

**Section 12      Export Controls**  
**Issued:          July 2020**  
**Replaces:**

---

**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 attached herein below as **Attachment 12A**.

**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 attached herein below as **Attachment 12B**.

**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 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, attached below as **Attachment 12C**; 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, attached herein below as **Attachment 12D**. All SIU employees are responsible for reviewing and complying with the procedure before they travel internationally to the high-risk countries of concern.

A handwritten signature in blue ink, appearing to read 'Daniel F. Mahony', is written over a horizontal line.

Daniel F. Mahony  
President

A handwritten date '9/25/20' in blue ink is written over a horizontal line.

Date

## Attachment 12-A: Export Control Policy

### 1. Purpose

To address the Southern Illinois University – System (SIU-S) obligations to comply with federal export controls. This policy applies to the SIU-S and each of its campuses-- Southern Illinois University Carbondale (SIUC), Southern Illinois University Edwardsville (SIUE), and the Southern Illinois University School of Medicine (SIUSOM). The policy codifies SIU's commitment to compliance with U.S. export controls, identifies the corresponding responsibilities of SIU-S personnel, and establishes the administrative foundation for the SIU-S export controls compliance program. These steps are required to ensure SIU-S compliance with U.S. export controls.

### 2. Scope

This policy applies to all members of the SIU-S community, including but not limited to employees, tenure-and non-tenure-track faculty, lecturers, students, postdoctoral fellows, postdoctoral scholars, and other postdoctoral personnel, independent researchers, visiting scholars, visiting scientists, contractors, subcontractors, and volunteers.

### 3. Policy

SIU-S is committed to complying with U.S. export controls including without limitation the Arms Export Control Act ("AECA"), 22 U.S.C. 2751 *et seq.*; the International Traffic in Arms Regulations ("ITAR"), 22 C.F.R. 120 *et seq.*; the Export Administration Regulations ("EAR"), 15 C.F.R. 730 *et seq.*; the Foreign Assets Control Regulations ("FACR"), 31 C.F.R. 500 *et seq.*; and all campus policies and procedures related to export controls.

SIU-S recognizes the importance of these laws and regulations and expects compliance from all of its personnel. No members of the SIU-S community may engage in any activity or commit the University to engage in any activity that violates U.S. export control laws and regulations. Individuals involved in research and academic projects that are subject to export controls must follow the requirements that are appropriate for the roles they serve. These individuals are responsible for reviewing the materials on the SIU-S Export Control Website and consulting with the Director of Export Controls when export controls apply.

SIU-S export control compliance efforts, screening, and training are coordinated through the Director of Export Controls. Export Control procedures will be drafted by the Director of Export Controls in conjunction with each campus. It is the responsibility of the Principal Investigator/Project Director (PI/PD) on any project or contract to be aware of this policy and to notify the Director of Export Controls of potential export control issues.

Violations can result not only in significant civil or criminal liabilities for SIU-S, and potentially 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.

#### 4. Definitions

- **Deemed Export:**

Any release of controlled technology or source code subject to the Export Administration Regulations ("EAR") to a foreign person in the U.S. is "deemed" an export to the person's country or countries of nationality. This deemed export rule does not apply to persons lawfully admitted for permanent residence in the U.S. and does not apply to persons who are protected individuals under the Immigration and Naturalization Act.

Refer to section 734.2(b) of the EAR. A "deemed" export situation can occur by access/use in research or training, visual inspection, or an oral exchange of information.

- **Export Administration Regulations ("EAR"):**

Regulations implemented by the U.S. Department of Commerce, which control the export of dual-use technologies (i.e., items used or having the potential to be used for both military and commercial purposes that could adversely affect national security if exported).

- **International Traffic in Arms Regulations (ITAR):**

Regulations implemented by the U.S. Department of State to regulate military or defense related articles, technologies, and services.

