



**Southern Illinois University System**

ONE SYSTEM | MANY LOCATIONS | STATEWIDE IMPACT

# Export Control Compliance Manual

# Table of Contents

1 Overview of Export Control Regulations.....	3
1.1 Introduction .....	3
1.2 Export Control Laws at SIU.....	3
1.3 Department of State Regulations (ITAR).....	4
1.4 Department of Commerce Regulations (EAR) .....	8
1.5 Department of Treasury Regulations (OFAC) .....	13
1.6 Records/ Record Retention.....	14
1.7 Penalties for Export Violations.....	14
2 SIU Export Control Procedures .....	15
2.1 Commitment to Export Control Compliance .....	15
2.2 Roles and Responsibilities for Export Controls at SIU.....	16
2.3 Export Control Analysis.....	19
2.4 Technology Control Plans (TCP) .....	20
2.5 Licensing.....	22
2.6 International Travel.....	22
2.7 Training .....	22
2.8 Recordkeeping .....	23
2.9 Monitoring and Auditing.....	24
2.10 Detecting and Reporting Violations .....	24
3 Appendices.....	26
Appendix 3.1: Glossary of Abbreviations.....	27
Appendix 3.2: Red Flags for Shipping Internationally.....	28
Appendix 3.3: SIU Clean Laptop Program .....	29
Appendix 3.4: Decision Tree .....	32
Appendix 3.5: University Guidelines (Section 12: Export Controls).....	33
Appendix 3.6: SIU Export Control Office Contact Information .....	38

# Export Control Contact Information

Export Controls is under the direction of the [Vice President for Academic Affairs](#) and is responsible for helping the University community understand and comply with export control laws and regulations. For additional information, tools to assist in determining how the regulations apply to your activity, and assistance with export control concerns, please contact the Export Controls Office using the contact information below.

## **Staff Contact Information:**

Todd Wakeland, JD, Director of Export Controls  
3311 Rendleman Hall  
Box 1259  
Edwardsville, Illinois 62026  
[twakela@siue.edu](mailto:twakela@siue.edu)  
618-650-2476

Brenda Martin, Export Control Officer  
363 Woody Hall  
Mailcode 4344  
Carbondale, IL 62901  
[bjmartin@siu.edu](mailto:bjmartin@siu.edu)  
618-453-2308

# 1 Overview of Export Control Regulations

---

## 1.1 Introduction

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

Several federal agencies have jurisdiction over the control of exports, including the Department of Commerce, the Department of Energy, the Department of State, the Department of Treasury, the Nuclear Regulatory Commission, and the U.S. Department of Agriculture. The three principal agencies among these are the Department of State, which administers controls of defense exports through its Directorate of Defense Trade Controls (DDTC), the Department of Commerce, which administers export of commercial, “dual-use,” and less sensitive defense items and technologies through the Bureau of Industry and Security (BIS), and the Department of Treasury, which administers exports to embargoed countries and specially designated nationals through its Office of Foreign Asset Controls (OFAC). While the discussion below focuses on these three agencies, it is important to remember that meeting the export requirements of one of these agencies alone is not sufficient, and the applicability of all of these regulations to a specific activity should be evaluated in order to ensure full compliance with the U.S. export control regulations.

## 1.2 Export Control Laws at SIU

The export control laws apply to many activities at SIU that do not involve research, and to which you might not expect these laws to apply. For example, just entering into a contract with certain people listed on certain government lists, or sending money to certain countries, may require a license from the U.S. government. As another example, shipping certain items, such as ancient artifacts from the SIU Museum to certain foreign destinations, robots for a competition outside the U.S., or inert plasmids to a Ph.D. student writing her dissertation at a foreign university, might involve complying with the export control laws. (These are all real examples from universities.)

However, research activities both at SIU and abroad do present the majority of the compliance challenges for SIU.

Universities in the United States, including SIU, have a long tradition of inventing and developing leading edge technologies that are important for national security and economic competitiveness as well as for educating and training scholars from around the world. In recognition of this role, export control laws of both the Department of State and Department of Commerce carve out special provisions whereby unrestricted research and classroom teaching activities at universities in the U.S. are excluded from the regulations. As a result, most research activities at SIU will be “fundamental research” as defined in the export control laws, and as a result, not require a “license” or permission from the government, and be exempt from the laws in most cases. Nonetheless, it is important to understand the limits on fundamental research in the context of the applicable export control regulations.

The U.S. export control agencies place the burden of understanding and complying with the regulations on the University.<sup>1</sup> Even though most research conducted on campus will not be subject to export control restrictions, it is important for the university community to be aware of when activities potentially become controlled. Many universities accept restrictions on publication and participation in sponsored research, so it is incumbent upon SIU researchers to verify what, if any, information is export controlled in the conduct of collaborative research with other institutions and to prevent the dissemination of such information at SIU. The export control laws may apply to research activities on campus if controlled equipment, data, or information is used in the conduct of that research. The export control regulations apply to the export (even temporary) of controlled, university-owned equipment for field research and to the shipment of research materials or equipment to locations outside of the United States.

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

## **1.3 Department of State Regulations (ITAR)**

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

The Arms Export Control Act (AECA), 22 U.S.C. § 2778 grants authority to the President of the United States to designate and control the export and import of defense articles and services.

---

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

Presidential executive order 11958 delegates this responsibility to the Secretary of State. The Department of State Directorate of Defense Trade Controls (DDTC) administers this authority through implementation of the International Traffic in Arms Regulations (ITAR), 22 C.F.R. §§ 120-130.

The ITAR contains the United State Munitions List (USML), which includes defense articles and related technical data that are controlled for export purposes. In addition to the defense article or related technical data, constituent parts and components of the defense article are controlled under the ITAR. For example, military aircraft are on the USML, as are their engines, electronic controls, and inertial navigation systems, even though such components may have other applications. If a commodity contains a part or component that is controlled under the ITAR, such as a controlled inertial navigation system, then that commodity is also controlled under the ITAR, regardless of whether or not that commodity has an inherently military purpose. Thus, an autopilot system used in basic robotics research at SIU may be controlled under the ITAR.

Many items designed for military use are also used for research completely unrelated to that military use. One possible example at SIU would be night vision goggles, which are used in research. The goggles allow the researchers to observe in low light conditions. The goggles are controlled under the ITAR even though they are not being used in a military activity. It is important to understand that the ITAR designation is unrelated to SIU's use of a controlled item.

### **1.3.2 Important ITAR Definitions**

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

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

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

**Defense Service** is defined in 22 C.F.R. § 120.9. The definition includes furnishing of assistance, including training, to a foreign person, whether in the 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. It also includes providing any foreign person any technical data as defined above.

The ITAR considers fundamental research in science and engineering at accredited institutions of higher learning in the United States to be in the public domain, and therefore, no export license would be needed to export the resulting information abroad or share it with foreign nationals in the United States.

**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 activity, or (ii) the research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable. (22 C.F.R. § 120.11.)

**Public Domain** is defined in 22 C.F.R. § 120.11. Public domain information is information, which is published, and which is generally accessible or available to the public. The ITAR describes means by which public domain information might be available, which in addition to libraries, subscriptions, newsstands, and bookstores, include published patents and public release at conferences, meetings, and trade shows *in* the United States where those venues are generally accessible to the public.

