CHARLOTTE
DIVISION OF RESEARCH

Export Management Plan

I. Introduction

The Policies of the Board of Governors of The University of North Carolina provide that

- the University environment must allow faculty and students to freely pursue learning and research,
- the University must also maintain its independence and integrity to assure impartiality, and it may not agree to any inappropriate limits on the freedom to publish research findings, and
- faculty and students of the University must have the right to disseminate freely and openly their research findings, and research sponsors may not abridge this basic right.

But over the past few years the Federal government has become increasingly concerned with protecting information and technology from disclosure by universities, the release of which could hamper U.S. economic vitality or contribute to the military potential of U.S. adversaries. Export laws and regulations are the bases for restricting use and access to this information and technology and these laws may conflict with our tradition of academic freedom and openness in research. In particular, a "deemed export" (one requiring a license and imposing access restrictions) exists whenever a foreign national on U.S. soil may be exposed to or be able to access an export controlled item of information. Although there is a general exception for "fundamental research" under the export control regulations, it is frequently the case that scientific equipment in university laboratories is subject to export controls.

The vast majority of UNC Charlotte research projects can be conducted in a manner fully consistent with the principles of freedom of inquiry and open exchange of knowledge. But UNC Charlotte also plays an important role in many areas of science and technology that are of great concern to the nation and to national defense and homeland security. In a very few cases, the pursuit of knowledge may involve critically important but sensitive areas of technology where the immediate distribution of research results would not be in the best interests of society. In such cases, exceptions to UNC policies regarding publication, classification, and access by foreign students and scholars may be made, but only in those rare instances where the area of work is crucially important to UNC Charlotte's educational mission and the exception is demonstrably necessary for the national good. Moreover, UNC Charlotte University Policy 308, "*Research Relations with Private Enterprise and Publication of Research Findings*," provides that any agreement that restricts the freedom of faculty and students to publish research findings must be coordinated through the Vice Chancellor for Research and reported to the President of The University prior to its execution, to ensure that the proposed agreement will not interfere with the publication or oral defense of research theses or with the scholarship of tenure-track faculty.

The following information is provided to assist principal investigators (PIs) and contract administrators in determining whether proposed research may be subject to export controls and is intended to promote understanding of and compliance with the export control regulations.

II. Background

The Department of Commerce Export Administration Regulations (EAR) and the Department of State International Traffic in Arms Regulations (ITAR) prohibit the export of specific unlicensed technologies for reasons of national security or for the protection of trade. Similarly, the Treasury Department's Office of Foreign Assets Control (OFAC) administers and enforces boycotts that have been imposed against specific countries for reasons of foreign policy, national security, or based upon international agreements.

Export control regulations, as well as boycott programs, have the potential to impact many aspects of the freedoms typically associated with research in a university setting. Publication rights, international collaboration, sending or bringing research equipment to foreign countries, and the sharing of research technology (verbally, in writing or visually) with persons who are not U.S. citizens or permanent resident aliens can be severely restricted. The consequences of violating export control regulations can be quite severe, ranging from loss of research contracts to monetary penalties to jail time.

University Policy 316, *"Export Control",* provides that the University shall comply with all United States export control laws and regulations, including those implemented by the Department of Commerce through its Export Administration Regulations (EAR), the Department of State through its International Traffic in Arms Regulations (ITAR), and those imposed by the Treasury Department through its Office of Foreign Assets Control (OFAC). To carry out this policy, the Vice Chancellor for Research serves as the Empowered Official for export control matters for UNC Charlotte and has overall responsibility for the University's compliance with this policy. The Vice Chancellor appoints and serves *ex officio* as chair of the Export Control Compliance Committee, which develops and maintains this Export Management Plan (EMP). The Vice Chancellor, as Empowered Official, is responsible for implementing and managing the EMP.

University research projects will be regulated under export control regulations when restrictive language appears in contracts or grants that destroys the fundamental research exclusion (defined below), or when access by foreign nationals (including faculty, staff, graduate or undergraduate students, or visitors) to controlled technologies used in the research is restricted or prohibited. In such cases, the University must conduct a thorough review of research projects and contract provisions and determine whether and how a particular project is impacted by those regulations.

The University will assist investigators in assessing the application of such regulations, but primary compliance responsibility must rest with the principal investigator of the research.

III. Definitions

Export control decisions depend on a correct understanding of the following terms. The official regulatory definition should be consulted in specific applications.

Export

The term export, as used in export control regulations has an expansive meaning. Generally, an export includes any:

1) actual shipment of any covered goods or items;
2) the electronic or digital transmission of any covered goods, items, or related goods or items;
3) any release or disclosure, including verbal disclosures or visual inspections, of any technology, software or technical data to any foreign national wherever located; or

4) actual use or application of covered technology on behalf of or for the benefit of any foreign entity or person anywhere.

