

|  |
| --- |
|  |
| Export Control Guidelines |
|  |

*Export Control laws are complex and specific to each circumstance. Rules, regulations, and laws related to export control are updated frequently. This manual is meant to serve as a guide to provide basic information related to export controls. It should not be relied upon exclusively nor should it be considered legal advice. For further information related to export controlled items or research, please contact UNCG’s Export Control Official.*

Acronyms

**AECA** Arms Export Control Act

**AES** Automated Export System

**BIS** Bureau of Industry and Security

**CCL** Commerce Control List

**CFR** Code of Federal Regulations

**CJ** Commodity Jurisdiction

**DDTC** Directorate of Defense Trade Controls

**DoD** Department of Defense

**EAR** Export Administration Regulations

**ECCN** Export Control Classification Number

**ECO** Export Control Official

**ITAR** International Traffic in Arms Regulations

**OFAC** Office of Foreign Assets Control

**OSP** Office of Sponsored programs

**PI** Principal Investigator

**RPS** Restricted Party Screening

**SDN** Specially Designated Nationals and Blocked Persons List

**TCP** Technology Control Plan

**USC** United States Code

**USML** United States Munitions List

Table of Contents

[Overview of Export Control Regulations 5](#_Toc447097177)

[Introduction 5](#_Toc447097178)

[Export Control Laws at UNCG 6](#_Toc447097179)

[Department of State Regulations (ITAR) 7](#_Toc447097180)

[*Regulatory Authority and Scope* 7](#_Toc447097181)

[*Important ITAR Definitions* 7](#_Toc447097182)

[*The USML Categories* 8](#_Toc447097183)

[*Exporting under the ITAR* 9](#_Toc447097184)

[*Commodity Jurisdiction* 9](#_Toc447097185)

[Department of Commerce Regulations (EAR) 10](#_Toc447097186)

[*Regulatory Authority and Scope* 10](#_Toc447097187)

[*Important EAR Definitions and Concepts* 10](#_Toc447097188)

[*The Commerce Control List* 11](#_Toc447097189)

[*License Exceptions* 12](#_Toc447097190)

[*Commodity Classification* 13](#_Toc447097191)

[*Anti-Boycott Restrictions* 13](#_Toc447097192)

[Department of Treasury Regulations (OFAC) 14](#_Toc447097193)

[*Regulatory Authority and Scope* 14](#_Toc447097194)

[*OFAC Licensing for Country Based Programs* 15](#_Toc447097195)

[Additional Considerations 16](#_Toc447097196)

[*Records/Record Retention* 16](#_Toc447097197)

[*Penalties for Export Violations* 16](#_Toc447097198)

[UNCG Export Control Procedures 18](#_Toc447097199)

[Commitment to Export Control Compliance 18](#_Toc447097200)

[Roles and Responsibilities for Export Controls at UNCG 19](#_Toc447097201)

[**Empowered Official** 19](#_Toc447097202)

[*Office of Sponsored Programs* 19](#_Toc447097203)

[*Research Administrators* 20](#_Toc447097204)

[*Business Administrators* 20](#_Toc447097205)

[*Principal Investigators* 20](#_Toc447097206)

[Export Control Analysis 21](#_Toc447097207)

[*Jurisdiction and Classification* 21](#_Toc447097208)

[Technology Control Plans (TCP) 22](#_Toc447097209)

[Licensing 22](#_Toc447097210)

[Training 23](#_Toc447097211)

[Hiring Practices 23](#_Toc447097212)

[*Hiring Foreign Nationals* 23](#_Toc447097213)

[*Orientation for New Employees* 24](#_Toc447097214)

[*Employee Transfers within UNCG* 24](#_Toc447097215)

[*Employee Termination* 24](#_Toc447097216)

[*Admission Practices* 24](#_Toc447097217)

[Recordkeeping 25](#_Toc447097218)

[Monitoring and Auditing 25](#_Toc447097219)

[Detecting and Reporting Violations 25](#_Toc447097220)

[Appendix 1: Export Control Project Review Questions 27](#_Toc447097221)

[Appendix 2: Technology Control Plan Template 29](#_Toc447097222)

[Appendix 3: Information for US Visa applications 49](#_Toc447097223)

[U.S. Consulate Application Review and Applicant Interview 49](#_Toc447097224)

[Inspection by Bureau of Customs and Border Protection 50](#_Toc447097225)

[SEVIS Validation and Tracking 50](#_Toc447097226)

[Visa Extensions / Renewals 50](#_Toc447097227)

[Applications for Immigration Benefits through the Department of Homeland Security 50](#_Toc447097228)

[Departure procedures about NSEERS 51](#_Toc447097229)

Overview of Export Control Regulations

## Introduction

Export control laws are a complex set of federal regulations designed to protect United States (U.S.) national security; to prevent the proliferation of weapons of mass destruction; to further U.S. foreign policy including the support of international agreements, human rights and regional stability; and to maintain U.S. economic competitiveness. In both the defense and high-technology sectors, the U.S. Government tightly regulates the export not only of equipment and components, but also of technology. Technology includes technical data, such as blueprints and manuals, as well as design services (including the transfer of “knowledge”) and training. U.S. laws assert jurisdiction over U.S.-origin equipment and technology even after it is exported (i.e., restricting the re-export or re-transfer to third parties). These export control regulations generally require a license for export of defense items, for items that have both commercial and military applications, and for exports to sanctioned persons and destinations. In addition, the United States maintains economic embargoes against a number of countries whose governments consistently violate human rights or act in support of global terrorism. Such embargoes bar most transactions by U.S. persons with these countries.

When research or educational activities involve providing information or services to foreign nationals, it is important to know whether the goods, services, data, or technology are covered by the export control laws and regulations. Generally, export controls cover all fields of science and engineering. An export occurs when there is a transfer of items/information or the provision of specific services to a foreign national (except for green card holders). The export can occur even if the foreign national is in the U.S. (i.e., a “deemed export”). It is important not to export any information, technology or service without having determined whether an export license is required.

Three federal agencies have primary jurisdiction over the control of exports, including the Department of Commerce, the Department of State, and the Department of Treasury. The Department of State 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.

Before discussing the regulations governing export controls, it is critical to have an understanding of the definition of an “export.” In general terms, an export can be any one of the following things:

* Actual shipment of goods, technology, or information out of the boundaries of the U.S. regardless of method
* Transmission of technology, technical data, or know-how to a foreign destination, for example through verbal conversations, email, fax, internet posting or deposits in shared servers.
* Transmission of technology, technical data, or know-how to a non-U.S. person, even in the U.S. When information is transferred to a foreign person within the U.S. it is deemed to be an export to the individual’s country of origin or citizenship. Such transfers of information are known as “deemed exports” and may require export controls depending on specific circumstances.

## Export Control Laws at UNCG

Export control laws relate to many non-research activities at The University of North Carolina at Greensboro (UNCG). For example, taking a laptop with certain controlled data to a conference in certain foreign countries may require a license from the U.S. government. Shipping biological samples to a research student at a foreign university for use in their dissertation research, or shipping robots for a competition outside the U.S. may require a license.

In recognition of the role institutions of higher education play in developing cutting-edge technologies and in educating and training scholars from around the world, both the Department of State and Department of Commerce export control laws carve out special provisions whereby unrestricted research and classroom teaching activities at universities in the U.S. are excluded from the regulations. As a result, most research activities at UNCG is considered “fundamental research” as defined in the export control laws, and, as a result, will not require a license or permission from the government, and will be exempt from the laws in most cases. Nevertheless, 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.[[1]](#footnote-1) 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 UNCG 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 UNCG. 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 U.S.

The following brief descriptions of the export control laws are meant to be only an overview of the regulations as they impact activities at UNCG. The information should be used with caution, and the UNCG community is encouraged to consult with the Export Control Official (ECO) in the Office of Research & Economic Development when contemplating new export activities.

## Department of State Regulations (ITAR)

### Regulatory Authority and Scope

The Arms Export Control Act (AECA), 22 U.S.C. § 2778 grants authority to the President of the U.S. to designate and control the export and import of defense articles and services. Presidential executive order 11958 delegates this responsibility to the Secretary of State. The Department of State Directorate of Defense Trade Controls (DDTC) administers this authority through implementation of the International Traffic in Arms Regulations (ITAR), 22 C.F.R. §§ 120-130.

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

Many items designed for military use are also used for research completely unrelated to that military use. Examples include chemical agents & biological agents and their associated equipment utilized in chemistry & biochemistry research, personnel protective equipment, and night vision goggles; these are all on the US munitions list and 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 UNCG’s use of a controlled item.

### 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 U.S. or abroad, in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles. It also includes providing any foreign person any technical data as defined above.

The ITAR considers fundamental research in science and engineering at accredited institutions of higher learning in the U.S. 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 U.S. **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 U.S. where those venues are generally accessible to the public.

### The USML Categories

The USML defines twenty-one 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 <http://pmddtc.state.gov/regulations_laws/itar_official.html>.