### **1.3.3 The United States Munitions List (USML) Categories**

The USML defines 21 classes of defense articles. The USML is found at 22 C.F.R. § 121. In the interest of brevity, only the main headings of the USML categories are listed here. For detailed descriptions of what is included in each category, the ITAR may be accessed on line at [https://www.pmdtc.state.gov/ddtc\\_public?id=ddtc\\_public\\_portal\\_itar\\_landing](https://www.pmdtc.state.gov/ddtc_public?id=ddtc_public_portal_itar_landing).

Note that category XXI is reserved for use by DDTC for controlling new technologies under the ITAR.

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

**1.3.4 Exporting under the ITAR**

An export as defined under the ITAR includes sending or taking a defense article out of the United States, disclosing (including oral or visual disclosure) technical data to a foreign person whether in the U.S. or abroad, or performing a defense service on behalf of a foreign person whether in the U.S. or abroad. (See 22 C.F.R. § 120.17 for a complete listing of export meaning under the ITAR.) **This definition is extremely broad. It includes taking controlled technical data out of the United States on a laptop computer, regardless of whether or not that information is viewed or accessed while abroad. It also includes allowing a foreign person to view or use a defense article in the United States. Most exports of defense articles and defense services must be licensed by DDTC.**

Generally, a U.S. person that manufactures, brokers, or exports defense articles or services must be registered with DDTC. Registration is required prior to applying for a license or taking

advantage of some license exemptions. Registered entities may apply for licenses, or permission, to export defense articles and defense services. DDTC reviews license requests on an individual basis and consults with other agencies, such as the Department of Defense, in consideration of the request. Exports of ITAR-controlled items are prohibited to some countries and individuals. The list of country policies may be found at [https://www.pmdotc.state.gov/ddtc\\_public?id=ddtc\\_public\\_portal\\_country\\_landing](https://www.pmdotc.state.gov/ddtc_public?id=ddtc_public_portal_country_landing).

### 1.3.5 Commodity Jurisdiction

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

## 1.4 Department of Commerce Regulations (EAR)

### 1.4.1 Regulatory Authority and Scope

The EAR controls the export of “dual-use” items, which are items that have civilian uses but that may also have military or other strategic applications. Common, real-life examples from SIU include certain chemicals, microorganisms, vectors, and toxins as well as laboratory equipment such as centrifuges, analyzers, and fabrication equipment, such as milling machines and etching equipment for electronics. These items are classified on the Commerce Control List (CCL). The CCL is a “positive list”; in other words, if an item is NOT listed on the CCL, then, generally, the EAR does not apply. The EAR also controls the export of purely commercial commodities in support of U.S. trade and embargo policies. Purely commercial items are classified as EAR99 and have very few export restrictions.

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

## 1.4.2 Important EAR Definitions and Concepts

**Export** is defined in 15 C.F.R. § 734.13 as an actual shipment or transmission of items subject to the EAR out of the United States as well as the release of technology or software subject to the EAR in a foreign country or to a foreign national either in the United States or abroad.

**Deemed Export** is defined in 15 C.F.R. § 734.13(a)(2) and 734.13(b). A deemed export is any release of technology or source code subject to the EAR to a foreign national, regardless of location. The release is deemed to be an export to the home country or countries of the foreign national. For the purposes of the EAR, legal U.S. permanent residents, naturalized citizens, and individuals protected under the Immigration and Naturalization Act (8 U.S.C. § 1324b(a)(3)) are not considered to be foreign nationals.

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

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

**Published** is defined in 15 C.F.R. § 734.7. Information is published when it is accessible to the interested public in any form. Publications may take the form of periodicals, books, print, electronic, public web sites, or any other media available for general distribution. General distribution may be defined as available to an interested community, such as a technical journal available to scientists in a relevant field, so long as the price charged for the publication does not exceed the cost of reproduction and distribution. Articles submitted to journals for consideration for publication are considered to be published, regardless of whether or not they are accepted. Published information also includes information readily available in libraries (including university libraries), as well as patents and published patent applications. Finally, release of information at a conference open to the participation of all technically qualified persons is considered to be publication of that information. Software is considered published when it is available for general distribution either free or at the cost of distribution. However, strong encryption software remains controlled, regardless of general availability.

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 (15 C.F.R. §

734.3(b)(3)(iii)). Educational Information is information released as part of a course listed in the university’s course catalog, and through instruction in the classroom or teaching laboratory. Participation in the course should be open to any qualified student enrolled at the academic institution. Educational information is not subject to the EAR, even if the faculty member is teaching the class at an institution outside the United States.

**Fundamental Research** is research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons (15 C.F.R. § 734.8(c)). The complete definition and discussion of fundamental research, including university-based research is found at 15 C.F.R. § 734.8. University research is considered to be fundamental to the extent that researchers do not accept restrictions on the publication of scientific and technical information resulting from the research. Temporary delays in publication for the protection of sponsor proprietary information do not remove research from the fundamental domain. However, if that sponsor’s proprietary information is subject to the EAR, then that information remains subject in the conduct of the research. **SIU researchers receiving proprietary information from corporate research sponsors should consult the Export Controls Office to ensure compliance with the EAR in the conduct of the related research.**

### 1.4.3 The Commerce Control List

The CCL is found at 15 C.F.R. § 774, which may be accessed at: <https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl>. Items included on the CCL are assigned an export control classification number (ECCN) based on a category and product group. There are 10 categories, numbered 0-9, and five product groups, labeled A-E, within each category. The category and product group generally describe the item being classified, and the remaining three digits of the ECCN relate to the item specifications. An ECCN follows the nomenclature of “#α###”, where the first “#” is the category, “α” is the product group, and “###” identifies the reasons for control. As an example, a plasmid with certain genetic characteristics has an ECCN of 1C353. In general, “###”, with lower numbers are controlled to more destinations than those with higher numbers. The categories and product groups are as follows:

Commerce Control List Categories	
0	Nuclear and Miscellaneous items
1	Materials, Chemicals, Microorganisms, and Toxins
2	Materials Processing
3	Electronics
4	Computers
5	Part 1 - Telecommunications

5	Part 2 - Information Security
6	Sensors and Lasers
7	Navigation and Avionics
8	Marine
9	Aerospace and Propulsion

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

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

#### 1.4.4 License Exceptions

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

**A complete listing of EAR license exceptions may be found in 15 C.F.R. § 740. Exceptions commonly applicable to members of the SIU community traveling abroad are BAG, which applies to personally owned items taken abroad for personal use while abroad, and TMP, which applies to the temporary export of SIU-owned equipment, including laptop computers and other equipment listed on the CCL, for work-related activities, including professional**

presentations, teaching, and field research. It is important to note that there are limitations on the use of the TMP license exception; items must be returned to the United States within 1 year of export, or if not returned, documentation of disposal is required. Items exported using the TMP license exception must be kept under the effective control of the traveler while abroad. Additionally, TMP is not applicable to some restricted locations, such as Cuba.

