or a U.S. company from engaging in a wide variety of activities involving any item subject to the EAR that has been or will be exported from the United States for a designated period of time.

D. Violations of Sanctions Regulations

The potential civil penalties that may be assessed in the event of a violation may change across the various OFAC sanctions programs and can exceed $1,000,000 depending on the specific program an entity or person under which a violation occurs. Those who violate sanctions imposed under the International Emergency

[19] Under the ITAR, violations of different provisions of the AECA will carry different penalties. Violations associated with the improper export of USML items currently carry a civil penalty not to exceed $1,272,251 (22 CFR § 127.10)

[20] For the complete legal authority for the EAR, including the Export Administration Act of 1979, the International Emergency Powers Act, as amended, other statutory provisions related to the EAR, and Associated Executive Orders and other Presidential documents, see https://www.bis.doc.gov/index.php/documents/regulations-docs/2263-legal-authority-for-the-export-administration-regulations-1

[21] Under the Ear, the maximum penalty is the greater of the listed fine or five times the value of the illegal transaction.

Economic Powers Act (IEEPA), which is the primary sanctions regime the University is most likely to encounter, may be subject to a maximum civil penalty of $284,582 per violation, except for exports to Cuba or North Korea under the Trading with the Enemy Act (TWEA). Violations of the TWEA are subject to a maximum civil penalty of $85,236 per violation. The U.S. Government can also criminally prosecute willful violations and in such circumstances, fines may reach $1,000,000 per violation and imprisonment of up to 20 years. In addition, where there is egregious conduct by the offender, BIS (who assists OFAC in enforcing sanctions) may suspend export privileges.

E. Voluntary Disclosures

Exports and sanctions regulations are complex, and accidental or inadvertent violations may occur. DDTC, BIS, and OFAC all have mechanisms in place for violations to be self-disclosed. These agencies will consider a voluntary disclosure (or lack thereof) as a mitigating or aggravating factor, respectively, when determining whether to assess penalties for a violation.

Mitigating factors include whether:

1) The disclosure was made voluntarily;
2) The violation was a first offense;
3) Compliance procedures were implemented;
4) Steps were taken to improve compliance after discovery of violations; and
5) The incident was unintentional, resulting from a mistake of fact or a good faith misapplication of the laws.

Aggravating factors include:

1) Willful or intentional violations;
2) Failure to take remedial action after discovery;
3) Lack of a compliance program;
4) Deliberate efforts to hide or conceal a violation.

The University encourages its employees to come forward with questions or concerns about potential export or sanctions violations. Employees can report export compliance concerns directly to Research Security and Compliance. Anonymous reporting is available to University personnel through the "Integrity and Accountability Hotline", which can be accessed by calling a toll-free number, 1-866-447-9821, or navigating to https://secure.ethicspoint.com/domain/media/en/gui/40803/index.html?123.[22] All efforts will be made to investigate credible claims of potential violations and provide appropriate protections to the individual(s) filing such claims, per UM Policy HR-520[23] and other policies.

IX. Key Issues in University Research

A. Deemed Exports

Both the ITAR and EAR place controls on deemed exports. A deemed export occurs when controlled technical data (ITAR), technology (EAR)[24], or software source code (EAR) is released or otherwise transferred to a foreign person in the United States. In other words, technical data, technology, or source code does not need to cross the physical borders of the United States to be considered an "export". Deemed exports may be made orally, visually, virtually, or by other means, such as:

- Demonstrations;
- Oral briefings;

[22] For more information, contact the hotline to ask how the hotline works or access the following "frequently asked questions" (FAQs) link: https://secure.ethicspoint.com/domain/media/en/gui/40803/faq.pdf

[23] UM System Human Resources Manual. HR-520 Reporting University-Related Misconduct. Created 09/01/2007, at https://www.umsystem.edu/ums/rules/hrm/hr500/hr520

[24] Under the EAR, the deemed export rule does not apply to physical items/products. Technology is information necessary to "develop", "produce", or "use" a physical item. "Use is defined as "operation, installation, maintenance, repair, refurbishing, and overhaul". All 6 elements must be present to trigger "use" technology.

- Telephone calls or messages;
- Collaborations with foreign colleagues;
- Laboratory or plant visits;
- Faxes or letters;
- Design reviews;
- Exchange of electronic communications;
- Hand-carried documents, hardware, or drawings; or
- Posting non-public data on the Internet or Intranet.

The issue of deemed exports is particularly relevant in university research where information is exchanged openly and broadly. While a university may only occasionally be involved in the shipment abroad of tangible items, most often faculty and students are engaged in teaching and research. Whenever teaching or research involves controlled equipment or technology and foreign students or researchers, export compliance management may be needed even when those activities are occurring solely in the United States.

B. U.S. Persons and Foreign Persons

The University of Missouri System is a public institution with a large population of foreign students, staff, visiting scholars, and faculty who are engaged in all aspects of the University's operations and are significant participants in the University's research mission.

Under export control regulations,[25] a U.S. person is defined as a U.S. entity or a U.S. citizen, a person lawfully admitted for permanent residence in the United States (i.e., green card holder), or a person who is a protected individual under the Immigration and Naturalization Act (i.e., certain classes of asylees). Generally, a U.S. person may be engaged in export-controlled activities without a license.

A foreign person is defined as anyone who does not meet the definition of a U.S. person. When making an export license determination, BIS considers the country(ies) of which a foreign person currently holds citizenship or permanent residence status. DDTC, on the other hand, evaluates all countries (past AND present) of which a foreign person has held citizenship or permanent residence status.

C. Controlled Unclassified Information

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. CUI is specifically information provided to the University by the government or information generated by the University on behalf of the government. There are approximately 20 categories of CUI, which include privacy information, export controls, proprietary business information, and others.[26] DoD contracts require CUI to be "marked or otherwise identified in the contract, task order, or delivery order" before being provided to, or generated by, the University. In addition, CUI may also be subject to export control regulations and may be subject to data security requirements that exceed those required by export control regulations.

D. Information Not Subject to or Excluded from Export Controls

Most University research and educational activities are not subject to export controls, or—if controlled—do not require licensing. Both the ITAR and EAR have special provisions relating to information that is not subject to export controls, including limited exclusions regarding the release of information in the context of university research and educational activities. The sanctions regulations also have exceptions for certain "information and informational materials".

[25] Note that the difference for a U.S. and foreign person differ for purposes of the OFAC sanctions. Please contact Research Security and Compliance for assistance with the application of any sanctions program.
[26] National Archives and Records Administration. CUI Categories. Retrieved November 29, 2022, from https://www.archives.gov/cui/registry/category-list

1) Publicly Available Information

The ITAR and the EAR do not control information that is published and/or otherwise generally accessible or available to the public. While both regulatory regimes are moving toward a more common definition of "published"[27] and "public domain"[28], the ITAR and the EAR vary in the specific information that qualifies as publicly available and each must be consulted as appropriate before making any determination as to whether information is publicly available and thus exempt from control.

In general, information that has been made available to the general public with no restrictions on access or further dissemination is not subject to export or sanctions controls. This includes, but is not limited to, information that is available:

- Through sales at newsstands and bookstores, or through subscriptions available with no restrictions on who may obtain the information;
- At libraries open to the public or from which the public can obtain documents;
- Through patents or published patent applications available at any patent office; or
- Through unlimited distribution at a conference, meeting, seminar, trade show, or exhibition that is generally open and accessible to the interested public.[29]

2) Educational Information

In general, University faculty do not need to worry about information they present in the classroom being subject to export controls. Both the ITAR and the EAR exempt from control general educational information related to items listed on the USML or CCL.

ITAR

The definition of 'technical data' does not include "information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges, and universities."[30]

EAR

Information and 'software' that "are released by instruction in a catalog course or associated teaching laboratory of an academic institution" are not subject to the EAR.[31] The information will not be controlled even if the course contains recent and unpublished results from laboratory research, so long as the university did not accept separate obligations with respect to publication or dissemination of those results (e.g., a contractual publication restriction).

The transfer or technology associated with *most* EAR-controlled equipment in an educational setting generally does not create a deemed export concern.[32] However, foreign persons may not use or operate ITAR-controlled equipment ("defense articles"), even in the context of an educational setting, without obtaining a license prior to use/operation.[33] Questions about the applicability of export control regulations regarding equipment in a teaching lab must be directed to Research Security and Compliance.