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, Propellants, Incendiary Agents, and their Constituents

VI Vessels of War and Special Naval Equipment

VII Tanks and Military Vehicles

VIII Aircraft and Associated Equipment

IX Military Training Equipment

X Protective Personnel Equipment

XI Military Electronics

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

XIII Auxiliary Military Equipment

XIV Toxicological Agents and Equipment and Radiological Equipment

XV Spacecraft Systems and Associated Equipment

XVI Nuclear Weapons, Design and Testing Related Items

XVII Classified Articles, Technical Data and Defence Services Not Otherwise Enumerated

XVIII Directed Energy Weapons

XIX [Reserved]

XX Submersible Vessels, Oceanographic and Associated Equipment

XXI Miscellaneous Articles

### Exporting under the ITAR

An export as defined under the ITAR includes sending or taking a defense article out of the U.S., 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 U.S. 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 U.S. 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 proscribed destinations may be found at <http://www.pmddtc.state.gov/embargoed_countries/index.html>.

### 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 UNCG, the ECO will assist with the submission of commodity jurisdiction requests as well with the determination of any export licensing requirements.**

## Department of Commerce Regulations (EAR)

### Regulatory Authority and Scope

The EAR controls the export of “dual use” items, which are items that have civilian uses, but which may also have military or other strategic applications. Common, real-life examples from UNCG include information security & encryption software, certain chemicals, microorganisms, vectors, toxins, and laboratory equipment such as centrifuges. 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 which 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.

### Important EAR Definitions and Concepts

**Export** is defined in 15 C.F.R. § 732.2(b) as an actual shipment or transmission of items subject to the EAR out of the U.S. 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 U.S. or abroad.

**Deemed Export** is defined in 15 C.F.R. § 732(b)(ii). A deemed export is any release of technology or source code subject to the EAR to a foreign national, regardless of location. The release is deemed to be an export to the home country or countries of the foreign national. For the purposes of the EAR, legal U.S. permanent residents, naturalized citizens, and individuals protected under the Immigration and Naturalization Act (8 U.S.C. § 1324b(a)(3)), are not considered to be foreign nationals.

**Reexport** 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 reexport**). Reexport is defined in 15 C.F.R. § 732(b)(4).

***De Minimis* U.S. content** is the amount of U.S. content, as determined by percentage of value of the U.S. content in the end item, required to make a foreign produced item subject to the EAR. For some items, there is no *de minimis* content, meaning that any U.S. content will make the foreign-produced item controlled under the EAR. For other items the *de* minimis U.S. content 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 Information and Software** is defined in 15 C.F.R. § 734.7. Information is published when it is accessible to the interested public in any form. Publications may take the form of periodicals, books, print, electronic, public web sites, or any other media available for general distribution. General distribution may be defined as available to an interested community, such as a technical journal available to scientists in a relevant field, 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 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.*

**Fundamental Research** is basic and applied research in science and engineering, where the resulting information is ordinarily published and shared broadly within the scientific community. Such research can be distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary reasons or specific national security reasons . . . . 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. **UNCG researchers receiving proprietary information from corporate research sponsors should consult the export compliance office to ensure compliance with the EAR in the conduct of the related research.**

**Educational Information** is defined in 15 C.F.R. § 734.9. Educational Information is information released as part of a course listed in the University’s course catalog, and through instruction in the classroom or teaching laboratory. Participation in the course should be open to any qualified student enrolled at the academic institution. Educational information is not subject to the EAR, even if the faculty member is teaching the class at an institution outside the U.S.

### The Commerce Control List

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.

### 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 UNCG community are encouraged to consult with the export compliance 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.[[2]](#footnote-2) Exceptions commonly applicable to members of the UNCG community travelling abroad are BAG (Baggage), which applies to personally-owned items, household effects, vehicles, and tools of trade taken for personal use while abroad, and TMP (Temporary Imports, Exports, Reexports, and Transfers (In-Country), which applies to the temporary export of UNCG-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 U.S. within one year of export, or if not returned, documentation of disposal is required. Items exported using the TMP license exception must be kept under the effective control of the traveler while abroad. Additionally TMP is not applicable to some restricted locations, such as Cuba.**

### 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 UNCG community who need assistance with classifying items should contact the export compliance office.

### Anti-Boycott Restrictions

The anti-boycott provisions of the EAR were designed and implemented to address foreign governments’ boycott of countries friendly to the U.S. The provisions were first implemented in response to the Arab League Boycott of Israel. As of February, 2012, Arab Countries including Kuwait, Lebanon, Libya, Qatar, Saudi Arabia, Syria, the United Arab Emirates, and Yemen continue to impose boycott restrictions on Israel and companies that do business with Israel.[[3]](#footnote-3) Such companies are “blacklisted” under the boycott.

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

* Agreement to refuse or actual refusing to do business with a boycotted country or with blacklisted person
* Agreement to discriminate or actual discrimination against other persons based on race, religion, sex, national origin, or nationality (for example, agreeing to refuse to hire Israeli nationals)
* Providing information about race, religion, sex, or national origin of another person
* Furnishing information about business relationships with boycotted countries or blacklisted persons (for example, providing information about current or previous business in Israel)
* Furnishing information about membership concerning associations with charitable and fraternal organizations
* Paying or otherwise implementing letters of credit containing prohibited conditions or requirements.

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

## Department of Treasury Regulations (OFAC)

### Regulatory Authority and Scope

The Office of Foreign Asset Controls (OFAC) administers and enforces economic and trade sanctions based on U.S. foreign policy and national security interests. 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. As of 2016, OFAC sanctioned countries include the **Balkans, Belarus, Burma, Cote d’Ivoire, Cuba, the Democratic Republic of Congo, Iran, Iraq, Lebanon, the Former Liberian Regime of Charles Taylor, Libya, North Korea, Somalia, Sudan, Syria, Ukraine/Russia, Venezuela, Yemen, and Zimbabwe**. 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.

Updated regulations related to Cuban Assets Controls Regulations have been provided by the Department of Treasury as of 1-27-16: <https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cacr_20160126.pdf> Cuba is **still prohibited** under most circumstances by U.S. State Department regulations. The recent change provides an exception under the Office of Foreign Assets Control (OFAC) general license for

“***full time professionals whose travel transactions are directly related to attendance at professional meetings or conferences in Cuba organized by an international professional organization, institution, or association that regularly sponsors such meetings or conferences in other countries. The organization, institution, or association sponsoring the meeting may not be headquartered in the U.S. unless it has been specifically licensed to sponsor the meeting***.”

It is very important that you check with OFAC to ensure that your conference or business purpose qualifies under the general license and/or a specific license. In addition, it is very important to note that while you may be authorized under the general license to travel to Cuba this does not automatically allow for the import of certain types of goods and or the provision of services. **There are specific limitations on how much and on what things you can spend money on while in Cuba,** and you will want to make sure that you are staying within the proscribed spending amounts (see [State Department’s Travel Per Diem Allowances for Foreign Areas](http://www.state.gov/travel/index.htm)). Additionally, there may be specific license requirements for equipment that you might need to take (e.g., laptop computers, cell phones, flash drives, other wireless/encryption technology, and other items).

OFAC has summary information on travel restrictions to Cuba along with information on who to contact if you have questions or need additional information: <http://www.treasury.gov/resource-center/sanctions/Programs/Pages/cuba.aspx>.

**If you are considering travel to Cuba, contact the University’s Export Control office at** [**exportcontrol@uncg.edu**](mailto:exportcontrol@uncg.edu) **or (336) 256-1173 as soon as possible** to get an export control review of your plans and the types of items you would like to take so we can determine if any licenses would be required.

### OFAC Licensing for Country Based Programs

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

## Additional Considerations

### 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 five years after the completion of the activity and made available to the regulating authority upon request. Records that should be retained include all memoranda, notes, correspondence (including email), financial records, shipping documentation, as well as any other information related to the export activities. Additionally, when a license exception (EAR) or license exemption (ITAR) is used, additional records documenting the applicability of the exception/exemption may be required and in some cases there may be additional reporting requirements.

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

### 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 UNCG should immediately be reported to the ECO or to the Office of General Counsel. 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 ECO prior to engaging in the activity.

UNCG Export Control Procedures

## Commitment to Export Control Compliance

**The University of North Carolina at Greensboro must comply with all applicable U.S. government export regulations.** UNCG is committed to the preservation of academic freedom. 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 U.S. as well as to information that is already publicly available**.** However, it is important to understand how the laws apply to activities at UNCG as well as the corresponding compliance obligations, which may extend to documenting the applicable licensing exception(s). The export regulations are complex and continually changing, so it is important to consider each activity on an individual basis.

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 travelling internationally). Exports also include the release of technology to foreign nationals within the U.S., the provision of training or services involving controlled equipment to foreign nationals in the U.S. 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 fines of up to $1,000,000 per violation, incarceration for up to 20 years, and the loss of future exporting privileges.

The UNCG Office of Export Control and Conflict of Interest is responsible for helping the community understand and comply with the export control laws, and apply for an export license when necessary. Please see <https://exportcontrol.uncg.edu> for additional information including analytical tools to assist you in determining if and how the regulations apply to an activity. Questions regarding export control laws or procedures for compliance at UNCG may be addressed to the Export Control Official at [lagoble@uncg.edu](mailto:lagoble@uncg.edu) or 336-256-1173.