The official definition of export under the EAR and ITAR should be consulted when determining whether a specific act constitutes an export. As is evident in many instances, export is defined so as to preclude the participation of foreign graduate students in research that involves covered technology without first obtaining a license from the appropriate government agency.

Foreign Person

Anyone who is "not a lawful permanent resident" of the United States (*i.e.*, not a green card holder) or does not have refugee or asylum status. The term also applies to 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).

The Export Administration Regulations (EAR)

The EAR, promulgated and implemented by the Department of Commerce, control the export of equipment, technologies (including software), and technical data identified on the Commodity Control List (CCL) that serve primarily civil uses. The prohibition on the export or disclosure of technical data controlled under the EAR is determined on a country- by-country basis for each disclosure of controlled technical data. As a result, it is unlawful to export technical data out of the US or to disclose technical data in or outside the US to foreign persons of countries for which a license is required as a condition of making such exports and disclosures. The CCL is divided into ten categories:

Category 0 - Nuclear Materials, Facilities and Equipment (and Miscellaneous Items)
Category 1 - Materials, Chemicals, Microorganisms and Toxins
Category 2 - Materials Processing
Category 3 - Electronics Design, Development and Production
Category 4 - Computers
Category 5 - (Part 1) - Telecommunications - (Part 2) - Information Security
Category 6 - Sensors and Lasers
Category 7 - Navigation and Avionics
Category 8 - Marine
Category 9 - Propulsion Systems, Space Vehicles and Related Equipment

The CCL also includes a separate category (EAR99) that covers everything not expressly listed elsewhere.

The complete text of the EAR and CCL are available from the Office of Research Protections and Integrity.

The International Traffic in Arms Regulations (ITAR)

The ITAR, promulgated and implemented by the Department of State, control the export of equipment, technologies and technical data identified on the U.S. Munitions List (USML) that are primarily military in nature. It is unlawful under the ITAR to send ITAR controlled technical data to ***any*** foreign persons outside the United States or to disclose – in written, oral or visual form -- ITAR-controlled technical data to ***any*** foreign persons ***in*** or ***outside*** the United States unless one of several exclusions applies or the State Department has issued a license authorizing the disclosure or export of the technical data to specific foreign persons. The USML is divided into 21 categories:

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

The items and services identified in the USML are primarily for military applications and are referred to as “defense articles” and “defense services.” Spacecraft systems and associated equipment are also on the USML (Category XV), even though they might be for civilian use only and are not developed or used for defense applications. Complete versions of ITAR and USML are available from the Office of Research Protections and Integrity.

Commodity Jurisdiction Ruling

Where an article is arguably covered by both the EAR and ITAR, a request can be made to the State Department to determine which agency will have jurisdiction over the export of the article.

Embargoed Countries

The Office of Foreign Assets Control (OFAC) in the U.S. Department of the Treasury administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. While embargoes vary from country to country, five countries have been identified as state sponsors of terrorism and have substantial restrictions on activities. The countries, informally referred to as the T5, include:

- Cuba
- Iran
- North Korea
- Sudan, North and South
- Syria

Contact the Office of Research Protections and Integrity for a list of countries currently on OFAC’s sanctions and denied parties lists. The list changes frequently as countries are added and dropped. Any questions or concerns should be addressed to the Export Control Office.

Fundamental Research

As used in the export control regulations, *fundamental research* includes 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 which 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 accepts any restrictions on the publication of the information resulting from the research, other than limited prepublication reviews by research sponsors to prevent inadvertent divulging of proprietary information provided to the researcher by sponsor or to insure 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 the university or the researcher. The citation for the official definition of Fundamental Research under the EAR is 15 CFR 734.8. The ITAR citation is 22 CFR 120.11. The Fundamental Research Exclusion never applies to the import and export of items restricted by an embargo.

Public Domain

As defined in 22 CFR 120.11, *public domain* means information that is published and that is generally accessible or available to the public: (1) through sales at newsstands and bookstores; (2) through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information; (3) through second class mailing privileges granted by the U.S. Government; (4) at libraries open to the public or from which the public can obtain documents; (5) through patents available at any patent office; (6) through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public, in the United States; (7) through public release (i.e., unlimited distribution) in any form (e.g., not necessarily in published form) after approval by the cognizant U.S. government department or agency; and (8) through *fundamental research.*

Technology (EAR)

Specific information necessary for the "development", "production", or "use" of a product. "Use" is further defined as "operation, installation (including on-site installation), maintenance (checking), repair, overhaul, and refurbishing" of equipment. Note the use of *and*: all six activities in the definition of "*use*" must be present to trigger a license requirement. Thus, in considering whether the export of technology has occurred when a foreign national "uses" equipment in a university laboratory, all six of these activities must have occurred for deemed export to have taken place.

Technical Data (ITAR)

Information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles, including information in the form of blueprints, drawings, photographs, plans, instructions, or documentation. This definition does not include information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities or information in the public domain. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles. The export laws and regulations determine if technical data is controlled, not your intended or actual use of the information.