#### 1.4.5 Commodity Classification

BIS encourages exporters to use the detailed descriptions in the CCL to self-classify items to be exported. However, in the event of an incorrect classification, the exporter is liable for any resulting violations of the EAR and may be subject to resulting penalties. Self-classification may be particularly difficult in the university environment where cutting edge-research pushes the boundaries of existing technologies, and in fact may not precisely meet the technical specifications as described in the existing CCL listings. When unsure about a self-classification, the exporter may submit the item/technology to BIS for a formal classification. Members of the SIU community who need assistance with classifying items should contact the Export Controls Office.

#### 1.4.6 Anti-Boycott Restrictions

The Anti-Boycott provisions of the EAR were designed and implemented to address foreign governments' boycott of countries friendly to the United States. The provisions were first implemented in response to the Arab League Boycott of Israel. Currently, Arab Countries including Iraq, Kuwait, Lebanon, Libya, Qatar, Saudi Arabia, Syria, the United Arab Emirates, and Yemen may require participation in an international boycott.<sup>2</sup> Such companies are "blacklisted" under the boycott.

The anti-boycott provisions are found in 15 C.F.R. § 760. The provisions apply to any person or entity in the United States as well as to U.S. persons or entities abroad. For example, SIU is a U.S. person because it is located and organized under U.S. law. The anti-boycott provisions specifically prohibit the following activities:

- Agreement to refuse or actual refusing to do business with a boycotted country or with blacklisted person
- Agreement to discriminate or actual discrimination against other persons based on race, religion, sex, national origin, or nationality (for example, agreeing to refuse to hire Israeli nationals)
- Providing information about race, religion, sex, or national origin of another person

---

<sup>2</sup> <https://www.federalregister.gov/documents/2017/03/30/2017-06264/list-of-countries-requiring-cooperation-with-an-international-boycott>

- Furnishing information about business relationships with boycotted countries or blacklisted persons (for example, providing information about current or previous business in Israel)
- Furnishing information about membership concerning associations with charitable and fraternal organizations
- Paying or otherwise implementing letters of credit containing prohibited conditions or requirements.

Exceptions to these prohibitions exist but are limited. **Additionally, U.S. persons asked to engage in the prohibited activities are required to report the request to BIS.** If you encounter boycott language in a SIU activity, please contact the Export Controls Office for assistance in determining whether an exception is applicable and if reporting to BIS is required.

## 1.5 Department of Treasury Regulations (OFAC)

### 1.5.1 Regulatory Authority and Scope

The Office of Foreign Asset Controls (OFAC) administers and enforces economic and trade sanctions based on U.S. foreign policy and national security interests. Many of the sanctions are based on United Nations and other international mandates. Sanctions are country/program specific and are subject to frequent change based on the changing geo-political landscape. In addition to foreign countries and regimes, OFAC imposes sanctions on individuals, such as people the U.S. government deems to be terrorists and narcotics traffickers. The implementing regulations for the OFAC sanctions are found in 31 C.F.R. §§ 500-599, the Foreign Asset Control Regulations.

The OFAC sanctions broadly prohibit most transactions between a U.S. person and persons or entities in an embargoed country or who have been declared specially designated nationals (SDNs). The prohibition generally includes importation and exportation of goods and services as well as related financial transactions or engaging in business activities with SDNs. Currently, OFAC sanctioned countries include **Cuba, Iran, North Korea, Sudan, Syria, and the Crimea region of the Ukraine**. Additional activity-based sanctions programs include Counter Narcotics Trafficking, Counter Terrorism, Non-Proliferation, and Transnational Criminal Organizations sanctions as well as the Rough Diamond Trade Controls. The activity-based sanctions programs are implemented through the designation of individuals engaging in the banned activities as SDNs. The OFAC sanctions program can change rapidly, so it is important to check for updates periodically.<sup>3</sup>

---

<sup>3</sup> <https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx>

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

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

### **1.6 Records/ Record Retention**

The ITAR, EAR, and OFAC regulations all stipulate record keeping requirements for regulated export activities. Under each of these sets of regulations, records must be retained for **5 years** after the completion of the activity and made available to the regulating authority upon request. Records that should be retained include all memoranda, notes, correspondence (including email), financial records, shipping documentation, as well as any other information related to the export activities. Additionally, when a license exception (EAR) or license exemption (ITAR) is used, additional records documenting the applicability of the exception/exemption may be required and in some cases, there may be additional reporting requirements.

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

### **1.7 Penalties for Export Violations**

Violation of the export control laws can result in both civil and criminal penalties, including fines and imprisonment. Although there is a maximum amount for a civil or criminal penalty, the actual penalty is often multiplied. For instance, if multiple unauthorized shipments of the same

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

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

Violations of export control laws discovered at SIU should be reported to the Export Controls Office or to the Office of General Counsel. Additionally, the SIU compliance hotline at (844)-597-8463 or at SIU-MED at (800) 910-6707; is available for confidential reporting of suspected violations. Most importantly, if there is a question as to whether an activity would be a violation of the export control laws, it is important to consult with the Export Controls Office prior to engaging in the activity.

## 2 SIU Export Control Procedures

---

### 2.1 Commitment to Export Control Compliance

**SIU must comply with all applicable U.S. government export regulations.** The vast majority of teaching and research activity at SIU falls within one or more of several exemptions and exclusions from licensing requirements. However, it is important to understand how the laws apply to activities at SIU as well as the corresponding compliance obligations, which may extend to documenting the applicable licensing exception(s).

The U.S. government defines exports to include not only tangible or “physical” items, such as biological materials, chemicals, and equipment, but also intangible information, which may include research data, formulae, engineering designs, and ideas. Furthermore, an export is defined not only as an actual physical shipment, but also includes electronic and voice transmissions out of the United States (e.g., email or a phone call to a colleague at a foreign

institution or remotely accessing controlled documents while traveling internationally). Exports also include the release of technology to foreign nationals within the United States, the provision of training or services involving controlled equipment to foreign nationals in the United States or abroad, and engaging in transactions or providing services to entities and individuals who are on embargo or specially designated nationals lists.

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

SIU is committed to the preservation of academic freedom. However, the University recognizes its obligation to comply with the U.S. export control regulations. Fortunately, most, but not all, research activities on campus fall under the “fundamental research exemption,” which provides that basic and applied research activities NOT subject to publication or access restrictions will not be subject to export controls. Other exemptions apply to information shared in the conduct of teaching activities on campus in the United States as well as to information that is already publicly available. The export regulations are complex and continually changing, so it is important to consider each activity on an individual basis.

The SIU Export Controls Office is responsible for helping the community understand and comply with the export control laws and apply for an export license when necessary. Please see <http://siusystem.edu/academic-affairs/export-controls/index.shtml> for additional information including analytical tools to assist you in determining if and how the regulations apply to an activity, as well as points of contact for assistance with export control matters. Questions regarding export control laws or procedures for compliance at SIU may be addressed to the Director of Export Control at 618-650-2476 or [twakela@siue.edu](mailto:twakela@siue.edu).

## **2.2 Roles and Responsibilities for Export Controls at SIU**

The Commitment to Compliance letter signed by the SIU President, Chancellors and Medical School Dean, is included in Appendix 3.5. While it is the responsibility of senior university management and senior school administrators to ensure the existence of adequate resources and management support to comply with the export control regulations and to resolve identified export control issues, the discussion below focuses on other key actors in export compliance at SIU.