---

[27] Export Administration Regulations. 15 CFR § 734.7 Published. Retrieved November 29, 2022, from https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734/section-734.7

[28] International Traffic in Arms Regulations. 22 CFR § 120.34 Public Domain. Retrieved November 29, 2022, from https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/subpart-C/section-120.34

[29] Under the ITAR, presentations at a conference, meeting, seminar, etc. only fall in the public domain for domestic, U.S.-based events. Presentations abroad may still require a license and Research Security and Compliance should be consulted.

[30] International Traffic in Arms Regulations. 22 CFR § 120.33 Technical data. Retrieved November 29, 2022, from https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/subpart-C/section-120.33

[31] Export Administration Regulations. 15 CFR § 734.3 Items subject to the EAR, paragraph (b)(3)(iii). Retrieved November 29, 2022, from https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734/section-734.3

[32] Under the EAR, if a student "is receiving technology in the context of instruction in a catalog course (or associated teaching laboratories) of an academic institution", then that technology is not subject to the EAR and no license is required for the release of that technology. See 15 CFR § 734.3(b)(3)(iii). Deemed Export FAQs are available on the BIS website at https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports/deemed-exports-faqs, retrieved May, 22, 2022.

[33] See the Definitions at the end of this document for definitions of technical data, defense service, export, and release.

3) Results of Fundamental Research

National Security Decision Directive (NSDD) 189, *National Policy on the Transfer of Scientific, Technical and Engineering Information*, was issued on September 21, 1985, and affirmed on November 1, 2001. NSDD 189 provides the generally accepted definition of fundamental research, which provides the basis for export compliance decisions relative to 'fundamental research' exclusions provided under both the ITAR and the EAR.

As a result of Export Control Reform, the EAR also now includes a definition of fundamental research that is similar to NSDD 189.

> *Fundamental research means research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons.*[34]

The ITAR also provides a definition of fundamental research and, while slightly different, is very similar to that in NSDD 189.

> *Fundamental research is defined to mean basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. University research will not be considered fundamental research if:*
>
> *(i) The University or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity, or*
>
> *(ii) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable.*

One key area in which the two definitions are currently different is that there is a requirement under the ITAR that research must be performed at accredited institutions of higher learning in the United States to qualify as fundamental research. Under the EAR, fundamental research may occur at facilities other than accredited institutions of higher learning in the United States.

Both the ITAR and the EAR are clear that fundamental research only applies to the information (ITAR) or technology (EAR) that results from research and does not apply to physical "things" (i.e., prototypes, equipment, etc.) that arise through a research project. Fundamental research also does not apply to research conduct or the inputs to a research project. If in the conduct of a project, a foreign person may be required to operate a controlled lab instrument or engage in other activities requiring government approval, a license may be required even if the research *results* are intended to be openly disseminated. Likewise, if the research project is dependent upon the receipt of controlled technology, such as third-party proprietary information that is subject to the ITAR or the EAR, a license may be required before it can be released to a foreign person, even if the research otherwise qualifies as fundamental research.

University-based research is not considered fundamental research if UM or its researchers accept restrictions on the publication of or access to scientific and technical information resulting from the project or activity. This includes any informal "side deals" between project staff and a sponsor that would remove the fundamental research exclusion, which is in violation of UM policy.

[34] Export Administration Regulations. 15 CFR § 734.8 "Technology" of "software" that arises during, or results from, fundamental research, paragraph (c) Fundamental research definition. Retrieved November 29, 2022, from https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734/section-734.8

Prepublication Review
While the ITAR does not currently address prepublication review, the EAR is useful in interpreting the limitations on fundamental research.[35] The EAR instructs that prepublication review by a sponsor of university research solely to ensure that the publication will not inadvertently divulge proprietary information that the sponsor has initially furnished, or compromise patent rights, does not constitute a restriction on publication. Such a review must also be conducted in a reasonable timeframe and not cause more than a "temporary delay" in publication. BIS has also published FAQs to guide exporters understanding of prepublication review.[36]

Access Restrictions vs. Funding Restrictions
On occasion, a research sponsor may limit recipients of funds associated with the award to U.S. citizens or U.S. persons. Often, these restrictions are associated with federally funded training programs whose citizenship restrictions result from a policy mandate to enhance U.S. capabilities or manpower in certain areas of science, engineering, or medicine. These types of funding restrictions are not access restrictions imposed as "specific national security controls" if foreign persons are otherwise permitted to participate in the project and there are not publication restrictions associated with the project. Examples of funding restrictions that do not nullify fundamental research are NIH and NSF training grants.

Additionally, NASA also has restrictions on funding activities with China.[37] NASA funds may not be used to "participate, collaborate or coordinate bilaterally in any way with China or any Chinese-owned company". This funding restriction is a policy decision about how funds coming to the university can be used and not necessarily an export control that restricts a Chinese citizen from participating on a NASA-funded project. "'China' or 'Chinese-owned' means the People's Republic of China, any company owned by the People's Republic of China, or any company incorporated under the laws of the People's Republic of China. Chinese universities and other similar institutions are considered to be incorporated under the laws of the PRC and, therefore, the funding restrictions apply to grants and cooperative agreements that include bilateral participation, collaboration, or coordination with Chinese universities."

The ability to apply the fundamental research exclusion to research results is based on contractual requirements and is a highly specialized determination. University researchers may not apply this exclusion independently for any University-related activity. Please contact Research Security and Compliance for assistance.

4) Release to "Bona Fide, Full-Time Employees"

In very limited circumstances, under both the ITAR[38] and the EAR[39], University personnel may be permitted to release controlled, unclassified technical data in the U.S. to a foreign person. Application of this exemption is specific and dependent upon meeting a specific set of requirements:

i) The foreign person is a bona fide and full-time, regular employee of the University;

[35] Export Administration Regulations. 15 CFR § 734.8 "Technology" of "software" that arises during, or results from, fundamental research, paragraph (b) Prepublication review. Retrieved November 29, 2022, from https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734/section-734.8
[36] Bureau of Industry and Security. (2016, September 1). *Revisions to Definitions in the Export Administration Regulations: Frequently Asked Questions (FAQs).* https://www.bis.doc.gov/index.php/documents/compliance-training/export-administration-regulations-training/1554-ear-definitions-faq/file
[37] National Aeronautics and Space Administration. (2012, February 16). Procurement Class Deviation: Class Deviation Implementing NASA Restrictions on Funding Activity with the Peoples Republic of China (PRC). https://www.hq.nasa.gov/office/procurement/regs/pcd/pcd12-01A.pdf
[38] International Traffic in Arms Regulations. 22 CFR § 125.4 Exemptions of general applicability, paragraph (b)(10). Retrieved November 29, 2022, from https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-125/section-125.4
[39] Export Administration Regulations. 15 CFR § 740.13 Technology and software - unrestricted (TSU), paragraph (f) Release of technology and source code in the U.S. by U.S. universities to their bona fide and full-time regular employees. Retrieved November 29, 2022, from https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-740/section-740.13

ii) The employee's permanent abode throughout the period of employment is in the United States;
    a. Note: The requirement that the employee's "permanent abode throughout the period of employment" is understood to mean "residence throughout the period of employment." Employees who return home for short periods of time (for example, over Winter Break) are not disqualified from qualifying as an "employee" for [these] purposes."[40]
iii) The employee is not a national of an embargoed country;[41, 42] and
iv) The University informs the employee in writing that the disclosed information, technology, technical data, source code, etc. may not be transferred to other foreign persons without prior government approval.

Foreign students, postdoctoral associates, and visiting scholars will generally not qualify for this exemption. University employees may not apply this exemption independently for any University-related activity. Contact Research Security and Compliance for assistance.

5) Informational Materials & Publishing Activities[43]

OFAC sanctions permit, without requiring a license, the export or import of information and informational materials, to *most* sanctioned countries. This does not permit the export of controlled technical data, which would still require a license from DDTC or BIS, nor the export/import of "information and informational materials not fully created and in existence at the date of the transaction." In addition, "the substantive or artistic alteration or enhancement of informational materials' is a service requiring an OFAC license unless engaging in certain peer review or style and copy-editing activities. None of these exceptions apply when engaged directly with sanctioned governments, though in limited circumstances OFAC may allow these activities with an academic institution that would otherwise be considered an agency or instrumentality of a sanctioned government.

University employees may not apply these exemptions independently for any University-related activity. Please contact Research Security and Compliance for assistance.