Classified Technical Data

Information only released to persons with the appropriate level of clearance and the appropriate need-to-know. Classified information is not authorized for release or disclosure to any foreign national.

No classified access will be provided to unauthorized foreign nationals. Foreign nationals will be denied access to areas where classified design, development, and testing occurs, as well as to any area where classified work is in progress.

Foreign nationals are not authorized access to classified contracts, contracts of a sensitive DOD nature (contracts that incorporate DFARS Clause 252.204-7000 or a modification thereof), or contracts with export restrictions without the proper authority and/or license.

Contact the Facilities Security Officer (704-687-1877 or fso@uncc.edu) for further information regarding security clearances, classified document control, foreign visitor information, security inspections, etc.

IV. Computer Software Export Rules

The export regulations have a number of special rules for computer software. Under ITAR, certain software might expressly be listed on the USML. Other software might be controlled because it relates to the design process, operation, maintenance or other activities specifically related to USML articles.

Each category of technology in the EAR CCL has a special subcategory for computer software, with its own special rules. The EAR also has special rules for mass-market software. In addition, the EAR has some extensive rules for software (specifically "encryption software") that performs security functions or uses such functions performed by other software or equipment.

V. Export Controlled Services

Export regulations control certain services (*e.g.*, "defense services" under ITAR), even if all of the information used or transferred in association with the services is publicly available and not otherwise controlled under the regulations. Controlled services may assist military or space activities, assist with encryption commodities or software, or assist embargoed countries.

VI. Exclusions and Exemptions under the Export Rules

Publicly available information is excluded from export regulations under both EAR and ITAR. Note that even though the information itself may not be subject to export control, the activity for which it is used may still be controlled, such as a defense service under ITAR or a service to an embargoed country.

These exclusions apply only to research results. They do not apply to controlled equipment and/or services, such as training foreign nationals inside or outside the U.S. on defense articles. A PI could have a contract that places no restriction on publishing research results or access to the project but requires a license for the PI to send controlled equipment to a foreign collaborator.

ITAR Exemptions

Under ITAR, the exclusion for publicly available information is made indirectly, by specifying that such information is not included in the definition of "technical data," as that term is used with regard to the controls under ITAR. ITAR references publicly available information as being "public domain." The term "public domain" under ITAR does not mean dedicated to the public, which is the definition under intellectual property law. Under the EAR, the exclusion for publicly available information is more directly and expressly made.

Under ITAR, public domain means information which is published and which is generally accessible or available to the public:

- through sales at newsstands and bookstores;
- through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information;
- through second class mailing privileges granted by the U.S. Government;
- at libraries open to the public or from which the public can obtain documents;
- through patents available at any patent office;
- through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public, in the United States;
- through public release (i.e., unlimited distribution) in any form (e.g., not necessarily in published form) after approval by the cognizant U.S. Government department or agency; or
- through fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community. Fundamental research is defined to mean basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or where specific U.S. Government access and dissemination controls apply.

University research will not be considered fundamental research if the university or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity; or the research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable.

ITAR also expressly excludes from the definition of "technical data," and thus from control, information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities. In general, to meet this test, the course in which the information is taught must be listed in the university catalog.

In addition, ITAR specifically exempts from the requirement of a license disclosures of unclassified technical data in the U.S by U.S. institutions of higher learning to foreign persons who are their bona fide and *full time regular employees*. This exemption is available only if:

- the employee's permanent abode throughout the period of employment is in the United States;
- the employee is not a national of a country to which exports are prohibited pursuant to Sec. 126.1 of ITAR; and
- the institution informs the individual in writing that the technical data may not be transferred to other foreign persons without the prior written approval of the Department of State.

Determinations on whether a foreign national qualifies for this exemption must be done on an individual basis by the Office of Research Protections and Integrity.

Further, ITAR includes an exemption from the licensing requirement for certain items and defense services for space applications by accredited U.S. institutions of higher learning when the items or services are for fundamental research and are for organizations in certain countries, such as those belonging to NATO.

EAR Exemptions

The following items *are not* subject to the EAR:

- items that are exclusively controlled for export or re-export by certain other departments or agencies of the U.S. Government;
- pre-recorded phonograph records reproducing, in whole or in part, the content of printed books, pamphlets, and miscellaneous publications, including newspapers and periodicals; printed books, pamphlets, and miscellaneous publications including bound newspapers and periodicals; children's picture and painting books; newspapers and periodicals, unbound, excluding waste; music books; sheet music; calendars and calendar blocks, paper; maps, hydrographic charts, atlases, gazetteers, globe covers, and globes (terrestrial and celestial); exposed and developed microfilm reproducing, in whole or in part, the content of any of the above; exposed and developed motion picture film and soundtrack; and advertising printed matter exclusively related thereto.
- publicly available technology and software, except certain encryption software, that:
    - are already published or will be published as generally accessible to the interested general public in any form, including
        - in periodicals, books, etc;
        - ready availability at libraries;
        - in patents and published patent applications;
        - released at an open conference, meeting, seminar, trade show, or other open gathering; or
        - submissions of papers to domestic or foreign editors or reviewers of journals or to organizers of open conferences with the understanding that the papers will be made publicly available if favorably received;
    - arise during or result from fundamental research;
    - are educational information released by instruction in catalog courses and associated teaching laboratories of academic institutions; or
    - are included in certain patent applications.
- fundamental research, defined in the EAR as 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 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. Research conducted by scientists, engineers or students at a university (defined as an accredited institution of higher education in the United States) normally will be considered fundamental research.

