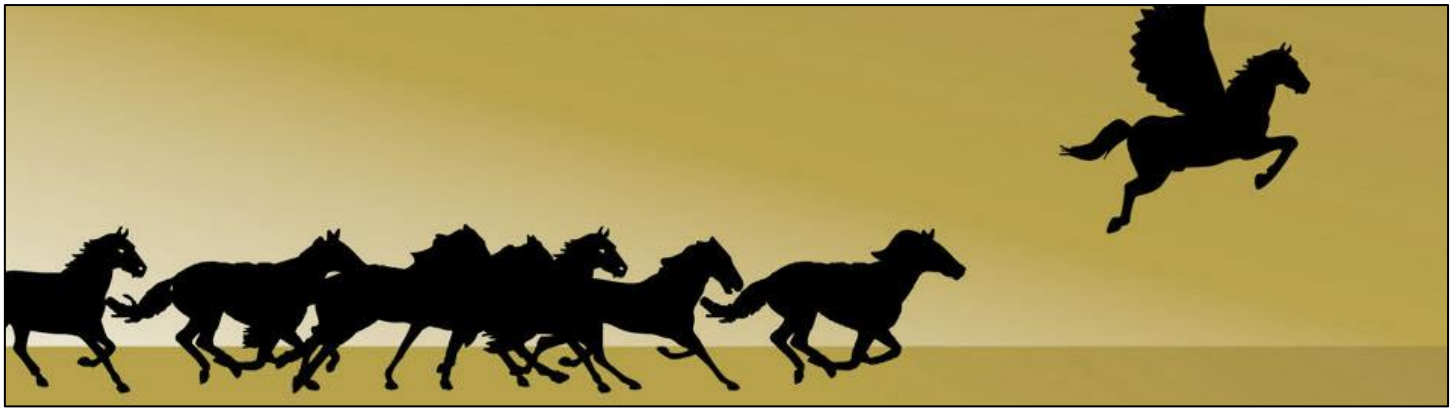
UNIVERSITY OF CENTRAL FLORIDA
EXPORT COMPLIANCE

EXPORT CONTROL

MANAGEMENT PLAN



UNIVERSITY OF CENTRAL FLORIDA – OFFICE OF EXPORT CONTROLS COMPLIANCE
12201 RESEARCH PARKWAY, ORLANDO FL 32826

CONTENTS

1.1.1 Forward

The purpose of university research is to develop technologies for the benefit of mankind and share knowledge with the world. There is a dichotomy between conducting university research and the limitations imposed on universities on the sharing of their research techniques and resulting fruits. On the one hand exists the researcher striving to acquire and disseminate knowledge. On the other is the U.S. Government, entrusted with ensuring the prosperity of our nation by "regulating" the dissemination of commodities and knowledge based upon constantly shifting geopolitical factors, such as national security, foreign policy, nonproliferation, and short supply interests.

The government, through various means, executes policy concerning how we, as a nation, are to interact with other countries, steering the best course for the United States as a whole. Of importance to the university researcher are the control measures the government has employed to regulate certain commodities and military technologies, and the sanctions imposed on specific countries. These control measures dictate how, to whom, and to what extent, research, techniques, and the resulting fruits can be shared, and are detailed in numerous export control laws, directives and regulations.

There has been an ongoing debate about whether the fruits and conduct, including information required to perform research qualify for exemption from U.S. export control regulations and sanctions. The sense of the U.S. Senate has been that "the use of technology at an institution of higher education in the United States should not be treated as an export of such technology for purposes of the Export Administration Act", which are typical only for commercial items on programs without proprietary or national security restrictions.

The arcane world of export controls consist of a variety of federal laws, enacted in multiple regulations, administered by numerous federal agencies, so many in fact that the regulatory structure is a patchwork of often overlapping regulatory regimes that are confusing. While certain agencies have exclusive jurisdiction over specific practices, commodities or activities, other agencies serve in oversight, enforcement or advisory capacities, with sometimes broader jurisdiction.

University operations in general are subject to all of these requirements, just as they apply to all U.S. corporations and entities, including you and me, for example, when we travel in and out of the U.S. UCF is one of the few institutions that self-impose additional security requirements by allowing researchers to accept and perform research subject to proprietary or national security restriction, which by their nature require additional regulatory oversight and compliance on our research activities. It is important to note that many of these regulatory requirements and burdens would apply to UCF regardless of whether we refused research subject to restrictions.

Because we have decided to engage in research that is not otherwise exempt from U.S. regulatory requirements, compliance is required, in particular but not exclusive to research activities, due to the severe civil and criminal fines and penalties associated with willful or knowing violations. These penalties are severe and may include incarceration and the loss of research privileges, or debarment. This is in addition to the routine export control compliance efforts that are separate from research activities, such as international travel or the transfer of certain monies in and out of U.S. territories.

This Export Control Management Plan is an instruction tool to document compliance protocols implemented at UCF for compliance with U.S. export control laws, regulations and sanctions.