- **Office of Foreign Asset Control (OFAC) Sanctions:**

A department of the U.S. Treasury that enforces economic and trade sanctions against countries and groups of individuals involved in terrorism, narcotics, and other disreputable activities enforced by the Office of Foreign Asset Control of the U.S. Department of Treasury.

- **Public Domain as defined by EAR:**

Covers published information and software. Information is "published" when it becomes generally accessible to the interested public in any form, including but not limited to:

- publication in periodicals, books, print, electronic, or other media available for general distribution, either free or at a price that does not exceed the cost of reproduction and distribution
- available at libraries open to the public or university libraries
- issued patents or open patent applications published and available at any governmental patent office
- released or publicly discussed at an open conference, meeting, seminar, trade show, or other open gathering

- **Public Domain as defined by ITAR:**

Covers published information generally accessible or available to the public through:

- sales at newsstands and bookstores

- subscriptions available without restriction
- second class mailing privileges granted by the U.S. government
- libraries open to the public or from which the public can obtain documents
- patents available at any patent office
- through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public, in the U.S.
- public release (i.e., unlimited distribution) in any form
- 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

### **5. Export Controls Record Retention**

SIU-S must comply with regulatory requirements regarding export control-related recordkeeping. These records must be organized to be available when requested by U.S. governmental authorities or for internal audit purposes. Records include printed and hard copy documents, as well as electronic records (including e-mail, e-mail attachments and other electronic files). All records will be retained for a minimum period of **five (5) years** from the date of export or from the date of license expiration, as per the requirements of ITAR Section 123.22 and EAR Section 762.6. Departments, researchers and all SIU-S offices must keep soft or hard copies of all their export documentation, including Restricted Party Screens, financial records such as purchase orders, and shipping documentation (commercial/pro forma invoices, packing lists, FedEx and other international freight forwarder/courier documents), in their research project files for a period of five years from the date of the export, re-export, or controlled deemed export.

(8-15-18)

Attachment 12-B: Letter to Community

1



To: The SIU community

From: SIU System President Dan Mahony

SUBJECT: Export Regulations

---

The Southern Illinois University System (SIU) is fully committed to compliance with the export control laws and regulations of the United States, and has established an export control compliance program as part of this commitment. The SIU Director of Export Controls has been charged with oversight of export control matters on all campuses (<http://siusystem.edu/academic-affairs/export-controls/index.shtml> ).

U.S. export controls are increasingly complex, and include laws and regulations enforced by multiple government agencies. Among these are the Department of Commerce (EAR: Export Administration Regulations), The Department of State (ITAR: International Traffic in Arms Regulations), and the Treasury Department (OFAC: Office of Foreign Assets Control). Export Controls include restrictions on various activities, such as:

- the physical export of items and technology;
- the disclosure of certain information to foreign nationals, even within the U.S. ( "Deemed Exports");
- providing certain training to foreign nationals or entities; and
- providing information or services to sanctioned persons, entities, and countries.


Accordingly, there are multiple activities at SIU that require Export Control review and approval to ensure compliance with these controls. Included among these activities are all international travel, visits by foreign persons to SIU, and international research collaborations, to list a few. Activities that are found to be in violation of these laws and regulations are punishable under both civil and criminal sanctions and penalties. These penalties can apply to both SIU and the individual violator. Additional sanctions could include suspension of faculty research or suspension of all governmental research by the entire SIU community.

SIU is committed to the preservation of academic freedom. Fortunately, most, but not all, research activities at SIU fall under the "Fundamental Research Exclusion" (FRE), which


2

provides that basic and applied research activities NOT subject to publication or access restrictions will not be subject to export controls. However, the export regulations are complex and continually changing, so it is important to consider each activity on an individual basis.

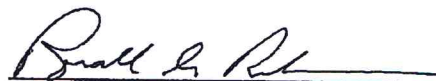
It is the responsibility of SIU faculty, administrators, and staff to be aware of and comply with these federal laws and all SIU policies and procedures. SIU's Director of Export Controls offers in-person export control training, and is available to assist all faculty, staff, administration, and students to interpret and meet the regulations. We encourage you to contact the Director of Export Controls with any questions, and in advance of any anticipated activities that might be impacted by these regulations. Please see, <http://siusystem.edu/academic-affairs/export-controls/index.shtml> for additional information, including analytical tools, regarding applicable regulations.