VII. Research Project Compliance

The Office of Research Protections and Integrity (ORPI) will work closely with faculty and staff engaged in research at the University to help them comply with export control regulations and identify appropriate actions to take, but primary responsibility for compliance rests with the PI. UNC Charlotte's research proposal development system has several questions pertaining to export control (traveling or shipping to a foreign country, sending software to a foreign country or foreign national, and foreign national participation on a research team) and PIs should answer these questions accurately when submitting a proposal to the college sponsored programs office or ORS. If a PI knows that a Materials Transfer Agreement will require shipping materials out of the country, or if a college sponsored programs officer believes that there is an export control issue with a proposal or agreement, they should notify the Export Control/Facility Security Officer (704-687-1877 or exportcontrols@uncc.edu), who will work with the appropriate persons to ensure compliance with export control regulations.

The Contracting Officer in the Office of Grants and Contracts Administration (GCA) will screen for export control issues during contract review, including research restrictions, international travel and/or shipments, third party provided information, military applications, foreign visitors, and denied parties. Such issues often require additional negotiations and coordination with the Export Control/Facility Security Officer.

Upon receipt of an award, and prior to release to post-award accounting, the Post Award Specialist in ORS will identify export control issues flagged during proposal development. If an award contains a research restriction that would take the project outside the Fundamental Research Exclusion, the Export Control/Facility Security Officer will determine whether the project involves any items on the Commerce Control List that would raise the risk of a deemed export violation and, if so, will coordinate the development of an appropriate Technology Control Plan (TCP) to ensure compliance with the export control regulations.

The University subscribes to the eCustoms Visual Compliance database and utilizes this service for screening companies, foreign visitors, and other individuals against the various denied parties lists. These reviews are conducted by the Contracting Officer, Export Control/Facility Security Officer, or college sponsored programs staff. Training for the use of eCustoms is offered several times each year to administrative staff who review proposals or contracts, manage controlled equipment or Technology Control Plans, or who need to screen for export control issues in Business Affairs (*e.g.*, Financial Services or Purchasing).

VIII. Encryption

Encryption software is controlled because of its functional capacity, and not because of any informational value of such software; such software is not accorded the same treatment under the EAR as other "software".

If you are working with encryption software in either source code or object code that is specifically designed or developed for a military, intelligence, or space application (including telemetry and GPS receiving equipment), you will be subject to the International Traffic in Arms (ITAR) regulations and you should contact the Export Control/Facility Security Officer at 704-687-1877 or fso@uncc.edu for guidance. The following information applies only to dual-use technology covered by the Export Administration Regulations (EAR).

Encryption is addressed under the EAR in Category 5 Part 2 of the CCL, at 5A002 (encrypted hardware) and 5D002 (encryption software) and includes any of the following:

- A "symmetric algorithm" employing a key length in excess of 56-bits (note: parity bits are not included in the key length);
- An "asymmetric algorithm" where the security of the algorithm is based on any of the following:
    - Factorization of integers in excess of 512 bits (*e.g.*, RSA);
    - Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (*e.g.*, Diffie-Hellman over Z/pZ); *or*
    - Discrete logarithms in a group in excess of 112 bits (*e.g.*, Diffie-Hellman over an elliptic curve);
- Designed or modified to perform cryptanalytic functions;
- Specially designed or modified to reduce the compromising emanations of information bearing signals beyond what is necessary for health, safety, or electromagnetic interference;

- Designed or modified to use cryptographic techniques to generate the spreading code for spread spectrum systems, including the hopping code for frequency hopping systems;
- Designed or modified to use cryptographic techniques to generate channelizing codes, scrambling codes, or network identification codes for systems using ultra- wideband modulation techniques and having a bandwidth exceeding 500 MHz or a "fractional bandwidth" of 20% or more;
- Communications cable systems designed or modified using mechanical, electrical, or electronic means to detect surreptitious intrusion;
- Designed or modified to use quantum cryptography, also known as quantum key distribution (QKD).

Encryption software that meets one of the bullet definitions above is referred to as "strong" encryption, but there may be other definitions or restrictions as well. For example, hash functions are generally considered to be strong encryption. Therefore, we may need to consult with the Department of Commerce if questions arise. Under EAR, strong encryption software is **NOT**:

- Cryptographic code limited to authentication and digital signature including associated key management functions;
- Software using fixed data compression or coding techniques;
- Encryption/decryption code designed to protect libraries, design attributes or associated data for the design of semiconductor devices or integrated circuits.