## Roles and Responsibilities for Export Controls at UNCG

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 UNCG.

### **Empowered Official**

The Export Control Official (ECO) is UNCG’s Empowered Official for export control matters. In this capacity, the Empowered Official has the authority to represent the university before the export control regulators in matters related to registration, licensing, commodity jurisdiction and classification requests, and voluntary or directed disclosures. While certain oversight functions may be delegated, only the Empowered Official may sign paperwork and bind the university in any proceeding before DDTC, BIS, OFAC, or any other government agency with export control responsibilities.

The Export Control Official (ECO):

1. identifies areas at UNCG 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 UNCG;
4. monitors and interprets export control legislation;
5. assists investigators, researchers and offices at UNCG when research involves export controlled equipment or information;
6. seeks advice from the Office of General Counsel in analyzing and handling export control compliance issues;
7. assists the PI in developing a technology control plan for research involving export controlled items or information to ensure compliance with export control regulations;
8. applies for export licenses, commodity jurisdiction and commodity classification requests;
9. advises and assists with record keeping for export controlled activities at UNCG;
10. maintains the export controls website.

### **Office of Sponsored Programs**

The Office of Sponsored Programs (OSP) provides assistance and expertise in export controls by working closely with the ECO in identifying export control issues and providing support for their solution. OSP has the sole authority to bind the University to research related agreements. OSP:

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

### **Research Administrators**

The school and department research administrators work closely with OSP and the PI. Together with OSP, 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 PI in identifying international components of sponsored program agreements, identifying potential export control issues in the proposed international component ;
3. communicate identified potential export control issues to the PI and the ECO;
4. communicate with the ECO and OSP about any changes in awards that necessitate a re-review of the project for export controls.

### **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 international shipping is compliant with export control laws, ensuring that payments do not go to, or contracts are not entered into, 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.

### **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 ECO in correctly classifying technology, information and equipment 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;
4. ensure that research staff and students have been trained on the technology plan and on the export control regulations should any apply.

## 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.

The Office of Sponsored Programs (OSP) performs an initial review of the request for proposal, broad agency announcement or award. A checklist is available to help identify potential export control issues (see Appendix 1). The OSP staff are trained to identify the following red flags which indicate the possible presence of export control issues:

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

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

### **Jurisdiction and Classification**

#### Technology Review

All items (hardware, software or technical data) that are exported by any means undergo an analysis by the ECO to determine which U.S. government agency has jurisdiction over the exported items. For each matter identified involving a potential export of controlled hardware/software/technology, the potential export is classified and evaluated for the applicability of any export control restrictions. The ECO will interview the researcher most knowledgeable about the technical aspects of the equipment or information under consideration for export. In addition, the items listed in the Commerce Control List and/or Munitions List, as appropriate, are reviewed. If an item is identified in one or more categories of a list, further analysis is done to determine whether the item is controlled for its intended destination, and if so, whether any License Exceptions may apply. If there is any uncertainty in this determination, outside counsel is consulted. If it is determined that a license is required, the procedures in Section XIII are followed.

#### Management of Biological Agents

The EAR Commerce Control List (CCL) and the ITAR U.S. Munitions List (USML) name many biological agents the use of which is a matter of export control management. In addition the Select Agents, approximately 40 viruses, bacteria, fungi, and toxins that are considered to potentially pose substantial harm to human health (the list is available at <http://www.cdc.gov/od/sap/docs/salist.pdf>) may also be subject to export regulations. However, certain strains of organisms and quantities are exempt from the regulations. Individuals should contact the ECO for additional information. The export of any regulated select agent requires review, and if sponsored program activity is involved, the written approval of the Vice Chancellor Research & Economic Development.

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

When export controlled equipment, data, or technology is identified for a project, the ECO will work with the PI to develop and implement a TCP to appropriately secure the equipment, data, or technology from access by unlicensed non-U.S. persons (see Appendix 2 for an example of a TCP). The TCP will include:

1. a commitment to export control compliance;
2. identification of the applicable export controls and items or technologies subject to the controls;
3. a description of the agreed upon security measures to control the item/technology including as appropriate:
   1. Laboratory compartmentalization
   2. Time blocking
   3. Marking
   4. Locked storage
   5. Electronic security
   6. Confidential communications;
4. identification and nationality of each individual who will have access to the controlled item or technology;
5. personnel screening measures for granting access to the controlled item/technology;
6. appropriate security measures for disposal of the item/technology when use is complete.

Before any individual may have access to export controlled items or technology, he or she must be informed of the conditions of the TCP and agree to comply with the security measures outlined in the TCP.

## 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 UNCG 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 UNCG. The Empowered Official is the individual at UNCG authorized to apply for licenses. In the event that a license is required, the ECO with the advice of the Office of General Counsel as required will prepare and sign the necessary documentation for preparing the license request. The ECO will be responsible for maintaining records associated with license requests.

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

## 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.

UNCG’s ECO will prepare updated training materials and will ensure that employees or students engaged in export controlled activities receive the appropriate briefing. The Export Control Office will also maintain records of training or briefings provided. Additional resources addressing special topics are available on the export control web page found at <https://exportcontrol.uncg.edu/> .

## Hiring Practices

### Hiring Foreign Nationals

At UNCG, only those full-time positions which are Exempt from the State Personnel Act (EPA) may be sponsored by UNCG for immigration benefits. EPA positions are generally instructional staff and faculty members, research staff, or senior academic and administrative officers.

EPA hiring is decentralized and managed within each department, laboratory, center, or division. Detailed hiring guidelines for both faculty positions and EPA non-faculty positions can be found online at <http://provost.uncg.edu/documents/personnel/facultysearch.pdf> and <http://web.uncg.edu/hrs/Recruitment/EPANF_Search_Committee_Resp.pdf>.

If the recommended candidate in an EPA search is not a U.S. citizen or permanent resident, the Immigration Services staff in the Office of the Provost should be consulted as soon as possible after selection to review the candidate’s current immigration documents and employment eligibility. Immigration Services will then advise and assist the recruiting unit with the procedures for hiring a foreign national employee. Immigration Services is the primary liaison to the Department of Labor and the Department of Homeland Security on immigration matters related to employment of foreign nationals in H-1B, TN, or O-1 status. This includes submitting labor-related and immigration-related documentation to the relevant government agencies either electronically or in hard copy, as required by regulation.

The Director of International Student and Scholar Services in the International Programs Center is the primary liaison when the foreign national is in J-1 (typically short-term or visiting scholars) or F-1 (student) status.

All appointment letters to non-resident aliens include a statement that the offer of an appointment to an individual who is not a U.S. citizen or permanent resident is made contingent upon receiving the appropriate immigration and work authorization documentation. The effective date of employment is consistent with the effective dates of the individual’s immigration and work authorization documents. The Office of Human Resources (HR) conducts employment eligibility verification on all new employees.

### Orientation for New Employees

Upon arriving at UNCG, foreign nationals meet with a member of the International Student and Scholar Services staff. The obligation to maintain valid immigration status and documents as a condition of employment as printed in the DS-2019 and I-20 forms are review verbally with each employee.

The International Programs Center (<http://www.uncg.edu/ipg/>) provides mandatory orientation for new international visiting scholars and students.

### Employee Transfers within UNCG

Employees may apply for other positions at UNCG in which they have an interest and for which they feel qualified. If they assume another position, the new employment is initiated by the hiring department or division. Changes in appointment/employment of foreign nationals in EPA positions must be reported to the Office of the Provost or the Office of International Programs, as appropriate. If necessary, amendments to visa documentation are sent to the appropriate government agencies, informing them of the changes.

### Employee Termination

Upon termination of employment, the employing department/division is responsible for deactivating computer and security accesses and email account, collecting UNCG keys, and forwarding the appropriate paperwork to the EPA Personnel Office. Upon termination of employment of a foreign national, the appropriate liaison withdraws or terminates labor and immigration-related documents with the relevant government agencies (Department of Labor and Department of Homeland Security). The Director of International Student and Scholar Services is notified if the employee is in J-1 status and follows regulations related to terminating the record.

### Admission Practices

Before an international student or scholar may be admitted to the United States to study, teach, or conduct research at UNCG, he/she must apply for a U.S. entry visa at a U.S. Consular post abroad. The exception to this rule is Canadian citizens, for whom the visa requirement is waived, but who must be screened by the Bureau of Customs and Border Protection before admission across the U.S. border and who must be tracked in all applicable government tracking systems. Additional information on obtaining a US Visa can be found in Appendix 3.