  
President SIU System  
Dan Mahony, PhD


7/1/20  
Date

  
Chancellor SIUC  
Austin Lane, PhD

7/1/20  
Date

  
Chancellor SIUE  
Randy Pembroke, PhD

7/1/20  
Date

  
Dean and Provost, SIU School of Medicine  
Jerry Kruse, MD, PhD

7/8/20  
Date

## Attachment 12-C: Export Control Procedures

**EXPORT CONTROLS PROCEDURES**

<b>Title: Restricted Party Screening in Virtual Compliance</b>		
<b>Procedure #:</b> EC001	<b>Effective Date:</b> 06/13/2018	<b>Author:</b> Todd Wakeland
<p><b>Purpose/Definitions:</b> The U.S. government restricts the University 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 the above regulation is a violation of U.S. law and can result in criminal or civil prosecution, as well as denial of export privileges.</p> <p><b>Procedure:</b></p> <ol style="list-style-type: none"> <li>1. Go to <a href="http://www.visualcompliance.com">www.visualcompliance.com</a></li> <li>2. Login with your username and password</li> <li>3. Click the RPS tab, enter the following information:               <ol style="list-style-type: none"> <li>a. Company name (also put company name in the comments box, see directions below)</li> <li>b. After you screen the company name, delete that name and then go to the individual name First, Middle (or initial), Last and enter it exactly as received.</li> <li>c. Any address information you have</li> <li>d. Country of birth (if available)</li> </ol> </li> <li>4. Click in the empty box next to the Comment box and add the reason you are screening the company or individual. For example: NIAR tour/ Professor Proton or person requesting the tour/ ABC Engineering Company or name of the group touring. Any information that may be needed to review the file if a hit is received in the future.</li> </ol> <p><b>Note:</b> If you have multiple names to screen you can click on the "Search Same Keywords Again" after you have completed the first screening so you do not have to retype all the above information again.</p>		

5. Select the Fuzzy Level 2 search option and click "Screen"
6. If the search brings back a result of "**No Matching Records Found**", email the result to yourself by using the, "Email these results" button; then proceed with your normal course of business.
7. If the search returns any results other than "No Matching Records Found" (a hit), further investigation is required; if you did not have a middle name for the individual, request one and add it to your original search. If your search still shows "a hit", pass the information on to the Director of Export Controls. To initiate the review, click "Email these results" and send to [twakela@siue.edu](mailto:twakela@siue.edu). At this point, the project is on hold and the screener must wait for approval from the Director of Export Controls before continuing.

#### **HITS:**

**False Hits:** These are hits that after evaluation are determined to be low risk; most commonly because the individual being screened is not the same individual showing up as restricted. This occurs frequently for individuals with common first and/or last names. When evaluating a situation keep in mind the purpose of the scan (what the person will be doing) and the reason the person is showing up in Visual Compliance. Approval is granted by the Director of Export Controls to allow the requestor to move forward with their request if considered a low risk. For hits that are quickly and easily determined to be a false hit, no additional documentation is required other than the above email in procedure 6.

**Not Enough Data:** If, after exhausting all research possibilities, it cannot be verified whether or not it is a positive hit the following steps will be taken:

- a. The individual will be asked to sign a verification statement that he or she is not on an excluded, debarred, blocked, wanted or otherwise prohibited entity list.
- b. Obtain a copy of the individual's passport, driver's license, or visa;
- c. All copies of relevant communications, signed verification statement and personal identification documents will be filed in the "RPS-Restricted Party Screening Info – Hit Documentation" file within the Director of Export Controls Office;
- d. Proceed with the transaction

If the individual is unwilling or unable to provide the required documentation to assist the Southern Illinois University System (SIU-S) in verifying he or she is not a restricted party individual, then the activity shall be terminated.