### **2.2.1 Empowered Officials**

The Director of Export Controls is SIU's Empowered Officials for export control matters in conjunction with the General Counsel's Office. In this capacity, the Empowered Official has the authority to represent SIU before the export control regulators in matters related to registration, licensing, commodity jurisdiction and classification requests, and voluntary or directed disclosures. While certain oversight functions may be delegated, only Empowered Officials may sign paperwork and bind the university in any proceeding before DDTC, BIS, OFAC, or any other government agency with export control responsibilities.

### **2.2.2 Export Controls Office**

The Director of Export Control, assisted by the Export Control Officer, together with senior management:

1. identifies areas at SIU that are impacted by export control regulations;
2. develops export control procedure guidance to assist the university in remaining in compliance with export control regulations;
3. educates inventors, principal investigators, research centers, and academic units about export control regulations and procedures at SIU;
4. educates others at SIU such as Procurement, Purchasing, Travel, International Programs, Office of International Affairs Student Success Center, Center for International Education, Human Resources, and the Technology Transfer Office about export control regulations and procedures at SIU;
5. monitors and interprets export control legislation;
6. works with others to facilitate understanding and compliance with export controls;
7. assists investigators, researchers, and offices at SIU when research involves export-controlled equipment or information;
8. seeks advice from the Office of General Counsel in analyzing and handling export control compliance issues;
9. assists the PI in developing a technology control plan for research involving export-controlled items or information to ensure compliance with export control regulations;
10. applies for export licenses, commodity jurisdiction and commodity classification requests;
11. advises and assists with record keeping for export-controlled activities at SIU; and
12. maintains the Export Controls website.

### **2.2.3 Office of Sponsored Projects/Office of Research and Projects**

The Office of Sponsored Projects (OSP) at SIUC, The Associate Dean of Research (ADR) at SIU-MED, and the Office of Research and Projects (ORP) at SIUE, provide assistance and expertise in export controls by working closely with the Export Controls Office in identifying export control

issues and providing support for their solution. OSP, ADR and ORP have the authority to bind the University to research-related agreements on behalf of The SIU Board of Trustees.

OSP/ORP/ADR:

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

#### **2.2.4 Research Administrators**

The school and department research administrators work closely with OSP/ORP/ADR and the PI. Together with OSP/ORP/ADR, they:

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

#### **2.2.5 Business Administrators**

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

Nationals (SDN) list, ensuring that international travel is compliant with applicable export control regulations, and ensuring that visa export certification information has been completed.

## **2.2.6 Principal Investigators**

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

1. understand his/her obligations under the export control laws;
2. assist the Export Controls Office in correctly classifying technology and items that are subject to export control laws;
3. assist in developing and maintaining the conditions of a technology control plan for any activity, data, or equipment where the need for such a plan is identified; and
4. ensure that research staff and students have been trained on the technology plan and on the export control regulations should any apply.

## **2.3 Export Control Analysis**

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

OSP/ORP/ADR performs an initial review of the request for proposal, broad agency announcement, or award. The OSP/ORP/ADR grant and contracts staff are trained to identify the following red flags that indicate the possible presence of export control issues:

1. references U.S. export control regulations (beyond a mere statement to comply with the law);
2. restricts access or participation based on country of origin;
3. restricts the use of proprietary or confidential information;
4. grants the sponsor pre-publication review and approval for matters other than the inclusion of patent or sponsor proprietary/confidential information;
5. allows the sponsor to claim the results or data generated in the agreement as proprietary or trade secret;
6. involves export-controlled equipment (if known);
7. includes foreign sponsors or collaborators;
8. travel, shipping, or work outside of the United States; and
9. military applications of project results.

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

## **2.4 Technology Control Plans (TCP)**

SIU may be in possession of items that are subject to U.S. export control laws and regulations. SIU aims to engage foreign nationals and host international visitors in the most welcoming manner possible, while still maintaining compliance with U.S. laws and regulations governing the export of certain equipment and materials, as well as protecting sensitive data.

Federal laws and regulations, including, but not limited to, the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR) regulate the transfers of physical items, technical information, data, products, software, hardware, biological materials, or chemical materials, hereafter referred to as “*export-controlled items and information*”, to certain non-U.S. persons and entities. It is unlawful under the EAR or ITAR to send or take *export-controlled items and information* out of the United States without proper authorization. This includes disclosing information orally or visually or transferring *export - controlled items or information* to a foreign person inside or outside the U.S. without proper authorization.

Under the ITAR or the EAR, an export license may be required for foreign nationals to access *export - controlled items and information*. A foreign person is a person who is not a U.S. citizen, a U.S. permanent resident or a person who is protected under the U.S. refugee and asylum status. The law does not make exceptions for foreign graduate students.

In order to follow best practices, SIU shall implement a Technology Control Plan (TCP) whenever a research activity is subject to export controls. The purpose of the TCP is to help ensure compliance with U.S. export control laws and regulations, to appropriately secure the *export-controlled items and information* from unauthorized access, and ensure the research teams understand their compliance obligations and responsibilities.

The Exports Control Office shall assist the Principal Investigator (PI) of the project to develop and implement the TCP. Before any individual may have access to *export-controlled items or information*, he or she must be informed of the conditions of the TCP and agree to comply with the security measures outlined in the TCP. SIU personnel subject to a TCP must complete an initial in-person export control training when the TCP is implemented and are required to complete follow up training annually. In addition, the Export Controls Office shall monitor compliance with the TCP and confirm its accuracy on an annual basis with the PI. It is the PI’s

responsibility to contact the Export Controls Office if any changes need to be made to the TCP during the course of the year.

If EAR equipment is identified, but there are no additional *export-controlled items and information*, a comprehensive TCP is not necessary. However, in order to ensure compliance with EAR requirements, an EAR Equipment Acknowledgement Form shall be completed by all parties that will be using the equipment.

Export Controls staff shall place an “SIU Export Control Property” sticker on all export-controlled equipment, whether EAR or ITAR controlled. This sticker will have a unique number on it and will be tracked on an inventory listing maintained by the Export Controls Office.

When a PI or other involved party believes a TCP may be necessary, they shall contact the Export Controls Office. If the Export Controls Office determines that a TCP is needed, the Export Controls Office shall assist the PI to develop and implement a TCP to secure the *export-controlled items and information* from unauthorized access. The TCP shall be customized dependent on the security measures needed for the circumstances and situations.