## Recordkeeping

UNCG’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 UNCG record retention policy, and shall be retained no less than five 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 UNCG’s five year retention period.[[4]](#footnote-4) Those records include:

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

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

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

## Monitoring and Auditing

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

## Detecting and Reporting Violations

Any individual who suspects a violation has occurred must immediately notify the university ECO. The ECO will work with the General Counsel’s Office to determine the appropriate follow-up to the notification, which may include a voluntary self-disclosure to the government. An empowered official may send an initial notification about the suspected violation to the appropriate government agency.[[6]](#footnote-6) The ECO, assisted by the General Counsel’s Office, will conduct an internal review of the suspected violation by gathering information about the circumstances, personnel, items, and communications involved. Once the review is complete, the ECO 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. which items and controlled categories were involved;
4. which dates the violations occurred on;
5. which countries were involved;
6. who was involved and their citizenships;
7. an explanation of why the alleged violation occurred;
8. any corrective actions taken; and
9. UNCG’s commitment to export controls compliance.

Once the initial notification and supplementary letter have been sent, UNCG will follow the government agency’s instructions.

# Appendix 1: Export Control Project Review Questions

For each proposal, the PI will be required to answer the following questions in our online submission system (Ramses):

|  |  |
| --- | --- |
| |  | | --- | | Export Control | |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  | | --- | | If you have specific questions about export control regulations, please visit this link <https://exportcontrol.uncg.edu/> or contact The Export Control Office at 336-256-1173. | | \* Indicates Required Fields | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | |  |  | |  | \* Does this project require the Sponsor’s prior approval of research publications or allows the Sponsor to claim resulting research information as proprietary or trade secret?  Yes     No | |  | \* Does the project sponsor prohibit access by non-U.S. Citizens to project information or the employment of non-U.S. Citizens to work on the project?  Yes     No | |  | \* Does the project require the sponsor’s approval before hiring non-U.S. Citizens to work on the project?  Yes     No | |  | \* Is any member of the research team (including students or any external contractors) a foreign national?  Yes     No | |  | |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | |  |  |  | | --- | --- | --- | | |  | | --- | | If yes, please list their name(s), (business entity & individual names), and their country(ies) of origin: | |  | | | |  | | | |  | \* Does the project require the delivery of a prototype, object, article, form of IP, or other discovery (other than technical reports)?  Yes     No | |  | \* Does the project terms state that work will be performed at a location other than at an “accredited institution of higher learning” in the U.S.?  Yes     No  (if yes, must obtain assurance that no Export Controlled information is involved.) | |  | \* Do you anticipate sending/transporting anything or receiving anything from outside of the US?  Yes     No | |  | |  |  |  |  |  | | --- | --- | --- | --- | --- | | https://uncg.myresearchonline.org/ramses/images/spacer.gif | |  |  |  | | --- | --- | --- | | |  | | --- | | If yes, please list the name(s) of the individual(s) you’re sending the item to and their country of origin, the entity(ies) that individual works for, and the name of the country(ies) you’re sending to, and provide a brief description of the item(s).  Keep in mind your proposed budget may have to include additional costs for permits, licenses, and tariffs, if applicable.  Contact the ECO asap for determination of need for export control license. | |  | | | |  | | | |  | \*Do you anticipate any travel outside the US associated with this project? | |  | Yes     No | |  | |  |  |  |  |  | | --- | --- | --- | --- | --- | | https://uncg.myresearchonline.org/ramses/images/spacer.gif | |  |  |  | | --- | --- | --- | | |  | | --- | | If yes, please list the name(s) of individuals you are meeting with, the entities they are employed by, and the country(ies) you are visiting: | |  | | | |  | | | |  | \*Will you send your research results in either paper or electronic format to a foreign country or foreign national?  Yes     No | |  | |  |  |  |  |  | | --- | --- | --- | --- | --- | | https://uncg.myresearchonline.org/ramses/images/spacer.gif | |  |  |  | | --- | --- | --- | | |  | | --- | | If yes, please list the name(s) of the country(ies): | |  | | | |  | | | |  | \*Does this proposal involve carrying out classified research, not to include work with "select agents", on campus or require a security clearance for UNCG personnel? | |  | Yes     No | |  | |  |  | | --- | --- | | https://uncg.myresearchonline.org/ramses/images/spacer.gif | If you answered yes to any of these questions, contact The Export Control Office at 336-256-1173 to determine the proper course of action and to minimize any risk from export control issues. | | | | | |

# Appendix 2: Technology Control Plan Template

**TECHNOLOGY CONTROL PLAN EXAMPLE**

**DATE:** [Fill In]

**PRINCIPAL INVESTIGATOR / PROJECT MANAGER:** [Fill In]

**TITLE OF SPONSORED PROGRAM / ACTIVITY:** [Fill In]

**RESEARCH I.D. / ACCOUNT NO. / CONTRACT NO:** [Fill In]

**SECURITY CLASSIFICATION**: [Fill In]

**PRIME SPONSOR:** [Fill In]

**GOVERNMENT AGENCY SPONSOR:** [Fill In]

**PREPARED BY:** [Fill In]

**APPROVED BY:** [Fill In]

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision Number** | **Date** | **Title or Brief Description** | **Entered By** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Introduction**

This Technology Control Plan (“TCP”) delineates and informs employees and visitors of the controls necessary to ensure that no transfer of technical information or data or defense services occur unless authorized pursuant to federal regulations.

**Purpose and Scope**

The purpose of this plan is to describe the methods to 1) identify program activities that are subject to federal regulatory requirements; 2) identify security responsibilities and requirements of project personnel; 2) establish methods for the identification and handling of controlled unclassified information (“CUI”); 3) allowable and unallowable access to the program, data and equipment, monitoring and control protocols, physical and electronic measures for access, use, storage, transfer and destruction.

This TCP delineates and informs UNCG representatives and visitors of the controls necessary to ensure that no transfer of classified defense information or controlled unclassified information (defined as technical information or data or a defense service as defined in ITAR paragraphs 120.9 & 120.10) occurs unless authorized by the U.S. State Department, Directorate of Defense Trade Controls (DDTC).

The TCP provides guidance on the control of access to classified and unclassified export controlled information by foreign persons employed by, and long-term foreign national visitors assigned to, a cleared U.S. contractor facility pursuant to the (including the Arms Export Control Act (“AECA”), as amended, an enumerated in the International Traffic Arms Regulations (“ITAR”) 22 CFR Parts 123 – 130, and the Export Administration Act (“EAA”) of 1979 enumerated in the Export Administration Regulations (“EAR”) 15 CFR Parts 730 through 774, and the Atomic Energy Act of 1954 (“AEA”) (Public Law 83-703), and both the Nuclear Regulatory Commission (“NRC”) 10 CFR Part 110 and the Department of Energy Regulations, 10 CFR Part 810 (“DEAR”) and the National Industrial Security Program Operating Manual (“NISPOM”).

A TCP is a roadmap of how UNCG will control restricted technology to ensure compliance with the ITAR, EAR, AEA, NRC, DEAR and NISPOM.

**Instructions**

All employees and other personnel, prior to receiving, accessing, handling, analyzing, or generating export controlled defense articles or restricted data must execute a standard document acknowledging their understanding of the controlled nature of the defense articles, technical data, or software (received or generated) and the required safeguards with which they must comply in their acceptance of such articles, technical data or software. When accepting such articles, you become personally liable (civil and criminal) for preventing improper disclosure even if in the academic setting. This requirement is applicable to the provisioning, procurement, acceptance or loan of USML defense articles that enter onto Campus for use in research or academics that are in the care, custody, access or use of UNCG employees and students.

**Allowing a foreign person to access defense articles, software or technical data, or providing instruction regarding any defense article may require a federal license before the “export” occurs. Failure to obtain a license before export may be illegal and could subject both the university and violator of crimes and penalties up to and including imprisonment.**

**Definitions:**

The following definitions clarify the terminology used throughout this TCP.

**Authorized Foreign National:** A Non-US Person who is authorized to receive access to Export Controlled items or information pursuant to an issued and current license or agreement (TAA, MLA), license exemption (ITAR) or license exception (EAR).

**Deemed Export:** In addition to actual shipment of Export Controlled items or information out of the country, export regulations also control the transfer, release or disclosure to foreign persons in the United States of technical data about Export Controlled items or information. “Deemed export” regulations provide that a transfer in the United States of source code or “technology” (EAR) or “technical data” (ITAR) to a Foreign Person is “deemed” to be an export to the home country of the Foreign Person.

**Defense Article:** Any item or technical data identified on the U.S. Munitions List or specifically designated by the Department of State as a Defense Article based on a determination that it (i) provides the equivalent performance capabilities of an item on the U.S. Munitions List; or (ii) provides a critical military or intelligence advantage such that it warrants control under the ITAR. Defense Articles include technical data recorded or stored in any physical form, or models, mockups or other items that reveal technical data directly relating to items on the United States Munitions List. It does not include basic marketing information on function or purpose, or general system descriptions.

**Defense Service:** Furnishing technical data or assistance (including training) to foreign persons (i.e., foreign nationals), 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; or, military training of foreign units and forces.

**Export:** Any of the following activities with respect to items, technology, or software subject to either the EAR or ITAR: (1) physical shipment outside the United States; (2) electronic or digital transmission outside the United States; (3) release or disclosure, including verbal disclosures or visual inspections, to any foreign national, whether in the United States or abroad (see definition of Deemed Export above); or (4) provision of Defense Services, as defined in the ITAR.