E. Remote Learning

Throughout the UM System, there are opportunities for students to engage in online learning courses. Generally, these activities should not raise concerns. However, if students are located in comprehensively sanctioned jurisdictions, sanctions compliance concerns will arise. General Licenses within many of the sanctions programs authorize the University to recruit faculty, staff, and students from these sanctioned jurisdictions, and once a person has been granted a visa, they are authorized to come to the U.S. and participate in activities consistent with their visa. Until they have arrived in the U.S., they may not be enrolled in online learning courses.

University personnel wishing to enroll a student located in a comprehensively sanctioned jurisdiction in an online learning course must first contact Research Security and Compliance and receive approval prior to enrollment in online learning courses.

[40] Association of University Export Control Officers. (2014, April 28). Bona fide, Full-time Employees (BFE). http://aueco.org/wp-content/uploads/2016/04/bonafideemployeeauecoguidance.pdf
[41] International Traffic in Arms Regulations. 22 CFR § 126.1 Prohibited exports, imports, and sales to or from certain countries. Retrieved November 29, 2022, from https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-126/section-126.1
[42] Export Administration Regulations. 15 CFR § 740 Supplement No. 1, Country Group D:5. Retrieved November 29, 2022, from https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-740/appendix-Supplement%20No.%201%20to%20Part%20740
[43] Office of Foreign Assets Control. (2016, October 28). *Guidance on Certain Publishing Activities.* https://home.treasury.gov/system/files/126/guidance_on_certain_publishing_activities.pdf

F. Telework

Per HR Policy HR-522 Telework Arrangements[44], "telework" is a work arrangement in which some or all of the work is performed from home or another off-site location on a regular basis. Telework arrangements include both fully remote and hybrid arrangements. When University devices and equipment are taken out of the country and when University resources are accessed remotely from outside the country, export control and sanctions concerns may arise.

University employees wishing to telework from a foreign location must work with Research Security and Compliance to address export control and sanctions risks. Human Resources will forward Telework Agreements with proposed foreign locations to Research Security and Compliance for review and approval as part of the overall Telework Arrangement approval process.

G. Use of Export Controlled or Restricted Research in Graduate Student Theses or Dissertations

The University of Missouri-Columbia's "Electronic Thesis & Dissertation Basics"[45] prohibit graduate students from using research data or other content that could be subject to publication or disclosure restrictions as the basis for their theses and/or dissertations. PIs must take this into consideration and discuss with graduate students before placing them on restricted research projects. Restricted research is permitted for graduate students engaged in nonthesis or nondissertation research.

The remaining three institutions within the University of Missouri System, University of Missouri-Kansas City, Missouri University of Science and Technology, and the University of Missouri-St. Louis, have no such policies in place.

H. Classified Research

The University of Missouri System has a Facility Clearance (FCL), with the University of Missouri-Kansas City holding a subsidiary Facility Clearance (FCL). These clearances come with obligations to safeguard classified, controlled unclassified information (CUI), and other export-controlled items and technology. The University complies with the National Industrial Security Operating Manual (NISPOM) and the University of Missouri System Standard Practice Procedures for Industrial Security (SPP) when performing classified research.

Due to the overlap with the ITAR[46], classified research projects will generally require the implementation of a Technology Control Plan (see Section VIII.E)

This Program is also intended to satisfy the University's obligations under the NISPOM to document in writing and implement procedures to control access by foreign persons to all export-controlled information, classified or unclassified.[47]

X. University of Missouri System Export Control and Sanctions Compliance Processes

The University of Missouri System has implemented Collected Rules and Regulations (CRR) 430.020 which incorporates this Export Compliance Management Program (ECMP), by reference.

---

[44] HR-522 Telework Arrangements. https://www.umsystem.edu/ums/rules/hrm/hr500/hr522

[45] University of Missouri Graduate School. *Electronic Dissertation & Thesis Basics.* Retrieved November 29, 2022, from https://gradschool.missouri.edu/current-students/thesis-dissertation/thesis-dissertation-guidelines/electronic-dissertation-thesis-basics/

[46] USML Category XVII *Classified Articles, Technical Data, and Defense Services Not Otherwise Enumerated* covers "all articles, technical data and defense services relating thereto, that are classified in the interests of national security and that are not otherwise enumerated on the U.S. Munitions List."

[47] NISPOM 10-509

A. Processes and Standard Operating Procedures

Each institution within the University of Missouri System shall establish Standard Operating Procedures to align with the processes outlined in this Export Compliance Management Program (ECMP).

B. Commitment to Compliance

"The mission of the University of Missouri System, as a land-grant university and Missouri's only public research and doctoral-level institution, is to achieve excellence in the discovery, dissemination, preservation and application of knowledge. With an unwavering commitment to academic freedom and freedom of expression, the university educates students to become leaders, promotes lifelong learning by Missouri's citizens, fosters meaningful research and creative works, and serves as a catalyst for innovation, thereby advancing the educational, health, cultural, social and economic interests to benefit the people of Missouri, the nation, and the world".[48] While the University of Missouri System endorses the principles of freedom of inquiry and open exchange of knowledge, the University System intends to comply with export control and sanctions regulations. The University System has adopted both of these principles into its Collected Rules and Regulations[49] and intends to comply with export control and sanctions regulations.

The University System reiterates a commitment to academic freedom; welcomes the contributions of international faculty, staff, students, and visitors; and asserts that research conducted by the faculty, staff, and students is in the public domain and considered fundamental research. Most research throughout the System is, therefore, exempt from these regulations. However, where export control and sanctions regulations apply to university activities, or a University within the System accepts restricted research projects, full compliance with the law is required. See our Export Compliance Commitment Statement.

The University of Missouri System is committed to export controls and sanctions compliance, and Research Security and Compliance is tasked with advising and assisting the University System community in its compliance obligations. More information and resources regarding export controls, sanctions, and other regulations that impact University activities can be found on the Research Security and Compliance website[50] or by contacting Research Security and Compliance.

C. Responsibility for Export Control and Sanctions Compliance

Responsibility for compliance with these regulations rests in all University System personnel; however, there are certain authorities and job functions that have specific procedural requirements helping the University System maintain compliance.

1) Empowered Official

As a part of the DDTC registration process, there is a designated Empowered Official at the University System who has the authority to represent the University System before DDTC in matters related to registration, licensing, CJ requests, or voluntary disclosures. While certain oversight functions may be delegated to others, only the designated Empowered Officials have the power to bind the University System in any proceeding before DDTC. The designated Empowered Official for the University of Missouri System and all its universities is the Director of Research Security and Compliance.

2) Research Security and Compliance

Research Security and Compliance is led by the UM System Director and delegated compliance officers embedded at each of the institutions who have responsibility for their institution's compliance with export control and sanctions regulations. More information about the structure of the UM Research Security and Compliance Team can be found in CRR 430.020. Research Security and Compliance has the authority and the responsibility for the implementation of the University System's Export Compliance Management Program by:

- Identifying University activities that are impacted by export control and sanctions regulations;

[48] https://www.umsystem.edu/about-us/weareum
[49] CRR 430.020 Export Control and Sanctions Compliance
[50] https://www.umsystem.edu/ums/ecas/research

- Recommending processes and procedures that strengthen compliance to senior leadership in order to gain support;
- Maintaining the University of Missouri System CRR related to export controls and sanctions compliance;
- Developing and implementing systemwide processes to ensure that the University remains in compliance with export controls and sanctions regulations and to ensure that each of the four institutions within the University of Missouri System are aligned in their approaches to addressing these risks;
- Ensuring that each institution within the University of Missouri System has standard operating procedures in place that align with the CRR and this ECMP;
- Educating the University community about export control and sanctions regulations and University compliance procedures;
- Monitoring and interpreting legislation;
- Working with others on campus to cultivate a culture of compliance;
- Assisting investigators, project staff, and university offices when the work they are doing or plan to do is subject to export control and sanctions regulations;
- Implementing appropriate measures to limit unauthorized access to export-controlled materials (see Section X.E.);
- Seeking assistance from the Office of General Counsel, as deemed necessary, regarding classification, filing of license applications, and voluntary self-disclosures;
- Responding to, and sometimes driving gap analyses, audits, investigations, and their findings to strengthen the export compliance and sanctions program.

3) University Leadership

Academic and administrative vice chancellors for research, deans, directors, and department heads share the responsibility of overseeing export control and sanctions compliance in their respective colleges, schools, departments, centers, or institutes and supporting the export compliance and sanctions program in implementing procedures as deemed necessary by Research Security and Compliance for export control and sanctions compliance.