Throughout this document, the term "encryption" shall mean "strong encryption" unless otherwise noted.

Both E*ncryption Technology* and *Encryption Software* are covered under the export control regulations, but the two categories are regulated differently. *Encryption Technology* broadly refers to algorithms, protocols, hardware (including embedded systems), or other forms of technology that perform encryption functions. *Encryption Software* refers to any source code or object code that implements encryption technology.

Encryption Technology is regulated in the same manner as other technology entries in the Commerce Control List (CCL) and can take advantage of the Fundamental Research Exclusion and the Educational Exclusion. Thus, encryption technology taught as part of the University curriculum is not subject to the export control regulations, but care needs to be taken that research on encryption technology is conducted under the umbrella of the Fundamental Research Exclusion. If a publication or other restriction has been accepted, thereby negating the Fundamental Research Exclusion, encryption research can be subject to Deemed Export restrictions. Encryption technology is also subject to §744.9, which states that "no U.S. person may, without authorization, provide technical assistance (including training) to foreign persons with the intent to aid a foreign person in the development or manufacture outside the U.S. of encryption commodities and software that, if of U.S. origin, would be controlled." The regulations specifically provide that university teaching does <u>not</u> constitute "technical assistance" as defined by §744.9, but consulting (including training) to a foreign national or foreign entity (whether for free or for a fee) <u>would</u> constitute such assistance. Working with foreign visitors who are not students or employees of the University, on topics involving encryption technology, would also constitute such assistance.
Encryption Software is regulated differently from other software entries in the CCL. Because encryption items can be used to maintain the secrecy of information, export controls on encryption software are distinguished from controls on other software, and the Fundamental Research Exclusion does not apply.

The regulations specifically provide that the release of object code within the U.S. does not constitute deemed export. The release of source code within the U.S. is covered by license exception ENC (§740.17.a.2.) and applies to all foreign nationals except those from the T5 (terrorist-supporting) countries. Source code or object code sent or taken outside the U.S. (including via email or provided to a foreign embassy or consulate within the U.S.) is subject to export control restrictions. License exception ENC may again apply and countries listed in Supplement 3 to Part 740 may be subject to favorable treatment but, as a general rule, University employees may not take or send source code or object code employing encryption outside the U.S. without the prior approval of the Vice Chancellor for Research.

Publicly available software under the EAR is exempt from export control. However, before strong encryption code is made publicly available via the internet or otherwise placed electronically in the public domain, the U.S. government must be notified of the internet location (URL) of the code. This must be done before making the software publicly available. Notification after the software is publicly available could be an export control violation.

ACTION REQUIRED: EAR Strong Encryption Compliance

Create a publicly accessible website where your UNC Charlotte-developed strong encryption software will be available and email the Export Control/Facility Security Officer (fso@uncc.edu) with the internet location or URL of that website. Next, send an email to **BOTH crypt@bis.doc.gov and enc@nsa.gov** with a short description of the software and the URL to the website where the software can be downloaded. Do **not** attach the software to the email. Then upload the software (both source code and object code) to the website. The encryption software must be freely downloadable by all interested members of the scientific community at no charge and without UNC Charlotte's knowledge of whom or from where the data is being downloaded. This means no login requirement or other password or authentication procedures. The government could view a login or other authentication requirement as an access control, and such a requirement could destroy the University's ability to characterize the generated software as in the public domain without restriction. Note that you do not have to notify the Government of updates or modifications to your encryption code as long as the URL of your publicly accessible website does not change.

Publicly available dual-use encryption software that does not entail "strong" encryption is controlled only for the T5 (terrorist-supporting) countries. For non-T5 countries, such "weak" encryption software requires neither government notification nor review and can be freely shipped, shared, transferred, or transmitted outside of the U.S.

Encryption Summary:

Faculty CAN:

- Teach any encryption topic to any student in a University class;
- Release any encryption software source code or object code to any person within the boundaries of the U.S., except that such code may not be provided to a foreign consulate or embassy or to a citizen of a T5 country;
- Publish open source encryption software, provided that appropriate notification has been given to the federal government;
- Submit a paper on any encryption topic for publication in any U.S. or foreign journal (a printed book or other printed material setting forth encryption source code is not itself subject to the EAR. However, encryption source code in electronic form or media, such as diskette or CD ROM, remains subject to the EAR);
- Submit and/or present a paper on any encryption topic to any U.S. or foreign "open" conference.

To qualify as an "open" conference, attendees must be permitted to take notes and any registration fee must be reasonably related to costs and reflect an intention that all interested and technically qualified persons should be able to attend.

Faculty and students CANNOT do any of the following without the prior approval of the Vice Chancellor for Research:

- Take or send outside the U.S. (physically or via email) any encryption technology or any software with strong encryption;
- Provide consulting or training services (either free or for fee) to a foreign national or foreign entity, or work with a foreign visitor, on encryption topics.