**Export Controlled:** Items, technology, or software found in either the Commerce Control List (CCL) of the EAR, or the Munitions list of the ITAR. Under the ITAR, provision of a Defense Service related to a Defense Article is also an Export Controlled activity.

**Export Administration Regulations (“EAR”):** Regulations are issued by the United States Department of Commerce, Bureau of Industry and Security (BIS) under laws relating to the control of certain exports, re-exports, and activities of the “dual use” items found on the Commerce Control List (CCL).

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

**Fundamental Research:** Basic or applied research in science and/or engineering at an accredited institution of higher learning in the United States where the resulting information is ordinarily published and shared broadly in the scientific community. Fundamental Research is distinguished from research which results in information that is restricted for proprietary reasons or pursuant to specific U.S. Government access and dissemination controls. University research will not be deemed to qualify as Fundamental Research if: (1) the University or researcher accepts any restrictions on the publication of the information resulting from the research, other than limited prepublication reviews by research sponsors to prevent the inadvertent release of proprietary information provided to the researcher by the sponsor or to ensure that publication will not compromise patent rights of the sponsor; or (2) the research is federally funded and specific access and dissemination controls regarding the resulting information have been accepted by University or the researcher.

**Media:** For purposes of this TCP, the term “Media” is defined to include both tangible media, such as paper, computer discs, and CDs, as well as electronic data, regardless of location and or storage methodology.

**Release:** Technology or software is “released” for export through: (i) visual inspection by foreign nationals of U.S.-origin equipment and facilities; (ii) Oral exchanges of information in the U.S. or abroad (iii) The application to situations abroad of personal knowledge or technical experience acquired in the U.S.

**Technical Assistance:** Instruction, skills training, working knowledge, consulting services and other similar forms.

**Technical Data:**  Information which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of Defense Articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation. Technical data includes classified information relating to defense articles and defense services, and some software may be considered technical data. This definition does not include educational materials and also does not include basic marketing information on function or purpose or general system descriptions of defense articles.

**Technology or source code:** Release of specific information (or source) code necessary to develop, produce, or "use" a product on the Commerce Control List without an export license or other government approval. "Use" is defined as "Operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing."

**U.S. Person:** A natural person who is (1) a U.S. citizen; (2) a lawful permanent resident of the United States (i.e., a “Greed Card” holder), as defined by 8 U.S.C. § 1101(a)(20); or (3) a protected individual (i.e., a legal asylee, a refugee, or other protected individual under the Immigration and Naturalization Act), as defined by 8 U.S.C. § 1324b(a)(3). It also means any corporation, business association, partnership, society, trust, or any other entity, organization or group that is incorporated to do business in the United States. It also includes any governmental (federal, state or local) entity. It does not include any Foreign Person as defined above.

**Penalties**

This TCP is designed to ensure compliance with U.S. export control laws and regulations. Individuals violating federal law and applicable regulations governing the conduct of restricted activities and exports are subject to civil and criminal penalties that include fines, jail terms, suspension, denial of export or research privileges and debarment from government contracting. In addition, such a violation of UNCG policy could result in discipline up to and including termination of employment. Criminal fines may range up to $1,000,000.00 per violation and up to imprisonment for 10 years.

**UNCG Statement of Commitment**

The University of North Carolina at Greensboro is committed to compliance with federal export control laws, regulations, and sanctions. The Export Control Official in the Office of Research & Economic Development (ORED) is the designated authority charged with compliance oversight of U.S. export control requirements for sponsored program and other activities at UNCG and has final authority on such matters. Individuals acting on behalf of the university are responsible for the proper handling, transfer, access, storage, control and dissemination of export controlled hardware, software, information, technology, and technical data to destinations and persons outside of the U.S., as well as in some cases, to foreign nationals at the university engaged in instruction, conducting research, or providing service activities.”

It is policy for UNCG and all members of the university community to fully comply with U.S. export control laws while ensuring that, to the extent possible, university instruction and research is conducted openly and without restriction on participation or publication. UNCG is committed to educating its employees, professors, students, researchers or other collaborators on U.S. export control laws and regulations and their particular application within a university research setting. As part of the University’s ongoing commitment to export control compliance and education, the University has established a website at: <https://exportcontrol.uncg.edu/> that contains university export control policies, forms, training modules and reference materials.

**ROLES AND RESPONSIBILITIES**

UNCG as well as its researchers and staff are responsible for complying with export control regulations, as follows:

**Export Control Official:**

The Export Control Official will be in charge of administering the TCP.

In regards to this TCP, the Export Control Official is responsible for:

1. Training UNCG Personnel regarding the requirements of the export control regulations and this TCP;
2. Coordinating and monitoring the implementation of this TCP;
3. Maintaining a list of UNCG personnel who are authorized to participate in projects subject to this TCP;
4. Serving as the focal point for questions/issues;
5. Maintaining copies of all records provided to the Export Control Official by PI’s related to TCP’s for at least three (3) years after project period of performance end date; and
6. Reporting violations.

**Principal Investigator**

The Principal Investigator has primary responsibility for ensuring research is conducted in a manner that complies with all applicable laws, rules and regulations, including this TCP.

The Principal Investigator is responsible for:

1. Notifying the export control official when an Award involves receiving and/or generating Export Controlled items or information;
2. Completing Project Specific TCP Information. (Attachment A);
3. Ensuring all UNCG Personnel working on a TCP-controlled award:
   1. Are informed the award is subject to this TCP
   2. Complete export control and TCP awareness training.
   3. Sign Attachments “A” and “B”.
4. Maintaining all records related to TCP’s applicable to their research for at least three (3) years after project period of performance end date and providing a copy of such records to the TCP Project Coordinator; and
5. Reporting violations of the TCP to the export control official.

**Research Personnel**

Research Personnel are responsible for:

1. Adhering to the requirements of any TCP applicable to their work;
2. Completing ICT’s TCP awareness training;
3. Signing Attachment “A” and/or Attachment “B” and complying with its requirements; and
4. Reporting violations of the TCP to the Principal Investigator.

**CONTROL REQUIREMENTS**

**Physical Security**

The following physical security measures shall be implemented on the project listed in Attachment “A”:

* 1. Foreign nationals will not be provided access to Export Controlled items or information unless they meet the definition of Authorized Foreign National, as described elsewhere in this Technology Control Plan.
  2. Export Controlled items or information must be stored either in a room permitting limited and controlled access, or in a locked desk/cabinet/file. Export Controlled items or information may not be left unattended when not under proper storage conditions.
  3. Export Controlled items, if they are hardware assemblies or their equivalent, also must be protected with seals to easily identify any evidence of physical tampering.
  4. Access to any ITAR-restricted hardware, including access via non-ITAR restricted software, must be limited to U.S. Persons and any other authorized personnel.
  5. Export Controlled items or information should also be clearly marked as export controlled.
  6. Physical access to hardware (such as servers) hosting Export Controlled information must be limited to those individuals who are authorized to receive such data under the applicable export control regulations and have completed TCP Awareness Training.
  7. Physical access for server operations, maintenance and repair will be restricted to those individuals who have completed TCP Awareness Training, are authorized to receive all technical data stored on the server, and whose job responsibilities reasonably require such access.

**Electronic/Information Security**

**E-mail:**

The body of an email may not contain Export Controlled information. All email attachments containing Export Controlled information must be encrypted. Passwords may only be exchanged in person or via a live telephone conversation. No voice mail or email messages are allowed which provide the password.

In addition, if an email has an attachment which contains Export Controlled information, the body of the e-mail must prominently include one of the following messages, as appropriate (consult Export Control Official for guidance):

Use and Disclosure of Data:

This email contains attached file(s), the content of which is subject to U.S. Government Export Restrictions under the International Traffic in Arms Regulations, 22 C.F.R. Parts 120–130 (the “ITAR”). Unless licensed or otherwise authorized by the U.S. Government, disclosure is limited to U.S. Citizens and U.S. Permanent Residents.

or

Use and Disclosure of Data:

This email contains attached file(s), the content of which is subject to U.S. Government Export Restrictions under the Export Administration Regulations, 15 C.F.R. Parts 730-774 (the “EAR”). This information may not be exported or otherwise released except as authorized under the EAR.

Prior to sending any such email, the sender is required to verify that the recipient is properly authorized under applicable export control regulations to receive the attached file(s).

**Server Access:**

Electronic access to server directories and or files will be limited by the use of passwords (file system permission). Passwords will be provided only to those individuals who have completed TCP Awareness Training, and are authorized to receive Export Controlled data on the server within the relevant password protected directories.

For each award/project, the Principal Investigator will specify any password protected directory(s) and will set up group access permissions. The Principal Investigator must have completed TCP Awareness Training prior to establishing and or modifying directories and/or server group membership. Requests for group access must be in writing, and the Principal Investigator is responsible for verifying that all individuals who will receive access have completed TCP Awareness Training.

**Conversation Security:** UNCG personnel who are working on a project subject to this TCP must ensure that conversations related to the project are only attended by other UNCG personnel authorized to work on the project.

