# Export Control Procedures

# University-Wide Export Control Procedures:

### Sponsored Research Proposals:

When developing a proposal for sponsored research, researchers are required to disclose proposed international activities and relationships to the Office of Sponsored Programs, who will work with the Office of Compliance to determine any potential export control compliance and research security requirements.

### MOUs/MOAs with International Institutions:

When exploring research, academic, or exchange agreements with international institutions, the Office of Academic Affairs will ensure that such parties are screened against the U.S. government’s restricted party lists and proactively referred to the Office of Compliance for export review.

### Visa Petitions:

When planning to host Visa holders (e.g., J-1 visiting scholars, H-1 or O-1 employees) within export-sensitive research environments, researchers will be required to complete a Visa/Deemed Export Questionnaire issued by the Office of Compliance, which enables the ECO to determine whether there are deemed export issues associated with the foreign national’s research work or potential campus access.

* + - The U.S. Citizen & immigration Service (USCIS) requires that the University certify whether a Foreign National staff hire (H-1/O-1) will be exposed to any export-controlled research, technology, or tools (instruments, software, materials, or proprietary technology) that may be present in the researcher’s laboratory or office environment, which could result in a deemed export which requires an export license. To address this Certification requirement and address deemed export exposure, the host faculty member or staff supervisor will complete the I-129 Deemed Export Questionnaire.
		- For J-1 visa candidates conducting research in STEM fields and other export controlled/IP-sensitive research environments, current best practice among research universities is to implement an extra level of due diligence concerning the candidate’s home country affiliations and funding source(s). As part of the J-1 visa process, the candidate will complete a Visa J-1 Candidate Due Diligence Form.

### Hosting International Visitors:

The international nature of the University’s work may increase the risk of the University and its representatives engaging with individuals or entities that are subject to certain U.S. government restrictions, controls, or sanctions. To mitigate this risk, individuals or businesses with a foreign affiliation should be screened prior to visiting campus or participating in virtual programming. Visitors and participants should be screened via the Office of Compliance’s International Partner Screening Request Form. This includes but is not limited to the following groups:

* Online program participants
* In-person programs
* Conferences and symposia hosted by Syracuse University
* Visiting faculty and/or guests of a school/college
* Award recipients outside of enrolled students or employed faculty/staff

### International Shipments:

When shipping internationally, all University employees and/or representatives must utilize the University’s online International Shipping Request Form to assist the Export Control Officer in identifying any international shipment that requires prior export control authorization from the U.S. government and/or a special U.S. Customs filing. The form submissions are directed to exportcontrol@syr.edu. Forms are reviewed by the Export Control Officer.

### Technology Sharing:

Certain items used in fundamental research, including instruments, software, biological materials (BSL-2 contained), and technical data, may be export-controlled, even if the research itself is not otherwise publication or citizenship-restricted. As such, the technical data associated with operating or modifying these items may also gain a level of control that would potentially impact foreign national access to such items, i.e. a deemed export. In the event there is the potential for a deemed export to occur, research faculty and staff should contact the ECO for guidance on how to determine whether there is in fact an access concern and how to address it either through a Technology Control Plan (TCP), export license, or other compliance steps.

### International Travel:

All faculty and staff are also required to register any international travel for university purposes via the University’s Campus Safety and Emergency Management Services Travel Registry prior to travel. Any reported and pending travel to OFAC sanctioned countries (including, but not limited to: Belarus, Cuba, Iran, North Korea, Russia, Syria and Ukraine) will trigger a notification to the Export Control Officer via the office email at exportcontrol@syr.edu. Travel requests to these regions are reviewed by the Export Control Officer.

When planning any engagement with any person or entity located in an embargoed country (China, Cuba, Iran, Syria, Russia, Ukraine etc.), proactively contact Export Control Officer who will assist you in complying with OFAC requirements.

### Purchasing and Vendors:

University vendors shall be screened against U.S. government restricted party lists to avoid engagement with restricted parties. In addition, procurement restrictions under the National Defense Authorization Act (NDAA) require that the University avoid using any telecommunications/digital platform procured or otherwise received from certain listed China-based entities, including (but not limited to) Huawei and ZTE, in the performance of federally funded research. The Office of Compliance shall be responsible for implementing proper controls to ensure these restrictions are observed.

### Restricted Party Screening

The international nature of the University’s work creates opportunities where the University and its representatives may encounter individuals or entities that may by subject to limitations based on certain restrictions, controls, or sanctions. The Export Control Officer coordinates screening efforts across various research, academic and business functions, designed to proactively identify parties of concern and can assist in resolving screening issues and determinations.