Faculty CANNOT:

- Provide any information outside the classroom to any citizen of a T5 (terrorist-supporting) country, including students, on any encryption topic, strong or otherwise.

Faculty SHOULD NOT:

- Accept any restrictions on encryption research (such as a publication restriction or an industry non-disclosure agreement) without a careful assessment of the risk of deemed export through foreign nationals (faculty, staff, or students) who might be exposed to the work.

In any case where a restriction exists, one can apply for an export control license. Licenses require several months for approval and have duration of 48 months; approximately 90 percent of applications related to encryption are approved.

IX. Controlled Equipment

The University must provide appropriate oversight of equipment and technology on either the Commerce Control List or the U.S. Munitions List in order to ensure that unlawful export or deemed export does not take place. To help manage this oversight responsibility, the Office of Research Protections and Integrity will maintain an inventory of controlled equipment. Laboratories or facilities that contain controlled equipment must develop a **Technology Control Plan** (TCP), describing procedures to prevent the occurrence of unlawful export or deemed export. Each TCP will be shared with the Export Control Compliance Committee to ensure that the plan and associated procedures are appropriate.

X. Foreign Visitors

Foreign visitors and post-doctoral fellows who will be given access to buildings or laboratories containing controlled equipment must be screened by the Office of Research Protections and Integrity and must have a plan of work or study approved in advance by the Vice Chancellor for Research. That plan cannot be specifically for the study of an item of controlled equipment or for training in the use of such equipment. Such equipment may be used as research tools, but cannot be disassembled or otherwise analyzed, and faculty or staff members who inadvertently enable visitors to access controlled technology could be at considerable personal legal risk. Foreign visitors could also be at risk if they are found alone in a laboratory which houses controlled equipment or if they are present when such equipment is being maintained. For these reasons, foreign visitors will not be granted open access to labs containing controlled equipment and must be accompanied at all times by a lab supervisor or their designee. Screening requests should be submitted to the Export Control/Facility Security Officer (704-687-1877, exportcontrols@uncc.edu). Plans of work or study should be discussed with the Vice Chancellor or Assistant Vice Chancellor of Research.

XI. Employment of Foreign Nationals

The U.S. Citizenship and Immigration Services (USCIS) Form I-129 (Rev. 11/23/10) "Petition for a Nonimmigrant Worker" requires U.S. employers to certify their compliance with U.S. export licensing requirements when petitioning for H-1B, H1-B1, L-1, and O- 1A visa classifications on behalf of employees. Affected employees requiring the export certification could include faculty, post-doctoral candidates, technicians, or other staff categories. This certification is not required for student (F-1) or Visiting Scholar (J-1) visa petitions.

Part 6 of the I-129 is formally referred to as a *Certification Regarding the Release of Controlled Technology or Technical Data to Foreign Persons in the United States*, and has to do with any technology or technical data that the University might release to the foreign national (which would constitute "deemed export") and whether an export license will be required if such release involves controlled technology (EAR) or technical data (ITAR). Specifically, the University is required to certify that it has reviewed the EAR and the ITAR and has determined that:

1. A license is not required from either the U.S. Department of Commerce or the U.S. Department of State to release such technology or technical data to the foreign person; *or*

2. A license is required from the U.S. Department of Commerce and/or the U.S. Department of State to release such technology or technical data to the beneficiary and the petitioner will prevent access to the controlled technology or technical data by the beneficiary until and unless the petitioner has received the required license or other authorization to release it to the beneficiary.

Completing Form I-129, Part 6

UNC Charlotte's Office of International Programs will inform the hiring official of the *Certification* requirement and will provide information from the visa petition to the Office of Research Protections and Integrity (ORPI). ORPI staff will work with the hiring official in reviewing the employee's planned work or research and will determine whether a license IS or IS NOT required, and will advise the certifying official in the Office of International Programs so that the correct box can be checked in Part 6 of Form I-129. If an export license is needed from the Department of Commerce or Department of State, ORPI will assist in preparing the license request and submit it on behalf of the University. Licenses can require several months for approval.

Completion of Part 6 of Form I-129 is a one-time requirement. No amendment to the form is required should circumstances change after the form is submitted.

XII. Travel to Foreign Countries & Sharing Information with Foreign Nationals

Most of the items, information, or software that UNC Charlotte shares with its colleagues and research partners are not of a nature subject to restriction by export control regulations, nor are they destined for countries or individuals subject to US embargoes or sanctions. The University must, however, exercise due diligence, and if you think there is any possibility that the items or information that you intend to share with a foreign national might be controlled, you should request a review by the Export Control/Facility Security Officer. This will ensure that we comply with US export law and will protect faculty and staff from unknowingly violating that law. Decision Trees for such review are provided on the Export Controls Resources page.