4) Office of Information Technology

The Office of Information Technology works with Research Security and Compliance to ensure that necessary data security CRRs, policies, processes, and procedures are in place ensuring the security of data subject to export control and sanctions regulations. They collaborate with Research Security and Compliance and Principal Investigators to ensure System Security Plans are implemented that meet the data security needs of researchers and to ensure that export control and sanctions regulations are followed and aligned with technology control plans.

5) Sponsored Programs

The sponsored programs offices at each campus provide support and assistance to the export compliance and sanctions program in identifying and managing restricted research activities. They identify and notify RSC of solicitations, proposals, or agreements involving any of the red flags outlined in their institutions' procedures.

6) Visa Processing Offices

Form I-129, Petition for a Nonimmigrant Worker, Part 6 requires the University of Missouri to provide a certification regarding the release of controlled technology or technical data to foreign persons in the United States. This section of the form is required only for H-1B, H-1B1 Chile/Singapore, L-1, and O-1A petitions. As such, offices within the University of Missouri System responsible for signing this document engage Research Security and Compliance prior to applying their signature. Each institution within the University of Missouri System will have specific procedures in place outlining what information to provide to Research Security and Compliance so that an assessment can be performed. Research Security and Complianec will advise how Section 6 of Form I-129 must be completed and will apply for any deemed export licenses necessary for the

employee, in collaboration with the visa processing office, the sponsoring faculty member, and the Office of General Counsel.

7) University Shared Services

The Accounts Payable (AP) Shared Services Center provides transactional processing for the four campuses comprising our University of Missouri System. As such, departments may focus on their core missions while they provide human capital and systems to ensure their payments are made in a timely and accurate manner while adhering to university policy, state law, and federal regulations. These federal regulations include responsibilities related to export controls and sanctions which may arise when working with and paying vendors and suppliers. University Shared Services, in cooperation with Research Security and Compliance, has developed the Sanctions and Restricted Parties business policy[51] outlining their responsibilities which support all institutions within the UM System.

8) Human Resources

Within the Human Resources Manual resides the Telework Arrangements policy[52]. Because teleworking from locations outside of the United States raises export controls and sanctions risks, Human Resources will ensure that all requests for University employees to work remotely from outside the U.S. are sent to Research Security and Compliance for review and approval.

9) Principal Investigators and Researchers

Principal Investigators (PIs) must carefully review the information on export controls and sanctions compliance provided in this document, on the University of Missouri System website, and on their local institution's website. They must contact Research Security and Compliance with questions or to request additional training.

PIs and researchers have the best understanding of their research and thus are best suited to advise Research Security and Compliance how particular technology, data, or information is classified by export control regulations. The PI and researchers may not start research until a fully executed agreement is in place with the sponsoring party.

PIs and researchers assist in the development of Technology Control Plans (TCPs) and Systems Security Plans (SSPs), attend export control training (as required by RSC), sign acknowledgments regarding TCPs, abide by the terms of their TCPs, notify Research Security and Compliance if they receive direction from a federal or industry sponsor that is contrary to their TCP, and work with Research Security and Compliance to update TCPs as needed.

PIs and researchers must notify Research Security and Compliance immediately if they know or suspect that a violation of their TCP, their institution's procedures, the ECMP, the CRR, or export control and sanctions regulations has or may occur.

10) All University Personnel

All university personnel must familiarize themselves with export control and sanctions regulations. Faculty sponsoring visa applicants must ensure that export control and sanctions regulations are followed for all activities of a visa applicant. All University personnel must report known or suspected violations of export control and sanctions regulations, the CRR, and/or the ECMP to Research Security and Compliance immediately.

D. Analysis of Sponsored Projects

An analysis must be performed when a PI submits a proposal, receives an award, or changes the scope of an existing project. The University of Missouri System recommends that each university implement the following RSC reviews, at a minimum:

[51] https://www.umsystem.edu/ums/policies/finance/sanctions-and-restricted-parties
[52] https://www.umsystem.edu/ums/rules/hrm/hr500/hr522

- International engagements, such that RSC can perform a restricted party screening
- Agreements with Department of Defense (DoD), DoD component agencies[53], Department of Energy (DOE), NASA, or an intelligence agency (including flow throughs)
- Foreign person restrictions that would limit the participation of non-U.S. persons or non-U.S. citizens in a project, including any sponsor requirement to pre-approve foreign participation or a specific "U.S. persons only" requirement
- Publication restrictions unrelated to third-party proprietary or confidential information that prohibit or otherwise require sponsor approval of any publications resulting from or related to a project
- Sponsor requests for our Military Critical Technical Data Agreement (DD-2345)
- Security language such as a DoD Contract Security Classification Specification (DD-254) or other indications in the award that the project will be classified for national security purposes, or that project staff will be required to obtain a Personnel Security Clearance (PCL) in order to perform work on the project
- Export control markings (i.e., Controlled Unclassified Information / CUI, Controlled Technical Information / CTI, Covered Defense Information / CDI) appear on the solicitation, proposal, or award documents or will be required on technical documents, reports, publications, etc.
- Notification from a 3rd party that they will be providing the University with controlled technology

At no time shall work begin on a project without a signed agreement in place and an agreement will be signed only after all export control and sanctions requirements are mitigated. Exceptions to this may be granted in writing by the Director of Research Security and Compliance on a case-by-case basis.

E. Technology Control Plans

Research Security and Compliance at each relevant institution will work with PIs to develop and implement Technology Control Plans (TCPs) for restricted research projects to secure controlled technology from access by unlicensed foreign persons. TCPs may also be appropriate when other national security requirements need to be met on a research project. TCPs will include the following components:

- Physical Security Plan
- Information Security Plan
- Personnel Security Plan
- Training/Awareness Plan
- Auditing/Monitoring Plan

All project personnel will be briefed on the procedures authorized under the TCP, certify agreement to comply with all security measures outlined in the TCP, and have that certification authorized by Research Security and Compliance before being allowed access to a restricted research project under a TCP. Research Security and Compliance will require the implementation of a TCP in the following circumstances:

- USML item will be stored at any University of Missouri location;
- USML technical data (including software) will be accessed or stored by the University;
- CCL source code will be accessed or stored by the University;
- CCL technology will be accessed or stored by the University;
- CCL items, if University personnel may work with the item such that technology would be revealed;
- Contractual requirements to obtain sponsor approval prior to engaging non-U.S. researchers on a project, which most commonly appear in DOE contracts applying either DEAR 952.204-71 Sensitive Foreign Nations Controls or DOE O 142.3; and/or
- Requirements to comply with NIST 800-171 or NIST 800-172 which generally appear in DoD and DOE contracts for safeguarding Controlled Unclassified Information (CUI) or one of the categories of CUI[54].

[53] https://samm.dsca.mil/glossary/dod-components
[54] https://www.archives.gov/cui/registry/category-list

F. System Security Plans

In order to accept some contracts funded by the U.S. Department of Defense (DoD) subject to Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 that has not otherwise been scoped and negotiated to be fundamental research, the University must agree to implement a System Security Plan (SSP) for the information security standards in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 to safeguard systems and networks that process, store, or transmit covered defense information (CDI). Non-DoD contracts or awards will not contain the DFARS clause but may still require compliance with similar data security requirements.

In order to demonstrate implementation of the security requirements, University personnel must work with the UM Information Technology Security Office to ensure they are provisioned access to a space that meets these data security requirements. Research Security and Compliance will engage the Information Technology Security Office in the TCP and SSP implementation process. Historically, the University has implemented limited in-house solutions to these safeguarding requirements. As of January 2023, UM has procured the Microsoft Azure GCC High environment to safeguard CUI and export-controlled information, and GGC High is the preferred safeguarding solution. However, there may be exceptions to the use of GGC High based on the specific research needs of an individual project or if a researcher is already using one of the in-house solutions, as long as the solution is fully compliant. Research Security and Compliance and the Information Technology Security Office will ensure that a System Security Plan (SSP) describing how the University meets the required data security controls is on file. Federal agencies may require that an SSP be submitted in a proposal package or prior to award, and they may consider the University's SSP in the contract selection process. Like TCPs and other compliance documents, the SSP must be in place prior to the release of funds.