**Publications/graduate theses:** PI’s and graduate students must ensure that no Export Controlled items or information are included in a thesis or other publication. The PI also must ensure that all UNCG personnel on a project adhere to sponsor review requirements associated with projects subject to this plan. While it is the university’s intent to protect unfettered rights to publication, this may not be possible on projects subject to this TCP. Graduate student involvement on such projects will be evaluated on a case-by-case basis to ensure that all degree objectives and sponsor restrictions can be achieved prior to commencing work on the project.

**Marking of Export Controlled items or information:**

**Restrictive Legends**

UNCG personnel shall endeavor to have all third parties disclosing Export Controlled items or information and Media to UNCG mark such items or information as controlled under the ITAR or the EAR, as appropriate. It is the duty of each person handling such items or information to ensure restrictive legends are placed on the outside of or first page of all items or information. In addition, the specific location containing the Export Controlled items or information, such as the page, shall be marked as well. If the Export Controlled item or information is copied, pasted or otherwise incorporated in another document, the marking requirements apply to the new document as well.

**Department of Commerce (EAR)**

*Title page legend-*

Use and Disclosure of Data:

This document contains data that is subject to U.S. Government Export Restrictions under the Export Administration Regulations, 15 C.F.R. Parts 730 -774 (the “EAR”). This information may not be exported or otherwise released except as authorized under the EAR.

*Page legend-*

Use or disclosure of data contained on this sheet is subject to the restriction on the Title page of this document.

**Department of State (ITAR)**

*Title page legend-*

Use and Disclosure of Data:

This document contains data that is subject to U.S. Government Export Restrictions under the International Traffic in Arms Regulations, 22 C.F.R. Parts 120 –130 (the “ITAR”). Unless licensed or otherwise authorized by the U.S. Government, disclosure is limited to U.S. Citizens and Permanent Residents.

*Page legend-*

Use or disclosure of data contained on this sheet is subject to the restriction on the Title page of this document.

**Screening:** UNCG employees will be screened against the U.S. Government’s restricted parties lists, including the Treasury Department’s List of Specially Designated Nationals and Blocked Persons, the Commerce Department’s Denied Person’s List, Entity List and Unverified List, and the State Department’s Debarred Parties List.

**Training/Awareness Program**

All individuals need to complete Technology Control Plan awareness training prior to receiving, handling or generating Export Controlled items or information. The training will address the following issues:

* The scope and restrictions of the EAR and the ITAR;
* The applicability of the export control regulations and this TCP to activities of UNCG Personnel;
* Penalties for violations of the EAR, the ITAR and this TCP; and
* Proper procedures for reporting export compliance issues.

Upon completion of the TCP awareness Training, UNCG Personnel must sign and date a certification (Attachment “B”) stating that they have been informed of and clearly understand their responsibilities regarding compliance with the EAR, the ITAR and this TCP. After signing the certification, the individual will be added to the Export Control Official’s list of authorized users.

A list of all individuals with access to Export Controlled items or information and/or facilities will be maintained by the Export Control Official. The Export Control Official will be responsible for keeping the list current. The Export Control Official will keep copies of all training acknowledgements (Attachment “A”) for three (3) years after project close out. The Export Control Official will also keep copies of briefing acknowledgements (Attachment “B”) with respect to all current UNCG Personnel who have signed one, and for three years after the UNCG Personnel’s employment or affiliation with UNCG has ended.

**End of Project Security Measures**

**UNCG generated Export Controlled items or information:**

Tangible items will be disposed of or appropriately secured at the end of the project. Electronic files will be purged from the hosting device or appropriately secured using standard file management tools. Please contact the Export Control Official to coordinate disposal.

**Third Party generated Export Controlled items or information:**

All Export Controlled items or information will be returned to the disclosing party, or parties, at the close of the contract under which such information or items were received, or to the parties that transmitted such information. If any party that has transmitted Export Controlled items or information refuses to accept them, then such items and/or information will be destroyed consistent with the provisions of this TCP.

**Physical Security Protocols**

| **Technology Control Requirement** | **Controls Addressed** | **Complete/**  **Monitored**  **(Date)** | **Describe how the control is met and any compensating control if control is not implemented as stated.** |
| --- | --- | --- | --- |
| Doors to individual offices and research facilities may not be propped or left open. Signs should be posted at the entrance to research facilities during times that ITAR-controlled items and information are visible on the desk or workspace, e.g. **“Restricted Access Area: Unauthorized Persons Not Permitted.”** |  |  |  |
| A time schedule should be posted noting the times when the area is subject to Restricted Access and who are the primary personnel for hosting foreign person escorts. |  |  |  |
| Doors should be locked and a clean desk policy in effect whenever these rooms or facilities are left unattended and ITAR-controlled items and information are visible on the desk or workspace. |  |  |  |
| ITAR-controlled equipment (if any) shall be labeled as such by suitable means and shielded from unauthorized visual access at all times. Foreign persons will not be allowed entry to offices or research facilities when ITAR controlled items are visible and/or in use, unless prior licensing approval has been obtained or an ITAR exemption is applicable. |  |  |  |
| Hard copies of ITAR-controlled information should be stored in a secure location (locked drawer or cabinet) when not in use. Only authorized individuals are to be permitted access. |  |  |  |
| Research deliverables containing ITAR-controlled technical data should be marked **“ITAR-controlled – do not distribute to non-U.S. Persons”** |  |  |  |
| Any ITAR-controlled technical data that is printed will be done on a printer located in one of the research areas identified in this section. Printed information will be retrieved immediately and shall be marked **“ITAR Controlled: Do Not Distribute to Foreign Persons”** |  |  |  |

**Researcher Responsibilities**

| **Technology Control Requirement** | **Controls Addressed** | **Complete/**  **Monitored**  **(Date)** | **Describe how the control is met and any compensating control if control is not implemented as stated.** |
| --- | --- | --- | --- |
| Personnel will not post any information regarding the specific work of the project or any technical data generated from the project on internet web sites, social media venues, or any other Information Technology systems not located inside the work center. |  |  |  |
| Excerpts of research team resumes, biographies, or similar professional documents of personal accomplishment pertaining to this project will not reveal any technical data related to the project. For certain programs, sponsor for review & approval of content may be required prior to release for public viewing. |  |  |  |
| Displays of information containing Cl will be positioned so that it is not viewable from outside the work center. This includes sight lines that are visible at a distance where binoculars or similar devices could make the information viewable. |  |  |  |
| Windows, doors, or other sightlines into work areas where Cl is present will be blocked or covered. Sightlines do not have to be blocked if CI is positioned in way that precludes its observation. |  |  |  |
| Personnel will not discuss CI on a cell phone or in a room where a cell phone or similar PDA is present. Personnel should not discuss the project's Cl outside the work center anywhere that they may be overheard. |  |  |  |
| Research materials that contain CI will not be taken outside of the access controlled work area except for when it is necessary to conduct approved project work in other official work locations (i.e. transit to an external location for testing, etc.). When taken outside the work center for official purposes Courier protocols need to be followed. |  |  |  |
| CI will be stored in a locked container (file box, briefcase, etc.) until it can be stored in a controlled access location. |  |  |  |
| Personnel will not respond to any information requests from other than the sponsor regarding the CI for this project. Report suspicious activities and all requests for information to the  ECO. |  |  |  |
| Visitors to the work area will be escorted by a member of the research team who is on the PI's authorized entry list. The team will maintain a visitor log to record the names, dates, times, and nationality of visitors into the area. Log entries must be maintained for 180 days. |  |  |  |
| All researchers shall read this TCP and sign the Non-Disclosure Statement that acknowledges that classified and controlled unclassified information will not be further disclosed, exported or transmitted by the individual to any foreign national or foreign country unless the U.S. Government authorizes such a disclosure and the receiving party is appropriately cleared in accordance with its government's personnel security system. |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Lab Instrument & Equipment Requirements**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Escort & Site Visit Controls**

|  |  |  |  |
| --- | --- | --- | --- |
| Foreign person(s) in areas with export controlled or proprietary technical data require an escort at all times. |  |  |  |
| The work area will be secured in a method that allows the PI to control who has access into the work area. The means of securing the work area must also provide for evidence of forced entry. |  |  |  |
| Brief all team members on threats surrounding visitor(s). |  |  |  |
| Inform researcher(s) of when visitor(s) will be in their space and shield restricted and proprietary info. |  |  |  |
| Do NOT conduct restricted research with foreign person(s) present. |  |  |  |
| Do not allow wandering, pictures, embarrassing incidents, unannounced changes, unannounced visitors, video crews, misinterpretations, multiple requests, etc. |  |  |  |
| Designated “safe harbor” areas |  |  |  |
| Lock-up restricted information / articles |  |  |  |
| Challenge any person in the restricted area who is not a part of the approved project team. |  |  |  |
|  |  |  |  |

**IT Security Protocols (252.204-7012 Compliant)**

It is the responsibility of the Principal Investigator to work with the Export Control Official and/or representatives from the UNCG ITS Department to ensure that the systems involved in this project meet the stated controls and that those controls remain in effect for the duration of the project unless this form has been updated and approved.