Faculty and staff who travel abroad with a laptop, PDA, cell phone, or digital storage device should know the risks involved. If the computer or other equipment is owned by the University, the equipment as well as any installed encryption software may be eligible for License Exception TMP (Temporary Exports). To qualify for this exception, the equipment:

- Must be a "tool of the trade."
- Must remain under your "effective control" while overseas. This means that it must remain in your personal possession (in a locked hotel safe or a locked hotel room is not sufficient) at all times.
- Must be returned to the U.S. (or destroyed) within 12 months.
- May not be taken to one of the T5 (terrorist-supporting) countries.

Before hand-carrying any of these items abroad, a certification form (International Travel with University-Owned Equipment) should be filed with the Export Control/Facility Security Officer to document that items are being exported under License Exception TMP. Contact the Export Control/Facility Security Officer at 704-687-1877 or exportcontrols@uncc.edu with any questions.

If you personally own the equipment, it may qualify for License Exception BAG (Baggage). To qualify for this exception, the equipment and retail-level encryption software must be for your personal use in private or professional activities.

You should also be aware that Federal agents may conduct searches of an international traveler's laptop computer or other electronic device without any suspicion of wrongdoing, including taking the device to an off-site location for an unspecified period of time. This policy applies to anyone entering the country, including US citizens.

The Vice Chancellor for Research will periodically send a travel advisory to faculty and staff to remind them of these issues.

XIII. Shipping to Foreign Countries

Before shipping any item to a foreign country, including to colleagues or research partners, you should determine if the item is controlled for export by contacting the Export Control/Facility Security Officer (704-687-1877 or exportcontrols@uncc.edu). In particular, note that shipment of "anything of value" to embargoed countries is restricted or prohibited.

In accordance with 15 CFR Part 30; shipments headed outside the U.S., except to Canada, that exceed $2,500 in value per Schedule B number must be filed electronically through the Automated Export System(AES) for most exports of merchandise valued at more than $2,500 from the United States, Puerto Rico and the U.S. Virgin Islands to foreign countries or between the U.S. Virgin Islands, Puerto Rico and the United States. The AES filing is also required for all exports under the Bureau of Industry and Security (BIS) or State Department export license or license exception/exemption regardless of the value unless the export is temporary and hand carried or exported in your personal baggage under a "tools of trade" license exception.

Shipments exempt from filing under 15 CFR 3O Appendix D shall provide for the legend describing the basis for the exemption which shall be made on the first page of the bill of lading, airway bill, or other commercial loading document for carrier use, or on the carrier's outbound manifest.

XIV. Records and Documentation

The export control regulations contain specific record keeping requirements that must be satisfied. Departments must keep copies of all export documentation, including required licenses, financial records and shipping documentation such as invoices, Shippers Export Declarations (SEDs), Automated Export System (AES) records, and any internal campus forms related to export control regulations in their research project files for a period of five years from the date of the export, re-export, or controlled deemed export. In addition, copies of such records should be sent to the Office of Research Protections and Integrity.

Record keeping requirements under the EAR are detailed under §762.2 - 762.7. Original records are required except as provided for in §762.4. These regulations also detail requirements for digital archives, and provisos for written procedures, authorized individuals, inability for records to be altered and the quality of copies. Destruction of records is allowed after five years except for records of voluntary self disclosures and records previously required by BIS. Both require BIS approval for destruction.

Record keeping requirements under ITAR are detailed under §122.5 (Maintenance of records by registrants) and §123.26 (Requirement for exceptions). Records must be retained for five years from the expiration of the ITAR license or other approval. Technical Assistance Agreements that are no longer needed must be terminated and any unused, expired, expended, suspended or revoked licenses must be returned immediately to the Department of State.

XV. Business Affairs

UNC Charlotte's Division of Business Affairs, which plans for and provides essential human, financial, facility, and administrative support services to the University, will help ensure compliance with export control regulations in the execution of its functions. [NOTE: Research Project Compliance is specifically addressed in Section VII of this plan, and all research activities should be monitored in accordance with that section.] Departments within Business Affairs include:

- Business Services;
- Facilities Management;
- Financial Services;
- Human Resources;
- Safety and Security;
- Technical Operations and Planning (TOP); and
- Internal Audit.

These departments may encounter export controls and help monitor transactions and activities subject to export control regulations in the following capacities:

Ancillary Activity

Business Affairs staff members may encounter export controls related activities in ancillary matters. If needed, staff will contact the Export Control Officer for guidance.

Awareness and Training

The Office of Research Protections and Integrity (ORPI) is responsible for conducting periodic training with potentially affected individuals or groups to ensure staff are properly trained in export control compliance.