To monitor the effectiveness of a contractor's SSP, the DoD has implemented a requirement that contractors conduct a self-assessment of their NIST SP 800-171 implementation[55]. The self-assessment will be conducted by the UM Information Technology Security Office and will generate a "score" based on the number of controls that have been implemented. The name of the SSP, self-assessment date and score, and other information will be uploaded into the Supplier Performance Risk System by Research Security and Compliance. As a consideration in the award process, the DoD will evaluate the score generated by the self-assessment process[56].

G. Deemed Export Attestation

The U.S. Citizenship and Immigration Services (USCIS) requires that immigrant visa petitioners complete a "deemed export attestation" during the processing of H-1B, H-1B1 Chile/Singapore, L-1, and O-1A visa applications for foreign employees being hired in specialty occupations. Specifically, the University must evaluate whether a deemed export license will be required before a foreign employee on such a visa can access controlled products or technology to perform the work specified on his or her application. An attestation about the applicant's need for a license is a required section of the visa application.

Many of the foreign persons employed by the University under these visas as scientists or researchers conduct fundamental research, which is not subject to export control requirements and does not require an export license. However, not all research is exempt from export controls and sanctions regulations, and an export license may be required for a foreign person employee. As such, offices processing visas at University of Missouri institutions must notify Research Security and Compliance during the visa application process for information on how to complete Part 6 of Form I-129. Institutions will have specific procedures implemented for the visa processing office to identify what activities the foreign employee will be engaged in at their institution

[55] See NIST SP 800-171A, *Assessing Security Requirements for Controlled Unclassified Information (CUI)*, which is 'intended to help organizations develop assessment plans and conduct efficient, effective, and const-effective assessments of the CUI security requirements defined in SP 800-171." https://csrc.nist.gov/News/2018/NIST-Publishes-SP-800-171A

[56] See DFARS 252.204-7019, *Notice of NIST SP 800-171 DoD Assessment Requirements*; DFARS 252.204-7020 *NIST SP 800-171 DoD Assessment Requirements*; and DFARS 252.204-7021 *Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement.*

allowing Research Security and Compliance to determine whether an export license is or is not required. Research Security and Compliance will also perform a restricted party screening on all visa applicants as part of its review. After Research Security and Compliance makes a licensing determination, Research Security and Compliance will work with the visa processing office and sponsoring department to ensure that the deemed export attestation in the visa application is completed correctly and that Research Security and Compliance submits a deemed export license request if necessary.

H. International Activities

Travel with, or transmissions of, controlled data to destinations outside the U.S. can have export control implications. A license may be required depending on the items, data, or software leaving the United States; the destination country(ies); the end-use or end application; and/or whether defense services are provided to a foreign person. However, an exception or exemption from license requirements may exist. Any University employee intending to travel with or transmit controlled data, transport-controlled equipment, or remotely access controlled data from outside the U.S. must first consult with Research Security and Compliance.

A license exception[57] may be available for EAR-controlled materials, technology, or software (items) such as research instrumentation or a University laptop if the individual traveling outside the U.S. can certify that he/she:

- Will ship or hand-carry the items for University purposes only;
- Will return within 12 months of departure from the U.S., or certify the destruction of the items;
- Will keep the items within his/her effective control; and
- Will take necessary security precautions to protect against the unauthorized export of technology.

A license exemption[58] may be available for ITAR-controlled technical data transmitted outside the U.S. if the individual transmitting the technical data can certify that:

- The technical data is to be used overseas solely by a U.S. Person(s);
- The U.S. Person(s) overseas is an employee of the University and is not an employee of a foreign subsidiary;
- If the information is “Classified,” for national security purposes under the National Industrial Security Program (NISP), it will be sent overseas in accordance with the requirements of the NISP Operating Manual (NISPOM); and
- No export will be made to countries embargoed under the ITAR[59].

All University engagements with people located in comprehensively sanctioned destinations must be reviewed by Research Security and Compliance prior to the engagement taking place. As of January 2023, these comprehensively sanctioned destinations are:

- Cuba
- Iran
- North Korea
- Syria; and
- Crimea, Donetsk, and Luhansk regions of Ukraine.

[57] Export Administration Regulations. 15 CFR § 740.9 Temporary imports, exports, reexports, and transfers (in-country) (TMP). Retrieved November 28, 2022, from https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-740/section-740.9

[58] International Traffic in Arms Regulations. 22 CFR § 125.4 Exemptions of general applicability. Paragraph (9). Retrieved November 28, 2022, from https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-125/section-125.4

[59] International Traffic in Arms Regulations. 22 CFR § 126.1 Prohibited exports, imports, and sales to or from certain countries. Retrieved November 28, 2022, from https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-126/section-126.1

I. Licensing

The University may be required to obtain an export license prior to authorizing a foreign person to access a restricted research project. Research Security and Compliance at each institution will identify if an export license is required before access can occur when they are aware of a deemed export.

Additionally, the University may be required to obtain a license prior to the export of physical items outside of the country (regardless of whether those items are shipped or hand-carried) and may need to obtain a license prior to engagements with persons located in comprehensively sanctioned destinations or found on restricted party lists. Research Security and Compliance at each institution will identify if a license is required when they have knowledge of the situation.

University personnel may not independently apply for an export or OFAC license to conduct University business. When a license is needed, Research Security and Compliance will prepare the necessary documentation for obtaining a license and an Empowered Official, or their delegate, will submit the application after consultation with the Vice Chancellor for Research and the Office of General Counsel. All parties involved must be aware that license applications require considerable time and effort to prepare, in addition to the (usually extensive) length of time needed for the government to evaluate and make a licensing determination. If approved, all University personnel will follow the terms of the license and will consult with Research Security and Compliance as questions arise.

J. Training Programs

Research Security and Compliance will prepare updated training materials and will require that employees or students engaged in an export-controlled project receive the appropriate briefing. Research Security and Compliance will also maintain records of training or briefings provided.

K. Recordkeeping

Research Security and Compliance shall maintain export-related records in their possession consistent with each institution's record retention policies and applicable agency requirements. Records shall be retained no less than five years after the project's TCP termination date, the date of export, or the license termination date, whichever is later. Records that must be retained include all memoranda, notes, correspondence (including email), financial records, shipping documentation, as well as any other information related to export activities.

L. Continuous Monitoring

To maintain the export compliance and sanctions program and ensure consistent adherence to U.S. export laws, Research Security and Compliance may conduct internal reviews of TCPs, certain projects, and the overall program. Ethics, Compliance and Audit Services may also perform audits of the export compliance and sanctions program periodically. The purpose of the reviews is: (i) to identify deficiencies in training, processes, procedures, etc. that can be rectified; (ii) develop mitigation plans that can be implemented; and (iii) follow up to ensure implementation of mitigation plans.

M. Detecting and Reporting Violations

It is the policy of Research Security and Compliance to voluntarily self-disclose violations as required by law. University personnel who suspect a violation has occurred must immediately notify Research Security and Compliance, an Empowered Official, or report through the University of Missouri System "Ethics and Compliance Hotline." Research Security and Compliance will notify the Office of General Counsel and Ethics, Compliance and Audit Services; will conduct an internal review of the suspected violation; and, as appropriate, will provide the cognizant government agency a thorough narrative account through a voluntary self-disclosure. Upon engagement with a government agency, Research Security and Compliance will follow the government agency's instructions concerning continued investigation and processing. Outside counsel may be retained in certain circumstances at the discretion of Research Security and Compliance, the Office of General Counsel, and Ethics, Compliance, and Audit Services subject to the University of Missouri Guidelines for Outside Counsel.

N. Disciplinary Actions

All University personnel responsible for export control and sanctions compliance or participating in restricted research projects shall be made aware of the substantial criminal and civil penalties imposed for violation of these regulations including personal liability, monetary fines, and imprisonment. Should disciplinary action be deemed necessary, appropriate action shall be taken as provided under the UM Collected Rules and Regulations and/or the Human Resources Manual.