NOTE: In special circumstances, the Associate Provost for Research, the Vice Chancellor for Research or the Associate Dean for Research, may authorize the

Research to proceed without the verification statement and/or personal identification document. In such cases, written authorization will be stored in the "Hit Documentation" file as documentation.

**Positive Hits:** If, after verification, it is determined to be a positive hit, the person that searched the matter, will notify the Director of Export Controls. The original requester will also be notified and a discussion will be held to address the matter and determine next steps. In these cases, General Counsel may be involved in the discussion process.

Any companies or individuals who are confirmed as a positive hit will be excluded from conducting **any** business with SIU-S. This restriction applies regardless of funding source (if any).

The Director of Export Controls will create a file on the Person or Company that had a positive hit or false hit stating how that conclusion was reached.

**WHEN TO SCREEN:**

All:	When shipping
HR:	Before hiring anyone
Contracts:	Before replying/sending any correspondence for the first time
	Whenever there is a change in people on or involved with project
PI:	Before replying/sending any correspondence for the first time
	Whenever there is a change in people on or involved with project
Pre-Award:	Before replying/sending any correspondence for the first time
	Whenever there is a change in people on or involved with project
Post-Award:	Before replying/sending any correspondence for the first time
	Whenever there is a change in people on or involved with project
Compliance:	When a request is received for visitors or tour participants to be screened
	When verifying a possible hit
	Whenever it is otherwise required
Purchasing:	When submitting RFP's or making a first time purchase from a vendor

## Attachment 12-D: Clean Laptop Procedures

**EXPORT CONTROLS PROCEDURES**

<b><u>CLEAN LAPTOP PROGRAM FOR INTERNATIONAL TRAVEL</u></b>		
<b>Procedure #:</b> EC002	<b>Effective Date:</b> 02/01/2019	<b>Author:</b> Todd Wakeland
<p><b>PURPOSE/DEFINITIONS:</b> 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 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. 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.</p> <p>Information, technology, software, and equipment you take with you may be subject to U.S. export control laws. You must ensure that all the information and software on your laptop can be safely and legally transported to another country.</p> <p><b>PROCEDURE:</b> To assist in compliance with U.S. export control laws: <b><u>ALL SIU TRAVEL TO THE BELOW COUNTRIES WILL REQUIRE THAT AN INFORMATIONAL TECHNOLOGY SERVICES CLEAN LAPTOP BE USED DURING TRAVEL TO THOSE COUNTRIES. YOUR SIU ISSUED LAPTOP COMPUTER SHALL NOT BE TRANSPORTED TO ANY OF THE BELOW COUNTRIES.</u></b></p> <p><b>RUSSIA</b>  <b>IRAN</b>  <b>SYRIA</b>  <b>SUDAN</b>  <b>NORTH KOREA</b>  <b>CUBA</b>  <b>UKRAINE (CRIMEA REGION)</b>  <b>CHINA</b></p> <p>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. Below is the procedure you must follow if travelling on SIU business or plan on taking your SIU issued laptop on personal business to the designated countries.</p>		

**DIRECTIONS:** TO REQUEST A CLEAN LAPTOP FOR TRAVEL TO THE DESIGNATED COUNTRIES, PLEASE DO THE FOLLOWING.

**SIUE:**

1. Email Sheryl Lauth in ITS at [slauth@siue.edu](mailto:slauth@siue.edu) AND [help@siue.edu](mailto:help@siue.edu). Include your name, eID, the date needed, and date to be returned.
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. ITS have 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 email. Note that ITS may be unable to accommodate your request.
5. Return the travel laptop to ITS once your travel has been completed.
6. **VERY IMPORTANT:** Upon returning to the United States, your password will need to be changed as soon as possible. **DO NOT CHANGE YOUR PASSWORD ON THE TRAVEL LAPTOP.**

**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.**

**SIU - MEDICAL SCHOOL:**

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 the [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.

**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~~