Units that are involved directly in export controls monitoring roles, including those involving research, technology transfers, procurement, shipping, and international transactions or travel, will be included in these trainings to ensure staff are adequately equipped to help protect the University from export control violations. Business Affairs staff identified to have direct monitoring roles include:

- CONTROLLER'S OFFICE: Accounts Payable, General Accounting, Travel & Complex Payments
- HUMAN RESOURCES: Staff Employment, Temporary Employment
- INTERNAL AUDIT
- MAIL SERVICES
- MATERIALS MANAGEMENT: Purchasing, Inventory Control & Surplus Property, Receiving & Stores
- SAFETY AND SECURITY

Shipping

The Mail Services unit within Business Services, as well as the Materials Management unit within Financial Services, will help ensure that no shipments are sent by the University to embargoed countries, nationals of sanctioned countries, or specific restricted foreign entities and individuals, as defined by OFAC. Mail Services will adhere to policies set forth by the United States Postal Service.

For United States Postal Service guidelines, see the USPS International Mail Manual – Issue 32, Non-postal Export Regulations, Section 530 Commodities and Technical Data.

Risk Management and System Reviews

Safety and Security and Internal Audit will assess risk and analyze the efficacy of the export control system on a periodic and as-needed basis. Staff will work with ORPI and the Export Control Officer in these cases to ensure accurate assessment. Review areas may include, but are not limited to:

- Record keeping system
- Awareness and training programs
- 'Reasonable' compliance with export control laws, regulations, and requirements outlined in this plan

Biosafety

The Export Control Officer will work with the Biosafety Officer to ensure compliance with export control regulations applicable to biological materials.

Employment

Human Resources will assist the University's Office of International Programs and the Office of Research Protections and Integrity (ORPI) for any employment of foreign nationals, as described in Section XI of this plan.

Financial Services

Staff members within several Financial Services units are in positions to identify transactions and activities that may be subject to export control regulations. When, during the course of their duties, it is determined that a transaction or activity may fall under these regulations, staff will notify the Export Control Officer of the transaction to determine whether documentation exists to support authorization of the activity, whether an exception or exemption applies, whether an export license is required, and/or whether the activity is prohibited.

The following schedule summarizes responsibilities of Financial Services units as they are relevant to export controls:

Financial Services Unit	Relevant responsibilities	EMP Section	Monitoring Activities	Internal Guidance
Accounts Payable	Processes vendor payments	XV	Check that financial transactions are not to/from restricted countries.	Accounts Payable procedures
General Accounting	Manages receipt and transmission of international wire transfers	XV	Check that international wire transfers and financial transactions are not to/from restricted countries.	Wire transfer procedures
Materials Management	Oversees all international business contracts; Manages purchasing, shipment, and payment for commodities (including chemicals, microorganisms, and toxins), supplies, equipment, and technology (including computers and software)	XIII	Review foreign contracts for prohibition of export regulation violations. Screen vendors and equipment suppliers to ensure that they are not on any government lists. Ensure shipments are not to/from restricted countries.	University Purchasing Manual
Travel & Complex Payments	Facilitates international travel and business expense payments	XII	Check countries employees are traveling to for embargoes, sanctions, and restrictions. Be aware of any prohibited financial transactions/ payments for services.	University Travel Procedure Manual

Please see the internal documents listed above for further guidance for staff in those respective areas.

Controlled Equipment

Controlled Equipment, as defined in Section IX of this plan, includes equipment and technology whose records are not maintained by the Fixed Assets or Inventory Control units; thus, ORPI must maintain a separate inventory of controlled equipment. Staff from both the Fixed Assets and the Inventory Control units will work with the Export Control Officer in any supporting function as appropriate.

The Office of Foreign Asset Control (OFAC)

The Office of Foreign Asset Control (OFAC), an agency under the U.S. Department of the Treasury, administers and enforces economic sanctions programs to block assets and restrict trade in accordance

with U.S. foreign policy and national security goals.

Embargoes and sanctions are enforced against foreign countries, individuals, and organizations identified as being terrorists, international narcotics traffickers, or those supporting proliferation of weapons of mass destruction. Individuals and companies that are owned or controlled by, or acting for or on behalf of, targeted countries, as well as targeted individuals, groups, and entities that are not country-specific, are referred to as 'Specially Designated Nationals' or 'SDNs'. OFAC publishes and maintains an SDN List on its website (see 'Further Resources' below).

OFAC monitors all financial and trade transactions with embargoed and sanctioned entities as described above. These transactions, including transmission of cash through wire transfers from U.S. banks, provision of technologies or services, and any other movement of cash or assets, are prohibited without an exemption or a general or specific license.

In general, the University should avoid activity with embargoed and sanctioned entities. If the activity is deemed necessary for research or other purposes related to the University's mission, the Export Control Officer should be contacted to facilitate requesting and obtaining the necessary license from OFAC and the U.S. Department of Commerce or State. The process for obtaining a specific license is necessarily rigorous and restrictive.

Questions about how the export regulations apply to specific situations may be directed to the Export Control/Facility Security Officer (704-687-1877, exportcontrols@uncc.edu) or Dr. Angelica Martins, Executive Director of Research Protections and Integrity (704-687-1876, A.Martins@uncc.edu).

Revision History
Created 07/25/12;
Updated 06/02/14; 01/15/16; 04/03/17; 02/10/2023