XI. Exhibit A

A. The United States Munitions List

Category I.	Firearms and Related Articles
Category II.	Guns and Armament
Category III.	Ammunition and Ordnance
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.	Personal Protective Equipment
Category XI.	Military Electronics
Category XII.	Fire Control, Laser, Imaging, and Guidance Equipment
Category XIII.	Materials and Miscellaneous Articles
Category XIV.	Toxicological Agents, Including Chemical Agents, Biological Agents, and Associated Equipment
Category XV.	Spacecraft and Related Articles
Category XVI.	Nuclear Weapons Related Articles
Category XVII.	Classified Articles, Technical Data and Defense Services Not Otherwise Enumerated
Category XVIII.	Directed 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

XII. Exhibit B

A. The Commerce Control List[60]

Categories

0	Nuclear Materials, Facilities and Equipment [and Miscellaneous Items]
1	Special Materials and Related Equipment
2	Materials Processing
3	Electronics
4	Computers
5	Telecommunications and "Information Security"
6	Sensors and Lasers
7	Navigation and Avionics
8	Marine
9	Aerospace and Propulsion

Product Groups

A	Equipment, Assemblies and Components
B	Test, Inspection and Production Equipment
C	Material
D	Software
E	Technology

Reasons for Control

AT	Anti-Terrorism
CB	Chemical & Biological Weapons
CC	Crime Control
CW	Chemical Weapons Convention
EI	Encryption Items
FC	Firearms Convention
MT	Missile Technology
NS	National Security
NP	Nuclear Nonproliferation
RS	Regional Stability
SS	Short Supply
UN	United Nations Embargo
SI	Significant Items
SL	Surreptitious Listening

Country Chart[61]

Commerce Country Chart

Reason for Control

Countries	Chemical & Biological Weapons			Nuclear Nonproliferation		National Security		Missile Tech	Regional Stability		Firearms Convention	Crime Control			Anti-Terrorism	
	CB 1	CB 2	CB 3	NP 1	NP 2	NS 1	NS 2	MT 1	RS 1	RS 2	FC 1	CC 1	CC 2	CC 3	AT 1	AT 2
Guyana	X	X		X		X	X	X	X	X	X	X		X		
Haiti	X	X		X		X	X	X	X	X	X	X		X		
Honduras	X	X		X		X	X	X	X	X	X	X		X		
Hong Kong	X	X		X		X		X	X	X		X		X		
Hungary	X					X		X	X							
Iceland	X			X		X		X	X							
India	X	X	X	X	X	X	X	X	X	X		X		X		
Indonesia	X	X		X		X	X	X	X	X		X		X		

[60] Supplement No. 1 to Part 774

[61] If there is an "X" in the column based on the reason(s) for control of the item and the country of destination, a license is required, unless a License Exception is available. If there is no "X" in the control column(s) specified under the ECCN and country of destination, no export license is needed unless exporting to an end-user or end-use of concern or any other General Prohibition applies.

XIII. Definitions

Arms Export Control Act (AECA)
https://www.govinfo.gov/content/pkg/COMPS-1061/pdf/COMPS-1061.pdf
The AECA provides the authority to control the export of defense articles and defense services. The AECA charges the President to exercise this authority, which has been delegated to the Secretary of State. The International Traffic in Arms Regulations (ITAR) implements the AECA.

Commerce Control List (CCL)
15 CFR 774
A part of the Export Administration Regulations (EAR), this list of items (including materials, software, and technology) includes purely civilian items, "dual use" items, or exclusively military items that are not controlled under the International Traffic in Arms Regulations (ITAR).

Commodity Jurisdiction (CJ)
22 CFR § 120.4
The purpose of a commodity jurisdiction request is to determine whether an item or service is covered by the USML and therefore to export controls administered by the U.S. Department of State pursuant to the AECA and the ITAR.

Controlled Unclassified Information (CUI)
https://www.archives.gov/cui/about
Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding classified information. (Classified information is information that Executive Order 13526 or the Atomic Energy Act of 1954 requires to have classified markings and protection against unauthorized disclosure).

Controlled Technical Information (CTI)
https://www.archives.gov/cui/registry/category-detail/controlled-technical-info.html
Technical information with military or space applications that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. CTI is marked with one of the Distribution Statements B through F. The term CTI does not include information that is lawfully publicly available without restrictions or is marked with Distribution Statement A. "Technical Information" means technical data or computer software.

Covered Defense Information (CDI)
https://www.archives.gov/cui/registry/category-list
Unclassified controlled technical information or other information as described in the Controlled Unclassified Information (CUI) Registry that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is:

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contact.

Deemed Export
22 CFR § 120.50 & 22 CFR § 120.56
Releasing or otherwise transferring technical data to a foreign person in the United States. Any release in the United States of technical data to a foreign person is deemed to be an export to all countries in which the foreign person has held or holds citizenship or holds permanent residency. Technical data is released through: 1) visual or other inspection by foreign persons of a defense article that reveals technical data to a foreign person; 2) oral or written exchanges with foreign persons of technical data in the United States or abroad; 3) the use of access information to cause or enable a foreign person, including yourself, to access, view, or possess unencrypted technical data; or the use of access information to cause technical data outside of the United States to be in unencrypted form. Authorization for a release of technical data to a foreign person is

required to provide access information to that foreign person if that access information can cause or enable access, viewing, or possession of unencrypted technical data.

15 CFR § 734.13 & 15 CFR § 734.15
Releasing or otherwise transferring "technology" or source code (but not object code) to a foreign person in the United States. Such a release is "deemed" to be an export to the foreign person's most recent country of citizenship or permanent residency. Technology and software are released through: 1) visual or other inspection by a foreign person of items that reveals technology or source code to the EAR to a foreign person; or 2) oral or written exchanges with a foreign person of technology or source code in the United States or abroad. Any act of causing the release of technology or software, through use of "access information" or otherwise, to yourself or another person requires authorization to the same extent an authorization would be required to export or re-export such technology or software to that person.

Defense Article
22 CFR § 120.31
Any item or technical data designated in the United States Munitions List and is applicable to designations 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 in the United States Munitions List. It also includes forgings, castings, and other unfinished products, such as extrusions and machined bodies, that have reached a stage in manufacturing where they are clearly identifiable by mechanical properties, material composition, geometry, or function as defense articles. It does not include basic marketing information on function or purpose or general system descriptions.

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

Development
15 CFR § 772
Development is related to all stages prior to serial production, such as design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, or layouts.

Dual Use
15 CFR § 772
Items that have both a commercial and military or proliferation applications. While this term is used informally to describe items that are subject to the EAR, purely commercial items and certain munitions items listed on the Wassenaar Arrangement Munitions List (WAML) or the Missile Technology Control Regime Annex are also subject to the EAR.

Export
22 CFR § 120.50
Except as set forth in the ITAR, Export means:
(1) An actual shipment or transmission out of the United States, including the sending or taking of a defense article out of the United States in any manner;
(2) Releasing or otherwise transferring technical data to a foreign person in the United States (a "deemed export");
(3) Transferring registration, control, or ownership of any aircraft, vessel, or satellite subject to the ITAR by a U.S. person to a foreign person;

(4) Releasing or otherwise transferring a defense article to an embassy or to any of its agencies or subdivisions, such as a diplomatic mission or consulate, in the United States;
(5) Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad; or
(6) The release of previously encrypted technical data

15 CFR § 734.13
Except as set forth in the EAR, Export means:
(1) An actual shipment or transmission out of the United States, including the sending or taking of an item out of the United States, in any manner;
(2) Releasing or otherwise transferring technology or source code (but not object code) to a foreign person in the United States (a "deemed export");
(3) Transferring by a person in the United States of registration, control, or ownership of:
    (i) A spacecraft subject to the EAR that is not eligible for export under License Exception STA (i.e., spacecraft that provide space-based logistics, assembly, or servicing of any spacecraft) to a person in or a national of any other country; or
    (ii) Any other spacecraft subject to the EAR to a person or a national of a Country Group D:5 country.

Export Administration Regulations (EAR)
15 CFR §§ 730-780
Export Administration Regulations are issued by the United States Department of Commerce, Bureau of Industry and Security (BIS) under laws relating to the control of certain exports, reexports, and activities related to items on the Commerce Control List. In addition, the EAR implement antiboycott law provisions requiring regulations to prohibit specified conduct by United States persons that has the effect of furthering or supporting boycotts fostered or imposed by a country against a country friendly to the United States.

Export Control Classification Number (ECCN)
15 CFR § 772
The numbers used in supplement no. 1 to part 774 of the EAR and throughout the EAR. The Export Control Classification Number consists of a set of digits and a letter. Reference § 738.2(c) of the EAR for a complete description of each ECCN's composition. This alpha-numeric designation (i.e., 1A984 or 4A001) is used to identify items for export control purposes. An ECCN categorized items based on the nature of the product (i.e., type of commodity, technology, or software and its respective technical parameters). The ECCN provides valuable information on the reasons for control of the item, which transactions may require an export license based on the country of destination and which license exceptions, if any, may apply. All ECCNs are listed in the Commerce Control List (CCL). Items that are "subject to the EAR" but not identified on the CCL are identified by the designator "EAR99".