However, at a minimum, the TCP shall include the following elements:

- A commitment to export control compliance
- Identification of the applicable export controls and items or technologies subject to the controls
- A description of the agreed upon physical and information security measures to control the item/technology, including as appropriate: laboratory compartmentalization, time blocking, marking, locked storage, electronic security, and/or confidential communications
- Identification and nationality of each individual who will have access to the controlled item or technology
- Personnel screening measures for granting access to the controlled item/technology
- Training and awareness program – Authorized project personnel shall complete an initial export control training, along with annual follow up training.
- Self-evaluation program – An internal assessment process shall be used to review procedures, ensure all information in the TCP is current, and report findings to the Director of Export Controls on at least an annual basis.
- Appropriate security measures for disposal of the item/technology when use is complete

## 2.5 Licensing

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

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

## 2.6 International Travel

The risks associated with carrying electronic devices while traveling arise from two sources: the likelihood that a device will be compromised and the impact of such a compromise. These risks fall into two main categories: exposing information the university is required to protect (i.e., restricted, classified or export controlled data) and being compromised by malware while traveling. The likelihood of being compromised by malware is greatest when traveling outside of the US and especially high when governments operate and manage the Internet. International travelers should take extra precautions. For travel to Iran, answers to frequently asked questions can be found at <https://siusystem.edu/academic-affairs/export-controls/faqs.shtml#iran>.

All SIU travel to certain countries require that an Informational Technology Services clean laptop be used during SIU business travel to these countries. These clean laptops provide both the employee and the SIU System extra security in the event that the laptop is compromised and will assist both the employee and the SIU System with maintaining export control compliance. See details of the SIU Clean Laptop Program at Appendix 3.3 and on the Export Controls website at <https://siusystem.edu/academic-affairs/export-controls/pdf/SIU-CLEAN-LAPTOP-PROGRAM.pdf>.

## 2.7 Training

Training is the foundation of a successful export compliance program. Well-informed employees minimize the likelihood that inadvertent violations of the law will occur. The greatest risk of non-compliance of export laws and regulations occurs during casual conversations in person, on the

telephone, or via e-mail. The way to prevent these types of violations is through awareness and training.

The Export Controls Office will prepare updated training materials and will ensure that employees or students engaged in export-controlled activities receive the appropriate briefing. The office will also maintain records of training or briefings provided. In addition to in person training sessions, training on export controls is available in the CITI system. Additional resources addressing special topics are available on the export control web page found at <http://siusystem.edu/academic-affairs/export-controls/index.shtml>.

## 2.8 Recordkeeping

SIU's policy is to maintain export-related records based on individual controlled items or activities. Unless otherwise provided for or instructed by the Office of the General Counsel, all records shall be maintained consistent with the SIU record retention policy, and shall be retained no less than 5 years after the TCP termination date or license termination date, whichever is later.

If ITAR-controlled technical data is exported under an exemption, certain records of the transaction must be kept even beyond SIU's 5-year retention period.<sup>4</sup> Those records include:

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

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

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

---

<sup>4</sup> See 22 C.F.R. §§ 122.5 and 123.26.

<sup>5</sup> See 15 C.F.R. § 762.6.

## 2.9 Monitoring and Auditing

In order to maintain SIU's export compliance program and to ensure consistent adherence to U.S. export laws, the Export Controls Office may conduct internal reviews of TCPs and export records. The purpose of the reviews is to: (i) identify possible violations; and (ii) identify deficiencies in training, procedures, etc. that can be rectified.

## 2.10 Detecting and Reporting Violations

Due to export control laws and regulations, it may sometimes be necessary to restrict certain individuals' ability to conduct, access the results of, or otherwise participate in certain research projects and other University activities. Because violations of export controls, including inadvertent failures to comply, may result in severe criminal and civil penalties both for individual faculty, staff, and students, as well as for Southern Illinois University as an institution, export compliance is the shared responsibility of all members of the University community.

Suspected violations should be reported to the Director of Export Controls, other Export Controls staff, SIU Office of General Counsel (OGC), or the SIU Export Control compliance hotline (618-650-2476). In consultation with OGC, the Director of Export Controls will initiate an investigation in conjunction with the affected administrative or academic units to determine if a violation has occurred and if subsequent self-disclosure to a government agency will be made.

Violations can result not only in significant civil or criminal liabilities for SIU and the individuals involved, up to and including termination of employment, but also in damage to national security and to the University's standing as an institution of research and learning. Early detection, investigation, and resolution, along with voluntary self-disclosure, can aid in lessening penalties and the impact of violations.

If voluntary self-disclosure is deemed as the best course of action, the Director of Export Controls may provide the government agency with a supplementary letter with a thorough narrative account of:

1. The project's description and background
2. A description of the suspected violation
3. The items and controlled categories involved
4. The dates the violations occurred
5. Countries involved
6. Individuals involved and their citizenship
7. Explanation of why the alleged violation occurred
8. Corrective actions taken

9. SIU's commitment to export controls compliance

Once the initial notification and supplementary letter have been reviewed, the University will follow the relevant government agency's instructions. The Director of Export Controls should retain documentation of the investigation, its results, and any corrective action taken in accordance with all University policies and federal laws and regulations.

---

# 3 Appendices

---

Appendix 3.1: Glossary of Abbreviations

Appendix 3.2: Red Flags for Shipping Internationally

Appendix 3.3: SIU Clean Laptop Program

Appendix 3.4: Export Controls Decision Tree

Appendix 3.5: University Guidelines (Section 12: Export Controls)

Appendix 3.6: SIU Export Control Office Contact Information

## Appendix 3.1: Glossary of Abbreviations

AECA- Arms Export Control Act

AES - Automated Export System

BIS - Bureau of Industry and Security

CCL - Commerce Control List

DDTC - Directorate of Defense Trade Controls

EAR - Export Administration Regulations

ECCN - Export Control Classification Number

ITAR - International Traffic in Arms Regulations

OFAC - Office of Foreign Asset Controls

ORS - Office of Research Services

SDN - Specially Designated National

TCP - Technology Control Plan

USML - United States Munitions List

## Appendix 3.2: Red Flags for Shipping Internationally

### Things to Look for in Export Transactions

Use this as a checklist to discover possible violations of the Export Administration Regulations. You may also wish to visit our page, "[Know Your Customer Guidance](#)."

- The customer or its address is similar to one of the parties found on the Commerce Department's [BIS'] list of denied persons.
- The customer or purchasing agent is reluctant to offer information about the end-use of the item.
- The product's capabilities do not fit the buyer's line of business, such as an order for sophisticated computers for a small bakery.
- The item ordered is incompatible with the technical level of the country to which it is being shipped, such as semiconductor manufacturing equipment being shipped to a country that has no electronics industry.
- The customer is willing to pay cash for a very expensive item when the terms of sale would normally call for financing.
- The customer has little or no business background.
- The customer is unfamiliar with the product's performance characteristics but still wants the product.
- Routine installation, training, or maintenance services are declined by the customer.
- Delivery dates are vague, or deliveries are planned for out of the way destinations.
- A freight forwarding firm is listed as the product's final destination.
- The shipping route is abnormal for the product and destination.
- Packaging is inconsistent with the stated method of shipment or destination.
- When questioned, the buyer is evasive and especially unclear about whether the purchased product is for domestic use, for export, or for reexport.

If you have reason to believe a violation is taking place or has occurred, you may report it to the Department of Commerce by calling its 24-hour hot-line number: 1 (800) 424-2980. Or, if you prefer, complete our Confidential Lead/Tip **Form**.