Please describe the system inventory for this project. Include all machine names and IP address for those with a fixed address and any non-University IT assets that will be used in this project, including mobile devices, laptop or desktop computers, tablet devices, removable drives and memory cards or memory sticks.

|  |
| --- |
|  |

Does information in this system need to be backed up? If so, on what frequency? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

| **Control Statement** | **Controls Addressed** | **Complete**  **(Date)** | **Describe how the control is met and any compensating control if control is not implemented as stated.** |
| --- | --- | --- | --- |
| Desktop/Laptop computers (along with flash drives and back-up hard drives) will have encrypted folders, encrypted files, or encrypted hard drives for working with and storing export controlled technical data. |  |  |  |
| Export-controlled files will be password protected and encrypted unless the ITAR files are stored on a verified secure server. |  |  |  |
| All computers that contain export-controlled technical data will be locked and password protected when unattended. |  |  |  |
| All devices that contain export-controlled data/information will be clearly labeled as containing ITAR-controlled data/information (e.g., flash drives, laptops, computers, back-up hard drives). |  |  |  |
| If removable storage devices are used for ITAR data back-up, those devices will be encrypted.   * Encryption Wizard (EW) is a simple, strong, Java file and folder encryptor for protection of sensitive information (FOUO, Privacy Act, CUI, etc.). EW encrypts all file types for data-in-transit protection and supplements data-at-rest protection. <http://www.spi.dod.mil/index.htm> * When not in use, back-up hard drives and flash drives that contain ITAR-controlled data or information will be stored in a secure location (secured drawer or cabinet) to prevent unauthorized access. * Only the individuals authorized by this TCP will have access to back-up hard drives and flash drives that contain project ITAR-controlled data and information, and specifically the individual who is the owner of the hard-drive/flash drive will have access to the key/lock of its secured location |  |  |  |
| ITAR-controlled technical data will not be distributed or received via email without encryption under any circumstances (e.g., to/from sponsor, between project personnel). |  |  |  |
| If it is necessary to transport electronic export controlled data or documents, the electronic data or documents will at all times be in the possession of the individual(s) listed in this TCP and   * be stored as encrypted files or in encrypted folders on devices such as a laptop or flash drive using <http://www.spi.dod.mil/index.htm>; * be secured in the individual’s briefcase (or other secure storage device), locked in a car and/or a hotel safe; or   be kept in a secure location in the individual’s residence to prevent access by unauthorized foreign persons. |  |  |  |
| Travel outside the U.S. with ITAR controlled documents, equipment, or data will not occur without authorization (license) from Department of State. |  |  |  |
| ITAR data will not be disclosed to or discussed with any persons other than authorized project personnel and should be distributed via secure means. |  |  |  |
| Disposal of computer floppy drives, compact discs, jump drives, and portable digital media devices that contain ITAR-controlled technical materials will be coordinated with the ECO. |  |  |  |
| No employee or other person acting on behalf of UNCG will, without prior approval, release, ship, mail, hand carry or transmit technical data arising from this research effort out of the U.S. or within the U.S. with the knowledge or intent that the data will be released, shipped, or transmitted from the U.S. to a foreign person. **Accessing, processing and storing controlled data on personally-owned equipment, at off-site locations (e.g. employees home, or “Approved Project Personnel’s home”), on “Cloud” computing or storage locations (e.g. Amazon EC2, Dropbox, OneDrive, iCloud, etc.), and/or non-UNCG managed IT services (e.g. Yahoo!, Gmail, etc.), is strictly prohibited.** |  |  |  |
| No personal electronic devices, including but not limited to smartphones, laptops, MP3s, PDAs or tablets are permitted to be used for the collection, storage, transmission or copying of export controlled project information. The use of “Cloud” computing or storage locations is also prohibited. Should an employee or student depart while the project is ongoing, scans and audits may be run on computers and data collection and storage devices to check for unauthorized downloads or uploads of controlled technical data from this project to unauthorized devices or persons. |  |  |  |
| Access to the system must be based on an authorized need to know and authorized in writing. All accounts must be maintained in a log, preferably the TCP, and be reviewed by the PI on at least a quarterly basis. Unnecessary accounts are to be removed or deactivated as soon as possible to reduce the potential for unauthorized access. | AC-2, IA-2, IA-4, IA-5 |  |  |
| The system must be configured to limit the flow of information out of the system to only known locations. If Internet access is necessary for information flow, transmission must be over encrypted channels. The use of firewalls configured to limit extraneous ports and protocols will aid in implementing this control. | AC-4 |  |  |
| The system enforces account lockout after 5 failed login attempts. This can be implemented in a delay fashion where the account is locked for a specified time or through hard lockout where an administrator must authenticate the user prior to access being granted. | AC-7 |  |  |
| The system enforces a session lock displaying a lock screen after 15 minutes of inactivity until a user authenticates to the system with a valid credential. | AC-11 |  |  |
| Remote access to the system must be authorized by the PI and granted using only approved methods as documented by the PI. | AC-17 |  |  |
| Wireless access to systems containing controlled technical information must only be permitted utilizing a VPN connection to the UNCG network. | AC-18 |  |  |
| Removable media must only be used when approved by the PI and data must be encrypted on such media to protect it in the event of loss. All auto-run functionality must be disabled on all systems containing controlled technical information. | AC-19 |  |  |
| The use of any external systems to process, store or transmit controlled technical information must be approved in writing by the PI and only when they have been validated to meet the same or similar controls listed in this plan. This includes any personally owned devices including laptops, desktops, tablet devices or cellular devices. | AC-20 |  |  |
| All system users will participate in security awareness training at least annually. | AT-2 |  |  |
| Systems must be configured to monitor system events and record those events in sufficient detail to determine what event occurred, when it occurred and who performed the action. Time events must be recorded in UTC format. | AU-2, AU-3 |  |  |
| Audits records must be sent to a central log server either within the local IT group or coordinated with the ECO and ITS. Audit records must be monitored via SIEM technology with alerts configured to indicate unauthorized or suspicious activity. Exception reports must be evaluated consistent with the University incident response procedures. | AU-6, AU-7, AU-9, SI-4 |  |  |
| Systems recording audit events must have their internal clocks synchronized with a recognized timeserver. | AU-8 |  |  |
| Departmental IT groups must develop and maintain a baseline configuration for systems to be used in the project. All systems must be configured with the least functionality necessary to accomplish the work for the project. The ISO security benchmarks should be used as a basis for configuration if the department does not have a baseline in place.  <http://benchmarks.cisecurity.org/downloads/> | CM-2, CM-6, CM-7 |  |  |
| All systems must be configured to uniquely identify individual users and uniquely identify the system as well. System identification must be managed by the Departmental IT or ITS. All user identification can be managed by the PI but must be documented and stored with this security plan. | IA-2, IA-4, IA-5 |  |  |
| Systems being used to process, transmit or store unclassified controlled technical information must have a vulnerability scan performed on at least a monthly basis and flaws remediated within guidelines established by the ECO. | RA-2, SI-2 |  |  |
| All users will follow the incident reporting protocols as established by the ECO, which is to report all known or suspected security incidents to the ECO. Incident handling and monitoring will be a coordinated responsibility between the departmental IT unit and the ECO. | IR-2, IR-4, IR-5, IR-6 |  |  |
| The PI will be responsible for establishing a process for storing all removable media and printed media in a secure location when not in use. | MP-4 |  |  |
| All media that is no longer needed for the project will be disposed of in a secure manner. Paper documents can be shredded. Electronic media must be wiped using secure methods unless data is encrypted using AES-256 bit encryption or comparable. | MP-6 |  |  |
| All systems processing, storing or transmitting unclassified controlled technical information must employ encryption to protect the data at rest and in transmission. | SC-8, SC-13, SC-28 |  |  |
| All systems processing, storing or transmitting unclassified controlled technical information must be running anti-virus/anti-malware software and be kept up to date with the latest signature files. | SI-3 |  |  |
| All system users are expected to attend security awareness training on at least an annual basis, while working on this project. | AT-2 |  |  |
| The PI will be responsible for maintaining a log of all individuals with physical access to the systems in use for this project. These access lists must be reviewed at least monthly to ensure those who no longer need access are removed. | PE-2, PE-3, PE-5 |  |  |
| Appropriate boundaries will be established for all systems processing, storing or transmitting unclassified controlled technical information to prevent external access or unintended transfer of information beyond the system boundaries. | SC-4, SC-7 |  |  |
| User functionality and system level functionality shall require different authentication. | SC-2 |  |  |
| All system maintenance must be performed via either departmental IT or ITS personnel as authorized by the University. Any remote maintenance or diagnostics must be specifically authorized in writing and controlled via the use of strong authentication. | MA-4, MA-5, MA-6 |  |  |