Empowered Official
22 CFR § 120.67
Empowered Official means a U.S. person who:
(1) Is directly employed by the applicant or a subsidiary in a position having authority for policy or management within the applicant organization; and
(2) Is legally empowered in writing by the applicant to sign license applications or other requests for approval on behalf of the applicant; and
(3) Understands the provisions and requirements of the various export control statutes and regulations, and the criminal liability, civil liability and administrative penalties for violating the Arms Export Control Act and the International Traffic in Arms Regulations; and
(4) Has the independent authority to:
    (i) Inquire into any aspect of a proposed export, temporary export, or brokering activity by the applicant;
    (ii) Verify the legality of the transaction and the accuracy of the information to be submitted; and
    (iii) Refuse to sign any license application or other request for approval without prejudice or other adverse recourse.

For the purposes of a broker who is a foreign person, the empowered official may be a foreign person who otherwise meets the criteria for an empowered official listed above.

Foreign Assets Control Regulations (FACR)
31 CFR §§ 500-599
Foreign Assets Control Regulations are issued by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), which administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction.

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

15 CFR § 772.1
Any natural person who is not a lawful permanent resident of the United States, citizen of the United States, or any other protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any corporation, business association, partnership, trust, society, or any other entity or group that is not incorporated in the United States or organized to do business in the United States, as well as international organizations, foreign governments and any agency or subdivision of a foreign government (e.g., diplomatic mission). "Foreign person" is synonymous with "foreign national," as used in the EAR, and "foreign person" as used in the International Traffic in Arms Regulations (22 CFR 120.63). This definition does not apply to part 760 of the EAR (Restrictive Trade Practices or Boycotts).

Fundamental Research
National Security Decision Directive (NSDD) 189
'Fundamental Research' means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.

22 CFR § 120.34(8)
Fundamental research is defined to mean basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. University research will not be considered fundamental research if:

(i) The University or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity, or
(ii) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable.

The research must be conducted by an accredited institution of higher learning in the U.S.

15 CFR § 734.8
Fundamental Research means research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons.

"Technology" or "software" that arises during, or results from, fundamental research and is intended to be published is not subject to the EAR.

Note: This does not apply to “technology” or “software” subject to the EAR that is released to conduct fundamental research. There are instances in the conduct of research where a researcher, institution, or company may decide to restrict or protect the release or publication of “technology” or “software” contained in research results. Once a decision is made to maintain such “technology” or “software” as restricted or proprietary, the “technology” or “software”, if within the scope of § 734.3(a), becomes subject to the EAR.

“Technology” or “software” that arises during, or results from, fundamental research is intended to be published to the extent that the researchers are free to publish the “technology” or “software” contained in the research without restriction. “Technology” or “software” that arises during or results from fundamental research subject to prepublication review is still intended to be published when:

(1) Prepublication review is conducted solely to ensure that publication would not compromise patent rights, so long as the review causes no more than a temporary delay in publication of the research results;
(2) Prepublication review is conducted by a sponsor of research solely to ensure that the publication would not inadvertently divulge proprietary information that the sponsor has furnished to the researchers; or
(3) With respect to research conducted by scientists or engineers working for a Federal agency or a Federally Funded Research and Development Center (FFRDC), the review is conducted within any appropriate system devised by the agency of the FFRDC to control the release of information by such scientists and engineers.

Although “technology” or “software” arising during or resulting from fundamental research is not considered intended to be published if researchers accept restrictions on its publication, such “technology” or “software” will nonetheless qualify as “technology” or “software” arising during or resulting from fundamental research once all such restrictions have expired or have been removed. Research that is voluntarily subjected to U.S. government prepublication review is considered “intended to be published” when the research is released consistent with the prepublication review and any resulting controls. “Technology” or “software” resulting from U.S. government-funded research that is subject to government-imposed access and dissemination, or other specific national security controls qualifies as “technology” or “software” resulting from fundamental research, provided that all government-imposed national security controls have been satisfied and the researchers are free to publish the “technology” or “software” contained in the research without restriction. Examples of specific national security controls include requirements for prepublication review by the Government, with right to withhold permission for publication; restrictions on prepublication dissemination of information to non-U.S. citizens or other categories of persons; or restrictions on participation of non-U.S. citizens or other categories of persons in the research. A general reference to one or more export control laws or regulations or a general reminder that the Government retains the right to classify is not a specific national security control.

Information or Informational Materials
31 CFR § 560.315
Per the Iranian Transactions and Sanctions Regulations, the term information or informational materials includes, but is not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds.

International Traffic in Arms Regulations (ITAR)
22 CFR §§ 120-130
The International Traffic in Arms Regulations are issued by the Department of State, which has responsibility for the control of permanent and temporary export and the temporary import of defense articles and services. The Arms Export Control Act authorizes the President to promulgate regulations with respect to exports of defense articles and defense services is delegated to the Secretary of State by Executive Order 13637. The International Traffic in Arms Regulations implements this authority.

License
22 CFR § 120.57(a)
15 CFR § 772.1
31 CFR § 542.309

A document issued by the appropriate export agency that authorizes an export, reexport, or other regulated activity as outlined on a license application prepared and submitted by the University.

License Exception
15 CFR § 772.1
An authorization described in the EAR that allows you to export or re-export, under stated conditions, items subject to the EAR that otherwise would require a license. Unless otherwise indicated, these License Exceptions are not applicable to exports under the licensing jurisdiction of agencies other than the Department of Commerce.

License Exemption
22 CFR § 120.57(c)
An authorization described in the ITAR that allows you to export or re-export, under stated conditions, items subject to the ITAR that otherwise would require a license. Unless otherwise indicated, these License Exemptions are not applicable to exports under the licensing jurisdiction of agencies other than the Department of State.

Production
15 CFR § 772.1
Means all production stages, such as product engineering, manufacture, integration, assembly (mounting), inspection, testing, and quality assurance.

Publication or Dissemination Restriction
Any contractual language or verbal agreement that allows a sponsor to prohibit, approve, or otherwise limit publications resulting from research and development. Allowing a sponsor a period of time to review proposed publications for comment or to request removal of proprietary or confidential information provided by another party does not necessarily constitute a publication restriction.

Public Domain
22 CFR 120.34
Information that is published and is generally accessible or available to the public:

(1) Through sales at newsstands and bookstores;
(2) Through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information;
(3) Through second-class mailing privileges granted by the U.S. Government;
(4) At libraries open to the public from which the public can obtain documents;
(5) Through patents available at any patent office;
(6) Through unlimited distribution at a conference, meeting, seminar, trade show, or exhibition, generally accessible to the public, in the United States;
(7) Through public release (*i.e.,* unlimited distribution) in any form (e.g., not necessarily in published form) after approval by the cognizant U.S. government department or agency (see also § 125.4(b)(13));
(8) Through fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community. Fundamental research is defined to mean basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. University research will not be considered fundamental research if:
    (i) The University or its researchers accept other restriction on publication of scientific and technical information resulting from the project or activity, or
    (ii) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable.

Published

15 CFR 734.7

Except as set forth in paragraphs (b) and (c) of this section, unclassified "technology" or "software" is "published," and is thus not "technology" or "software" subject to the EAR, when it has been made available to the public without restrictions upon its further dissemination such as through any of the following:

(1) Subscriptions available without restriction to any individual who desires to obtain or purchase the published information;
(2) Libraries or other public collections that are open and available to the public, and from which the public can obtain tangible or intangible documents;
(3) Unlimited distribution at a conference, meeting, seminar, trade show, or exhibition, generally accessible to the interested public;
(4) Public dissemination (i.e., unlimited distribution) in any form (e.g., not necessarily in published form), including posting on the Internet on sites available to the public; or
(5) Submission of a written composition, manuscript, presentation, computer-readable dataset, formula, imagery, algorithms, or some other representation of knowledge with the intention that such information will be made publicly available if accepted for publication or presentation:
    (i) To domestic or foreign co-authors, editors, or reviewers of journals, magazines, newspapers, or trade publications;
    (ii) To researchers conducting fundamental research; or
    (iii) To organizers of open conferences or other open gatherings.
    (iv)

Published encryption software classified under ECCN 5D002 remains subject to the EAR unless it is publicly available encryption object code software classified under ECCN 5D002 and the corresponding source code meets the criteria specified in § 742.15(b) of the EAR.