### Export control classification and license determination

If export control regulations apply to a research project, the principal investigator is expected to work with the Export Control Officer (ECO) to develop an appropriate management plan. The ECO uses the following to manage export-controlled technology and to reduce the potential for violations of export control regulations:

• Technology Control Plans (TCP)

• Federal Export Licenses

• Export License Exceptions or Exemptions

###

## Technology Control Plans and Licenses

If export control regulations apply to a research project, it may be possible to put a Technology Control Plan (TCP) in place instead of applying to the government for an Export License. A TCP may also be required if a contract or other agreement contains language restricting the use of Foreign Nationals or delaying the publication of research results beyond 180 days and/or for reasons other than the review of patent or proprietary sponsor information.

If it is not possible to manage an export-controlled technology through a TCP, then a License may be required.

It is important to note that it is not always possible to obtain a License or to develop an appropriate TCP, so there may be some proposed activities that cannot be conducted at Syracuse University.

1. Technology Control Plans (TCP)

A Technology Control Plan (TCP) is a formal document that outlines procedures the researcher will implement to prevent export-controlled technology from being accessed by unlicensed non-U.S. persons. A TCP may be required to safeguard and control access to items that are export controlled to prevent access to foreign nationals that is prohibited by federal regulations. A TCP may also be drafted for sponsored research projects that do not qualify as fundamental research or otherwise require limitations on access by foreign nationals.

A TCP specifies the security measures that will be used by the research team from the point that the technology is delivered to or generated by Syracuse University to the return or disposal of the technology when the project is completed. The TCP remains in effect for as long as Syracuse University retains the export- controlled data or item, even if the project is over.

“Technology” includes, but is not limited to, certain types of export controlled:

* Equipment (including systems and components)
* Software (source/object code)
* Materials and substances
* Services (e.g., training, instruction)
* Data or information about an item or material
* Funds (e.g., payments)

The TCP must list the names and citizenship of all University personnel who will have access to the controlled technology. Each individual listed on the TCP will be screened against restricted party lists by the ECO. All project personnel listed on the TCP are required to complete export control training.

The PI is the ultimate responsible party for adherence to the TCP by project personnel. The PI is also responsible for helping develop the TCP and for subsequent monitoring. The TCP will include elements such as project information, personnel identification, technology and technical data, security, a thorough description of the information and/or items to be protected; specific measures to control access within the facility; procedures for control of access to equipment; and certification by all project personnel.

TCPs protecting export-controlled information generally require the following:

* Operate in secured laboratory space or during secure times so you can prevent unauthorized persons from observing the activities.
* Lock data, lab notebooks, hard copy reports and research materials in fireproof cabinets in rooms with key-controlled access.
* Do NOT transmit export-controlled information through email.
* Encrypt electronic records on a stand-alone storage device that is not networked with other university computers.
* Limit your discussions about the project or work products to the identified contributing investigators and talk where unauthorized persons are not present.
* Complete a signed confidentiality agreement before discussing with third-party subcontractors, such as identified manufacturing sites.

To fully understand the items being protected, documentation such as export classifications, equipment spec sheets, contracts/agreements etc., may be needed to be included with the TCP as appendices.

Because the TCP is a living document, a copy of the TCP will be maintained by the PI through the duration of the project and be accessible to only those authorized. An official copy of the TCP will be maintained by the responsible department for five (5) years from the project completion or expiration of the license, as applicable. A copy of the TCP will also remain on file with the ECO. An electronic version of the TCP and its supporting documents is acceptable for record retention.

In those cases when a Technology Control Plan (TCP) is required to support an application for export license involving technology transfer, the elements BIS looks for in the TCP are as follows:

* + - Management commitment to export compliance
		- Physical security plan
			* Physically secure space in which export controlled technology (physical items and hard copy documents) are housed
			* Physically secure space where computers used to receive, process, and store export controlled electronic information are
			* Restrict access to spaces to only authorized persons
		- Information security plan
			* Access controls (e.g., user ID/password authentication, firewall, encryption)
			* Storage and transmission
			* Device configuration and management
		- Personnel screening procedures
		- Training and awareness program
		- Self-evaluation program
1. Licenses

A federal license may be required to export ITAR or EAR controlled items from the U.S. to foreign countries, persons, or entities. In general, a license application:

* Lists the items/information being exported
* Identifies the use of the item or information
* Identifies who will use the item(s) or information
* Identifies the individuals or entities in the chain of custody prior to the item(s) or information reaching its destination or the end user
* Indicates the value of the item(s) or information

The license represents approval from the regulatory agencies to export the specific items. A license can be revoked if the individual is found in violation of the export controls regulations.

Plan ahead if you need to apply for a license; it takes time to complete the detailed application. Upon application submission, it may take 14 – 60 days to receive a license from a regulatory agency.

Your export-controlled technology may qualify for a license exception or exemption under the federal export control regulations. There are a variety of license exceptions and exemptions available in the federal regulations, each of which has its own set of requirements. If you can satisfy those requirements, your technology may qualify for a license exception or exemption, and you may be able to export the controlled technology without the need to apply for an export license.