## Appendix 3.3: SIU Clean Laptop Program

### Purpose:

The risks associated with carrying electronic devices while traveling arise from two sources: the likelihood that your device will be compromised and the impact of such a compromise. These risks fall into two main categories: exposing information the university is required to protect (i.e., restricted, classified or export controlled data) and being compromised by malware while traveling. The likelihood of being compromised by malware is greatest when traveling outside of the US and especially high when governments operate and manage the Internet. International travelers should take *extra* precautions. Understand that foreign universities, governments, and companies are often linked. Any inquiry regarding your research may have an ulterior motive, such as stealing intellectual property. Be cautious of unsolicited requests and questions about your research or other sensitive information. These clean laptops provide both you and the SIU System extra security in the event that the laptop is compromised and will assist both you and the SIU System with maintaining export control compliance.

### Who Should Use The SIU Clean Laptop Program?

All SIU System employees, SIUE faculty and staff, SIUC faculty and staff, SIU School of Medicine faculty and staff; as well as all satellite campus faculty and staff, including but not limited to, the SIU School of Dental Medicine, The National Corn to Ethanol Research Center, The East St. Louis Center, SIU Law School and all SIU Extended Campus locations that travel to the designated foreign countries.

**All SIU travel to the below countries WILL REQUIRE that an Informational Technology Services clean laptop be used during SIU business travel to those countries.**

Your SIU issued laptop computer **SHALL NOT** be transported to any of the below countries.

IRAN	SYRIA	SUDAN
CUBA	NORTH KOREA	UKRAINE (Crimea Region)
RUSSIA	CHINA	VENEZUELA
IRAQ	CAMBODIA	

### For How Long Can I Borrow A Laptop?

The length of checkout should not be longer than the below periods. If you must keep it longer, specify the reason in your request email. Note: ITS may be unable to accommodate your request.

## To Request A Clean Laptop For Travel, Do The Following:

### SIUC:

1. Submit a Travel Laptop Reservation request at <https://ithelp.siu.edu> by clicking on Travel Laptop in the Hardware section of Computers & Technology.
2. Complete the [TMP Certification.docx](#) and return to the Director of Export Controls at [twakela@siue.edu](mailto:twakela@siue.edu)
3. Allow at least a week to prepare the laptop for travel. The Office of Information Technology (OIT) has limited availability and requests will be processed on a first come, first serve basis.
4. The length of checkout should not be longer than a month. If you must keep it longer, specify the reason in your request. Note that OIT may be unable to accommodate your request.
5. Pick up the travel laptop at the SalukiTech Service Center in Morris Library upon notification.
6. Return the travel laptop to the SalukiTech Service Center when you return.
7. **VERY IMPORTANT:** Upon returning to the United States, change your password as soon as possible. **DO NOT CHANGE YOUR PASSWORD ON THE TRAVEL LAPTOP.**

Note: VPN is required to access some campus resources while traveling. If you need VPN access, please visit <https://ithelp.siu.edu> and click on Request Access in the VPN section of Information Security.

### SIUE:

1. Apply for 2-Factor VPN access before requesting a travel laptop from ITS. This will allow you to securely access everything you need in association with your work at SIUE. In some countries, this will be the only way you can access your SIUE resources remotely. Start here to see if you need VPN access or to update your existing access to 2-factor: [https://www.siu.edu/its/fac\\_staff/vpn.shtml](https://www.siu.edu/its/fac_staff/vpn.shtml)
2. Complete the [TMP Certification.docx](#) and return to the Director of Export Controls at [twakela@siue.edu](mailto:twakela@siue.edu)
3. Email the ITS Help Desk at [help@siue.edu](mailto:help@siue.edu)
4. Include your name, eID, the date needed, destination, and date to be returned
5. Allow at least 10 business days to prepare the laptop for travel. ITS has limited availability on travel laptops and requests will be processed on a first come, first serve basis.
6. The length of checkout should not be longer than a month. If you must keep it longer, specify the reason in your request email. Note that ITS may be unable to accommodate your request.
7. **VERY IMPORTANT:** Upon returning to the United States, change your password as soon as possible. **DO NOT CHANGE YOUR PASSWORD ON THE TRAVEL LAPTOP.**

## SIU-MED:

1. Email [techsupport@siumed.edu](mailto:techsupport@siumed.edu). Include your name, the date you need a laptop, and the date the laptop will be returned.
2. Complete [TMP Certification.docx](#) and return to the Director of Export Controls at [twakela@siue.edu](mailto:twakela@siue.edu)
3. Please allow at least a week to prepare the laptop for travel. Information Technology has a limited number of travel laptops available. Travel laptops will be reserved on a first come, first served basis.
4. The length of the laptop checkout should not be more than three weeks. If you need a laptop for a longer period, please specify the reason in your request email. Note: Information Technology may be unable to accommodate extended requests due to equipment availability.
5. Return the travel laptop to Information Technology when you return from your travel.
6. **VERY IMPORTANT:** Upon returning to the United States, your SIUMED password will need to be changed as soon as possible. **DO NOT CHANGE YOUR PASSWORD ON THE TRAVEL LAPTOP.**
7. If you need assistance, please contact the Information Technology Service Desk at [techsupport@siumed.edu](mailto:techsupport@siumed.edu) or 217-545-HELP.

## What Types Of Laptops Are Available?

ITS has available for travel

- Windows 7 - Dell Laptop Latitude E6520, and
- Dell Laptop Latitude E6530

## What Software Is Available On These Laptops?

The laptop will have:

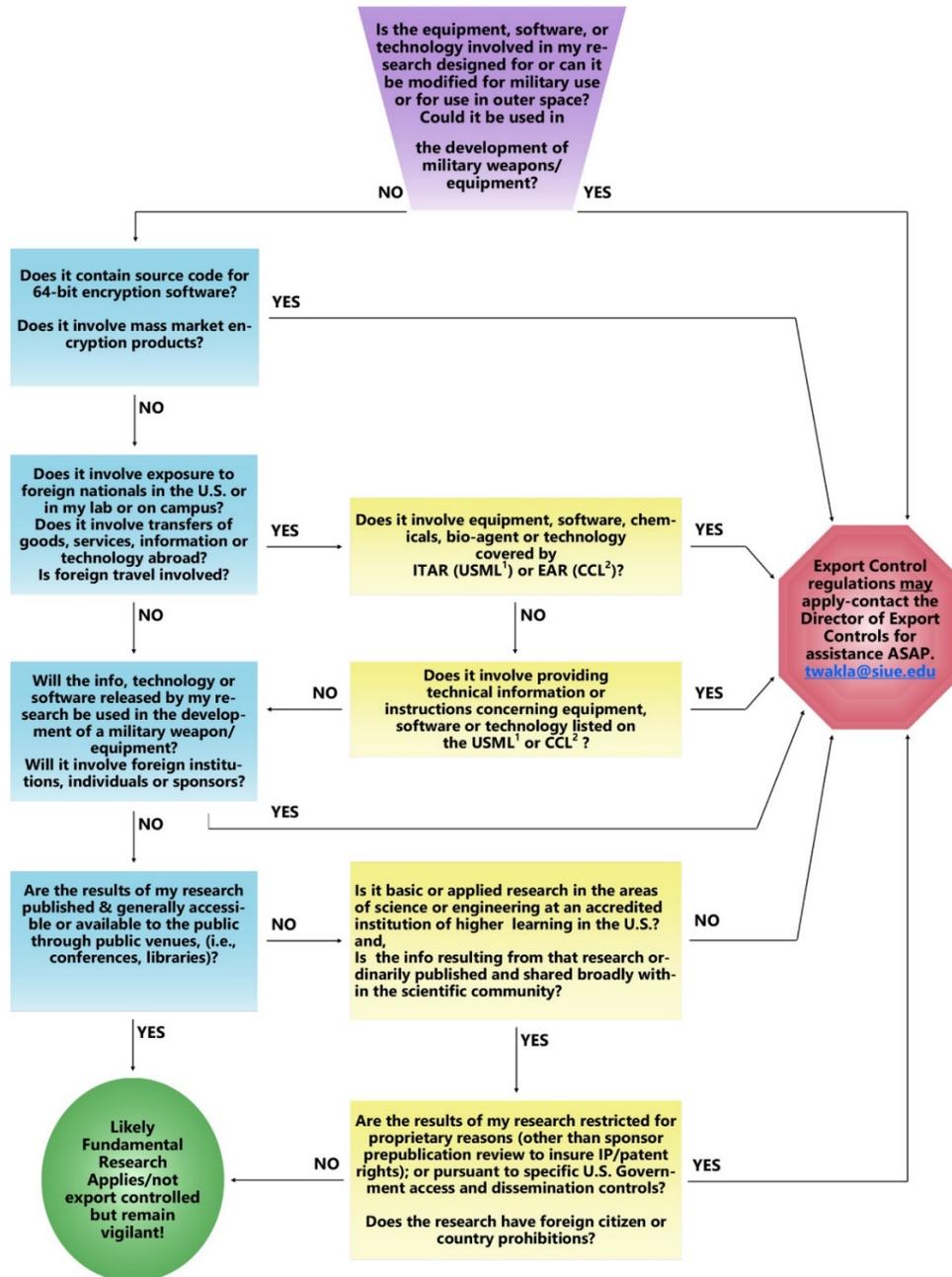
- Microsoft Office Adobe Reader
- Internet Explorer
- VLC Media Player
- Mozilla Firefox/Google Chrome

## What Happens Upon My Return?

After returning to the United States, you will need to change your University ID password. You can do this either by coming to our office to have it changed, or by changing it yourself using your home or office computer. Do not use the travel laptop to change your password.

## Appendix 3.4: Decision Tree

### DO I HAVE A POTENTIAL EXPORT CONTROL ISSUE?



<sup>1</sup>United States Munitions List (International Traffic in Arms Regulations (ITAR)) available online at: [https://www.pmdc.state.gov/regulations\\_laws/itar.html](https://www.pmdc.state.gov/regulations_laws/itar.html)

<sup>2</sup>Commerce Control List (Export Administration Regulations (EAR)) available online at: <http://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear>

## Appendix 3.5: University Guidelines (Section 12: Export Controls)

**Section 12**      **Export Controls**  
**Issued:**        **December 2021**  
**Replaces:**     **March 2021**

---

### 12.1 Introduction

These Guidelines for University-wide U.S. export control compliance are intended to provide the Office of the President, The Board of Trustees and each SIU campus, with the information and means to coordinate export control policy. They establish the administrative foundation for the export controls compliance program by which SIU will comply with U.S. export control laws. These guidelines are drafted in conjunction with the Export Control Policy, which can be found on the SIU Board of Trustees Policies website at <https://siusystem.edu/board-oftrustees/legislation/board-legislation-policies.shtml#7N>.

### 12.2 Leadership Responsibilities

Leadership, (SIU President, Chancellors of each SIU campus and the Dean of SIU-School of Medicine) are responsible for being aware of export control issues in their area of responsibility. No individual in a leadership position at SIU shall knowingly engage in an activity or commit the University to engage in an activity that violates U.S. export control laws and regulations. Leadership is responsible for ensuring their areas follow appropriate export control regulations. These individuals are responsible for reviewing the materials on SIU's Export Control Website and consulting with the Director of Export Controls when export controls apply. Leadership acknowledges its responsibility to export control compliance in a "Commitment to Compliance" correspondence located on the SIU System Export Controls website at <https://siusystem.edu/academic-affairs/export-controls/pdf/Letter-to-Community.pdf>.

### 12.3 Employee Responsibilities

University employees are responsible for being aware of export control issues in their departments and research. Any violation of U.S. export control laws must be reported to their supervisor or the Director of Export Controls. All employees are required to participate in export control training every three years. It is the responsibility of the Principal Investigator/Project Director (PI/PD) on any project or contract to be aware of the Export Control Policy and to notify the Director of Export Controls of potential export control issues. No employee of the SIU community may knowingly engage in any activity or commit the University to engage in any activity that violates U.S. export control laws and regulations. Employees are responsible for reviewing the materials on the SIU System Export Control website and consulting with the Director of Export Controls when export controls apply.

### 12.4 Restricted Party Screening

The U.S. government restricts SIU from exporting any service or product to any party listed in a U.S. government export denial, blocked, or debarred persons lists. The failure to comply with this regulation is a violation of U.S. law and can result in criminal or civil prosecution, as well as sanctioned under the institutions appropriate disciplinary process. All SIU employees shall abide by this regulation and comply with the SIU Restricted Party Screening Procedure, located on the SIU System Export Controls website at <https://siusystem.edu/academic->

[affairs/exportcontrols/policies.shtml](https://siusystem.edu/academic-affairs/exportcontrols/policies.shtml); and notify the Director of Export Controls of a possible restricted party.

### **12.5 Clean Laptop Requirements**

The risks associated with carrying electronic devices while traveling abroad can be high. They include but are not limited to exposing private information the university is required to protect (i.e., restricted data) and being compromised by malware while traveling. The likelihood of being compromised by malware is greatest when traveling outside of the US and especially high when governments operate and manage the Internet. International travelers should take extra precautions. Information, technology, software, and equipment you take with you may be subject to U.S. export control laws. One must ensure that all the information and software on a laptop can be safely and legally transported to another country. While traveling to certain high-risk countries, all SIU employees, including administration, staff and faculty, shall abide by the SIU Clean Laptop Procedure, located on the SIU System Export Controls website at <https://siusystem.edu/academic-affairs/export-controls/policies.shtml>. All SIU employees are responsible for reviewing and complying with the procedure before they travel internationally to the high-risk countries of concern.

### **12.6 Sabbatical Documents**

Sabbaticals can be an integral part of Faculty research and may include foreign components or research in foreign countries. In order to properly comply with U.S. export control laws and regulations, the SIU Export Controls Office shall, in conjunction with the Provost's Office on each SIU System campus, review all sabbatical applications that have a foreign component for export control issues. A foreign component is a sabbatical occurring in a foreign country, a sabbatical with foreign co-researcher or a sabbatical sponsored by or involving a foreign business or government. Sabbatical applications shall be provided to the SIU Export Control Office before the Provost(s) approves or denies the sabbatical application. Specific procedures shall be documented in the SIU Export Controls Office's written procedures which can be found on the SIU System Export Controls website at <https://siusystem.edu/academic-affairs/exportcontrols/policies.shtml>.