The following remains subject to the EAR: "software" or "technology" for the production of a firearm, or firearm frame or receiver, controlled under ECCN 0A501, that is made available by posting on the internet in any electronic format, such as AMF or G-code, and is ready for insertion into a computer numerically controlled machine tool, additive manufacturing equipment, or any other equipment that makes use of the "software" or "technology" to produce the firearm frame or receiver of complete firearm.

Reexport

22 CFR § 120.51

15 CFR § 734.14

Except as set forth in §§ 734.18 and 734.20, reexport means:

(1) An actual shipment or transmission of an item subject to the export control regulations from one foreign country to another foreign country, including the sending or taking of an item to or from such countries in any manner;
(2) Releasing or otherwise transferring "technical data", "technology", or source code subject to export control regulations to a foreign person of a country other than the foreign country where the release or transfer takes place (a deemed export);
(3) Transferring by a person outside the United States of registration, control, or ownership of any aircraft, vessel, or satellite between foreign persons.

Release

22 CFR § 120.56

15 CFR § 734.15

"Technical Data" subject to the ITAR, and "technology" and "software" subject to the EAR are "released" through:

(1) Visual or other inspection by a foreign person of a defense article that reveals technical data to a foreign person;
(2) Visual or other inspection by a foreign person of the item that reveals the "technology or source code subject to the EAR to a foreign person;
(3) Oral or written exchanges with a foreign person of technical data subject to the ITAR or "technology" or source code subject to the EAR in the United States or abroad;

(4) The use of access information to cause or enable a foreign person, including yourself, to access, view, or possess unencrypted technical data subject to the ITAR; or
(5) The use of access information to cause technical data subject to the ITAR outside of the United States to be in unencrypted form.

Restricted Parties
Individuals and entities with whom the University may be prohibited by law from engaging in export transactions or who may require a license or other government approval in order for the University to export to or engage in controlled transactions. These include individuals and entities appearing on lists that include but are not limited to: (1) the Department of Commerce Denied Persons List, Entity List, and Unverified List; (2) the Department of State Nonproliferation Sanctions List and AECA Debarred List; and (3) the Department of the Treasury Specially Designated Nationals and Blocked Persons List.

Restricted Research
University research, development, or testing that is subject to export controls such as the ITAR or EAR, sanctions regulations, controlled information restrictions, and/or security restrictions and may require a license or other government approval for foreign person participation. Research is considered restricted if it requires the University to: (i) accept publication restrictions; (ii) accept access and dissemination controls; (iii) accept federally funded research with contract-specific national security restrictions; (iv) accept third-party controlled items or information; or (v) provide access to, or defense services on, a defense article. Restricted research is generally subject to the ITAR or the EAR, and a license or other governmental approval may be required for foreign person participation.

Retransfer
22 CFR § 120.52
A change in end use or end user, or a temporary transfer to a third party, of a defense article within the same foreign country; or a release of technical data to a foreign person who is a citizen or permanent resident of the country where the release or transfer takes place.

Sanctioned Destinations
31 CFR §§ 500-599
Countries, and more recently regions of countries, designated by OFAC or through Executive Orders as having limited or comprehensive trade sanctions imposed by the United States for reasons of anti-terrorism, non-proliferation, narcotics trafficking, or other reasons.

Technical Data
22 CFR § 120.33
Technical data means:
(1) Information, other than software as defined in § 120.40(g), which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions, or documentation.
(2) Classified information relating to defense articles and defense services on the U.S. Munitions List and 600-series items controlled by the Commerce Control List;
(3) Information covered by an invention secrecy order; or
(4) Software (see § 120.40(g)) directly related to defense articles.

Technical Data does not include information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities, or information in the public domain as defined in § 120.34 or telemetry data as defined in note 3 to Category XV(f) of part 121.1. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles.

Technology
15 CFR § 772.1
Information necessary for the “development”, “production”, “use”, operation, installation, maintenance, repair, overhaul, or refurbishing (or other terms specified in ECCNs on the CCL that control “technology”) of an item. “Technology” may be in any tangible or intangible form, such as written or oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, electronic media or information revealed through visual inspection.

Transfer
15 CFR § 772.1
15 CFR 734.16
A shipment, transmission, or release of items subject to the EAR either within the United States or outside the United States. A change in end use or end user of an item within the same foreign country.

United States Munitions List (USML)
22 CFR § 121.1
A part of the ITAR, articles, services, and related technical data are designated as defense articles or defense services pursuant to sections 38 and 47(7) of the Arms Export Control Act constitute the U.S. Munitions List.

Use
15 CFR § 772.1
Operation, installation (including on-site installation), maintenance (checking), repair, overhaul, and refurbishing. If an ECCN specifies one or more of the six elements of “use” in the heading or control text, only those elements specified are classified under that ECCN.

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

15 CFR § 772.1
U.S. Person includes:
(1) Any individual who is a citizen of the United States, a permanent resident alien of the United States, or a protected individual as defined by 8 U.S.C. 1324b(a)(3);
(2) Any juridical person organized under the laws of the United States or any jurisdiction within the United States, including foreign branches; and
(3) Any person in the United States

15 CFR 740.9(a)(12)
For purposes of this § 740.9, a U.S. person is defined as follows: an individual who is a citizen of the United States, an individual who is a lawful permanent resident as defined by 8 U.S.C. 1101(a)(2), or an individual who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). U.S. person also means any juridical person organized under the laws of the United States, or any jurisdiction within the United States (e.g., corporation, business association, partnership, society, trust, or any other entity, organization, or group that is authorized to do business in the United States).

XIV. Commonly Used Acronyms

AECA	Arms Export Control Act
BIS	Bureau of Industry and Security
CCL	Commerce Control List
CJ	Commodity Jurisdiction
CUI	Controlled Unclassified Information
CTI	Controlled Technical Information
CDI	Covered Defense Information
DDTC	Directorate of Defense Trade Controls
EAR	Export Administration Regulations
ECCN	Export Control Classification Number
FACR	Foreign Assets Control Regulations
ITAR	International Traffic in Arms Regulations
OFAC	Office of Foreign Assets Controls
RSC	Research Security and Compliance
TCP	Technology Control Plan
USML	United States Munitions List

XV. References

Arms Export Control Act (AECA)	22 U.S.C. § 2778
Atomic Energy Act of 1954, as amended	42 U.S.C. § 2011
BIS Export Compliance Guidelines	pdf
Bureau of Industry and Security, U.S. Department of Commerce (BIS)	bis.doc.gov
Department of Energy (DOE)	energy.gov
DDTC Compliance Program Guidelines	pdf
Directorate of Defense Trade Controls, U.S. Department of State (DDTC)	pmddtc.state.gov
DoD Instruction 5230.24, "Distribution Statements of Technical Documents"	pdf
DoD Policy Memorandum Contracted Fundamental Research (26 Jun 2008)	pdf
DoD Policy Memorandum Fundamental Research (24 May 2010)	pdf
DOE O 471.7 Controlled Unclassified Information	pdf
Energy Reorganization Act of 1974	42 U.S.C. §§ 5801 et. seq.
Executive Order 13526 Classified National Security Information	79 FR 44093
Executive Order 13556 Controlled Unclassified Information	75 FR 68675
Executive Order 13637 Administration of Reformed Export Controls	78 FR 16127
Export Administration Act of 1979	50 U.S.C. §§ 4601-4623
Export Administration Regulations (EAR)	15 CFR §§ 730-774
Export Control Reform Act of 2018	50 U.S.C. §§ 4801-4852
Export and Import of Nuclear Equipment and Material Regulations	10 CFR § 110
Foreign Assets Control Regulations (FACR)	31 CFR §§ 500-599
International Emergency Economic Powers Act (IEEPA)	50 U.S.C. §§ 1701-1707
International Traffic in Arms Regulations (ITAR)	22 CFR §§ 120-130
National Industrial Security Program Operating Manual	32 CFR § 117
National Security Decision Directive 189 (21 Sep 1985)	online
NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	online
Nuclear Regulatory Commission (NRC)	nrc.gov
Assistance to Foreign Atomic Energy Activities	10 CFR § 810
OFAC Framework for Compliance Commitments	pdf
Office of Foreign Assets Control, U.S. Department of the Treasury (OFAC)	treasury.gov
Trading with the Enemy Act (TWEA)	22 U.S.C. §§ 7201-7211

University of Missouri System

Research Security and Compliance

University of Missouri System

310 Jesse Hall
Columbia, Missouri 65211

www.umsystem.edu