**Shipping / Transporting / Courier Controls**

|  |  |  |  |
| --- | --- | --- | --- |
| International shipping is unallowable and unauthorized for any item, material or data related to this program. |  |  |  |
| ITAR items will require a license from Department of State and cannot be shipped until the license is received. |  |  |  |
| **The ECO will apply for all export licenses**. Copies of the license will be retained by the ECO and a copy will be sent to the PI/Project Director. A copy of all shipping paperwork will be sent to the ECO. |  |  |  |
| If ITAR-controlled, only the inner packaging of the box or container will be marked **“ITAR-CONTROLLED - NO FOREIGN PERSON ACCESS” WARNING - This package contains defense articles and technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979 (Title 50, U.S.C., App. 2401 et seq.), as amended. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25** and will be placed inside of an unmarked box, crate or container for shipping or transporting. |  |  |  |
| Trucking Companies used to transport ITAR goods within the U.S. must be informed in writing that the cargo is ITAR-controlled, and the company must certify in writing that no foreign persons will have access to the ITAR goods. NOTE: This is not applicable for large transportation companies such as FedEx or UPS.  The signed letters will be kept by the PI/Project Director and/or the appropriate Export Control Liaison and be available for review by the ECO. |  |  |  |
| Couriers transporting export controlled data, documents or equipment across or off university premises should be adequately trained:   * All export controlled items, documents or equipment must be in the possession of the courier at all times * be secured in the individual’s briefcase (or other secure storage device), locked in a car and/or a hotel safe; or   be kept in a secure location in the individual’s residence to prevent access by unauthorized foreign persons |  |  |  |

**Project Completion & Disposal**

|  |  |  |  |
| --- | --- | --- | --- |
| Upon departure from the program, employees will be required to execute a statement regarding equipment and written matter (at the discretion of). This statement will certify that foreign persons have not given or disclosed to any unauthorized person documents, reports, or other data which is considered company proprietary. Foreign visitors will also return to the EIA the photo ID badges that were issued to them. |  |  |  |
| Printed matter containing ITAR-controlled data will be disposed of by crosscut shredding prior to disposal or recycling. |  |  |  |
| IT System sanitization |  |  |  |

**REPORTING VIOLATIONS**

All instances of non-compliance with the requirements of this TCP must be reported immediately to the Export Control Official. The incident report should identify all relevant information, including but not limited to the date and nature of any disclosure or export; the name(s) of the person(s) involved; and a description of the disclosed or exported items or information.

1. Penalties

U.S. export control laws authorize the imposition of both civil and criminal penalties for violations, including significant fines, the potential loss of export privileges, and in certain instances criminal penalties, including severe fines and prison time.

1. Questions and Related Information

Questions related to the implementation of this TCP with respect to a specific project should first be directed to the Principal Investigator and/or the Export Control Official. General questions relating to the TCP should be directed to the university ECO.

# Appendix 3: Information for US Visa applications

### U.S. Consulate Application Review and Applicant Interview

Visa Application Forms: All foreign national applicants must complete visa application forms. These forms ask specific questions. The answers to these questions will reveal issues that might make certain people ineligible for U.S. entry visas (as defined in the Immigration and Nationality Act, Title II: Chapter 2, Section 212 General Classes of Aliens Ineligible to Received Visas and Ineligible for Admission, found at <http://www.fourmilab.ch/uscode/8usc/www/t8-12-II-II-1182.html>).

Consular Lookout System: Once the visa application is submitted, consular officials make an electronic inquiry to CLASS (Consular Lookout system). If there is a “hit” or match with a visa applicant’s name, date of birth, or other identifiers, further investigation is done to determine visa eligibility. Information about CLASS is found at <https://foia.state.gov/_docs/PIA/ConsularLookoutSupSystem_CLASS.pdf>

Numerous government agencies serve as sources of information for the CLASS database, including the following: Department of State, National Crime Information Center, Drug Enforcement Agency, Federal Bureau of Investigations, Interpol, Central Intelligence Agency, National Security Agency, Office of Foreign Asset Control, Bureau of Non-Proliferation, Department of Commerce, and others. If any of these agencies believe the individual is a risk, a CLASS “hit” will appear at the time of consular inquiry.

Other databases: Consulates also have the ability to check criminal history in local and national databases in the home country where the alien is applying for the visa.

INA 212(a) Technology Alert List: If any foreign national’s field of study or research is deemed to be in a sensitive technology, or if the individual is from a country which the Department of State deems a risk (for espionage, export risk, etc.), the Consulate may ask for a Security Advisory Opinion (SAO) from the Department of State in Washington, DC. More information on Security Advisory Opinions can be found at <http://travel.state.gov/content/visas/en/general/advisory-opinions.html>

Student and Exchange Visitor Information System: The Department of Homeland Security’s tracking system is called the Student and Exchange Visitor Information System (SEVIS). This system specifically tracks students and scholars in F, J and M status. Consular officials can see data in their own systems which have been forwarded from SEVIS. When a student or scholar appears at the consulate for a visa interview, consular officials can match the documents presented with the information in the computer database. Information is available on the Immigration and Customs Enforcement web site at <https://www.ice.gov/sevis>.

U.S. Visitor and Immigrant Status Indicator Technology (US VISIT): Ultimately, if the decision is made to grant an applicant a visa, the U.S. Consulate scans the index fingerprints of the applicant and takes a digital photograph. This information is fed into the US-VISIT system, a congressionally-mandated entry and exit tracking system. US-VISIT is designed to track the arrivals and departures of *all* non-immigrants, regardless of visa type. For more information, consult the Federal Register, Vol. 69, No. 2, January 4, 2004, Rules and Regulations, located at <http://grants.nih.gov/grants/policy/fed_reg_peer_rev_20040115.pdf>. See also <http://www.dhs.gov/us-visit>

### Inspection by Bureau of Customs and Border Protection

Border Inspection: When the student or scholar arrives at the port of entry to the U.S., he/she is interviewed/inspected by immigration and customs officials. The Bureau of Customs and Border Protection enters the arrival information into the SEVIS system.

US-VISIT Biometrics: In addition to being questioned by an official and having his/her documents and baggage inspected, the individual is required to insert index fingers into the US-VISIT machine to verify that the person entering the US is the person who originally applied for the visa.

US-VISIT technology is being rolled out gradually, and is currently in place at more than 30 ports of entry. US-VISIT will be implemented nationwide over time. DHS is also conducting a pilot program now involving exit points, collecting biometric data on individuals as they *depart* the U.S.

### SEVIS Validation and Tracking

Validation of Program Participation: Upon arrival at the destination institution, students and scholars in F and J status must report to the appropriate International Office to check in. In addition to providing welcome and orientation information at that time, the International Programs Center is required to “validate” the SEVIS record, confirming arrival in the government database. If an individual fails to appear and the SEVIS record is not validated within 30 days, the SEVIS record will revert to “inactive” status and the individual is subject to immigration enforcement action.

Program Updates: During the course of study/research/teaching, the International Programs Center is required to report progress, extensions, change of address, transfers, and other “events” to the Department of Homeland Security via SEVIS. If, at any time, the institution is unable to verify compliance of the individual with regulations in SEVIS, the SEVIS record reverts to “inactive” status and the person becomes subject to immigration enforcement action.

### Visa Extensions / Renewals

When the initial visa stamp expires and a student or scholar travels outside the U.S., he/she must seek an extension of the U.S. entry visa before returning to the U.S. All application procedures, interviews, and security checks must be repeated at the U.S. Consulate before a visa renewal is granted, in accordance with regulations.

### Applications for Immigration Benefits through the Department of Homeland Security

Students and scholars may apply within the U.S. for immigration benefits, such as a change of immigration status or employment authorization based on practical training. This application is reviewed by the Department of Homeland Security. In addition to adjudicating the application on its merits, the Department of Homeland Security’s Citizenship and Immigration Service (CIS) Service Center is required to conduct name check procedures on the applicant. CIS will not reveal the details of this process to the public.

Once an immigration benefit is granted, record of that action is entered by the CIS Service Center into the Computer Linked Application Information Management System (CLAIMS). This data is then available to ports of entry, CIS Service Centers and federal agencies.

### Departure procedures about NSEERS

National Security Entry-Exit Registration System (NSEERS), also known as Special Registration, is a U.S. government system instituted to track the entry and exit of persons born in or nationals of certain identified countries. These individuals may become subject to special registration at the time of entry to the United States. These subject individuals are required to report to the Department of Homeland Security at the international port of exit any time they depart from the country.

Staff members of the International Programs Center (IPC) provide related information and assistance to students and scholars subject to NSEERS registration during their new student and scholar orientation and prior to travel overseas

1. 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/assets/260/254194.html> [↑](#footnote-ref-1)
2. <https://www.bis.doc.gov/index.php/forms-documents/doc_view/986-740> [↑](#footnote-ref-2)
3. <https://www.federalregister.gov/articles/2012/02/13/2012-3090/list-of-countries-requiring-cooperation-with-an-international-boycott> [↑](#footnote-ref-3)
4. *See* 22 C.F.R. §§ 122.5 and 123.26. [↑](#footnote-ref-4)
5. *See* 15 C.F.R. § 762.6. [↑](#footnote-ref-5)
6. For EAR violations, see 15 C.F.R. § 764.5. For ITAR violations, see 22 C.F.R. § 127.12(c). [↑](#footnote-ref-6)