### **12.7 Conflict of Interest Documents**

The term "conflict of interest in research" refers to situations in which financial or other personal considerations may compromise, or have the appearance of compromising a researcher's professional judgment in conducting or reporting research. The presence of conflicts of interest poses a problem for professional and public trust in research and the research enterprise. Effective means of identifying and managing conflicts are an important element in successfully achieving the goals of research.

Conflict of interest in research may also include foreign components or research in foreign countries. In order to properly comply with U.S. export control laws and regulations, the SIU Export Controls Office shall, in conjunction with the applicable campus office on each SIU System campus, review all conflict of interest forms that have a foreign component for export control issues. A foreign component is research or an interest that could occur in a foreign country, research or a possible interest with a foreign co-researcher or research sponsored by or

involving a foreign business or government. Conflict of interest forms shall be provided to the SIU Export Control Office before the applicable campus office finalizes its review of the conflict of interest form. Specific procedures shall be documented in the SIU Export Controls Office's written procedures which can be found on the SIU System Export Controls website at <https://siusystem.edu/academic-affairs/export-controls/policies.shtml>.

### **12.8 Transfer of University Intellectual Property**

The transfer of University intellectual property can create an export control risk. SIU's central Office of Technology Management and Industry Relations works with SIU faculty, students, and staff to protect and commercialize intellectual property generated from all system campuses. In order to properly comply with U.S. export control laws and regulations, the SIU Export Control Office shall coordinate with the Office of Technology Management and Industry Relations to review agreements and request forms as detailed in the procedures below, as well as any other similar matters, that have a foreign component or technology that may be export-controlled. A foreign component is a matter in which there is involvement with a foreign entity or individual. Technology may be export-controlled if it is controlled by a U.S. export control law or regulation. The Export Controls office shall provide pre-approved export control language to the Office of Technology Management and Industry Relations that can be used in agreements, requiring each party to comply with all relevant United States laws governing the exports and reexports of technical data or commodities. The Export Controls office shall review and approve all agreements that do not use the pre-approved export control language. Specific procedures shall be documented in the SIU Export Controls Office's written procedures which can be found on the SIU System Export Controls website at <https://siusystem.edu/academic-affairs/exportcontrols/policies.shtml>.

### **12.9 Technology Control Plan**

SIU may be in possession of items that are subject to U.S. export control laws and regulations. SIU aims to engage foreign nationals and host international visitors in the most welcoming manner possible, while still maintaining compliance with U.S. laws and regulations governing the export of certain equipment and materials, as well as protecting sensitive data.

Federal laws and regulations, including, but not limited to, the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR) regulate the transfers of physical items, technical information, data, products, software, hardware, biological materials, or chemical materials, hereafter referred to as "*export-controlled items and information*", to certain non-U.S. persons and entities. It is unlawful under the EAR or ITAR to send or take *export-controlled items and information* out of the United States without proper authorization. This includes disclosing information orally or visually or transferring *export-controlled items or information* to a foreign person inside or outside the U.S. without proper authorization.

Under the ITAR or the EAR, an export license may be required for foreign nationals to access *export-controlled items and information*. A foreign person is a person who is not a U.S. citizen, a U.S. permanent resident or a person who is protected under the U.S. refugee and asylum status. The law does not make exceptions for foreign graduate students.

In order to follow best practices, SIU shall implement a Technology Control Plan (TCP) whenever a research activity is subject to export controls. The purpose of the TCP is to help

ensure compliance with U.S. export control laws and regulations, to appropriately secure the *export-controlled items and information* from unauthorized access, and ensure the research teams understand their compliance obligations and responsibilities.

The Exports Control Office shall assist the Principal Investigator (PI) of the project to develop and implement the TCP. Before any individual may have access to *export-controlled items or information*, he or she must be informed of the conditions of the TCP and agree to comply with the security measures outlined in the TCP. SIU personnel subject to a TCP must complete an initial in-person export control training when the TCP is implemented and are required to complete follow up training annually. In addition, the Export Controls Office shall monitor compliance with the TCP and confirm its accuracy on an annual basis with the PI. It is the PI's responsibility to contact the Export Controls Office if any changes need to be made to the TCP during the course of the year.

Specific procedures shall be documented in the SIU Export Controls Office's written procedures which can be found on the SIU System Export Controls website at <https://siusystem.edu/academic-affairs/export-controls/policies.shtml>.

### **12.10 Handling Export Violations and Taking Corrective Actions**

Due to export control laws and regulations, it may sometimes be necessary to restrict certain individuals' ability to conduct, access the results of, or otherwise participate in certain research projects and other University activities. Because violations of export controls, including inadvertent failures to comply, may result in severe criminal and civil penalties both for individual faculty, staff, and students, as well as for Southern Illinois University as an institution, export compliance is the shared responsibility of all members of the University community.

Suspected violations should be reported to the Director of Export Controls, other Export Controls staff, SIU Office of General Counsel (OGC), or the SIU Export Control compliance hotline (618-650-2476). In consultation with OGC, the Director of Export Controls will initiate an investigation in conjunction with the affected administrative or academic units to determine if a violation has occurred and if subsequent self-disclosure to a government agency will be made.

Violations can result not only in significant civil or criminal liabilities for SIU and the individuals involved, up to and including termination of employment, but also in damage to national security and to the University's standing as an institution of research and learning. Early detection, investigation, and resolution, along with voluntary self-disclosure, can aid in lessening penalties and the impact of violations.

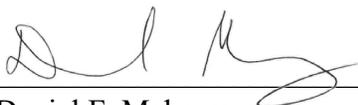
Specific procedures shall be documented in the SIU Export Controls Office's written procedures which can be found on the SIU System Export Controls website at <https://siusystem.edu/academic-affairs/export-controls/policies.shtml>.

### **12.11 Campus Department Coordination**

In order to identify activities and assets which may be subject to export controls, as well as to prevent activities with restricted parties, the Export Controls office shall coordinate with campus departments that may be able to assist in export control activities.

Specific procedures for the coordination with each of these departments shall be documented in the SIU Export Controls Office's written procedures which can be found on the SIU System

Export Controls website at <https://siusystem.edu/academic-affairs/export-controls/policies.shtml>.

  
\_\_\_\_\_  
Daniel F. Mahony

\_\_\_\_\_  
Date 12/14/2021

President

## Appendix 3.6: SIU Export Control Office Contact Information

Export Controls is under the direction of the [Vice President for Academic Affairs](#) and is responsible for helping the University community understand and comply with export control laws and regulations. For additional information, tools to assist in determining how the regulations apply to your activity, and assistance with export control concerns, please contact the Export Controls Office using the contact information below.

### **Staff Contact Information:**

Todd Wakeland, JD, Director of Export Controls  
3311 Rendleman Hall  
Box 1259  
Edwardsville, Illinois 62026  
[twakela@siue.edu](mailto:twakela@siue.edu)  
618-650-2476

Brenda Martin, Export Control Officer  
363 Woody Hall  
Mailcode 4344  
Carbondale, IL 62901  
[bjmartin@siu.edu](mailto:bjmartin@siu.edu)  
618-453-2308