1. GENERAL

1.2 REVISION HISTORY

Revision	Date	Paragraph	Description of changes
1	1/20/2010	Document	Initial
2	3/25/2014	Document	Update with revised ORC processes

1.3 RESERVED

1.4 ACRONYMS

Term	Meaning
AECA	Arms Export Control Act
BIS	Bureau of Industry and Security
CCL	Commerce Control List
CFR	Code of Federal Regulations
CAU	Custody, Access and Use Agreement
DDTC	Directorate of Defense Trade Controls
DoC	U.S. Department of Commerce
DoS	U.S. Department of State
DoT	U.S. Department of the Treasury
EAA	Export Administration Act
EAR	Export Administration Regulations
ECCN	Export Control Classification Number
ECO	Export Control Officer
FACR	Foreign Assets Control Regulations
FSO	Facility Security Officer
ITAR	International Traffic in Arms Regulations
MOU	Memorandum of Understanding
NISPOM	National Industrial Security Program Manual
OFAC	Office of Foreign Assets Control
ORC	Office of Research and Commercialization
PI	Principal Investigator
TCP	Technology Control Plan
UCF	University of Central Florida
USML	U.S. Munitions List

1.5 ACKNOWLEDGEMENTS

The University of Central Florida (UCF) acknowledges and appreciates Virginia Polytechnic Institute and State University (Virginia Tech) and the University of Florida (UF) for granting UCF permission to alter selected portions of their "Export Control Compliance Program Guidelines" for use in this instruction.

1.6 DISCLAIMER

The UCF Export Controls Compliance Program, Guidelines, Technology Control Plan, process and other materials are specifically tailored to the UCF research community. This instruction and all other materials therein are not intended to replace any regulatory document of interpretation or to relieve importers or exporters of their statutory responsibility to comply with current laws, regulations, policies and procedures of the U.S. Government. UCF's export control content may not apply to other specific situations that occur outside of the UCF research community or may be incomplete. UCF's export control materials do not constitute legal advice. Those outside of the UCF research community should not act or rely on any of this information and should seek the advice of an attorney before taking any actions.

This section intentionally blank

2 APPLICABLE U.S. LAWS & REGULATIONS

As a public institution of higher education, UCF employs foreign nationals and hosts foreign visitors in connection with international exchange programs, international students, international research collaborations, and other business agreements. It is the intent of UCF to employ foreign nationals and host international visitors, both long and short term, in the most welcoming manner possible while also assuring compliance with U.S. laws, regulations and trade sanctions governing the export of certain commodities and technical data.

2.1 INTERNATIONAL TRAFFIC IN ARMS REGULATIONS

The Arms Export Control Act ("AECA"), implemented by the International Traffic in Arms Regulations ("ITAR") and administered by the State Department's Directorate of Defense Trade Controls prohibits the export, temporary import of defense articles and technical data, the manufacture abroad of defense articles using U.S. technology, the provision of defense services to foreign persons and the brokering of defense articles or services by all U.S. persons unless approved in advance by a DDTC-issued export license, agreement, or by qualification of an ITAR exemption. This includes the export of defense articles and defense services from the United States to any foreign destination or to any foreign person, whether located in the United States or abroad. The ITAR prohibits the export of all defense articles and services unless specifically permitted by the process described in the ITAR. ITAR controls are based on national security/nonproliferation and foreign policy considerations. There is considerable overlap among the policies underlying the ITAR and the Export Administration Regulations administered by the Commerce Department. Nevertheless, the objective of ITAR is to limit access to and use of "munitions" and related services and data— as opposed to dual-use items and technologies—to purposes and end-users that serve the foreign policy interests of the United States. As a result, the State Department is generally considered much less sensitive to commercial considerations than the Commerce Department.

Definitions important and specific to the ITAR include:

- A "defense item" is defined by the AECA at 22 U.S.C. 2778(j)(1)(4)(a) as follows: "The term "defense items" means defense articles, defense services and related technical data.

- A "defense article" is defined as any item or technical data on the United States Munitions List ("USML"). Pursuant to the AECA at 11 U.S.C. 2794(s), defense articles include: (A) any weapon, weapon system, munition, aircraft, vessel, boat or other implement of war, (B) any property, installation, commodity, material, equipment, supply or goods used for the purpose of making military sales, (C) any machinery, facility, tool, material, supply, or other item necessary for the manufacture, production, processing, repair, servicing, storage, construction, transportation, operation, or use of any article listed in this paragraph, (D) any component or part of any article listed in this paragraph, but does not include merchant vessels,…source material,… byproduct material, special nuclear material, production facilities, utilization facilities, or atomic weapons or articles involving Restricted Data.

- A "defense service," is defined as "(1) The furnishing of assistance (including training) to foreign persons, 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." (2) The furnishing to foreign persons of any technical data controlled under the ITAR. (3) Military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice, not defined as "assistance."

- Technical Data means "(1) Information, other than software 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. (2) Classified information relating to defense articles and defense services; (3) Information covered by an invention secrecy order; (4) Software directly related to defense articles; (5) 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 as defined in the ITAR. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles.

2.1.1 U.S. Munitions List (USML)

The U.S. Munitions List ("USML") is enumerated in 22 CFR Part 121 and specifies twenty-one (21) "Categories" of defense articles, with sub-itemization of "Significant Military Equipment" (SME) articles. SME is defined in 22 CFR § 120.7 as "articles for which special export controls are warranted because of their capacity for substantial military use or capability. An electronic version of the USML is available on the Department of State website at: http://www.pmddtc.state.gov/regulations_laws/documents/official_itar/2013/ITAR_Part_121.pdf

The twenty-one categories found on the USML are as follows:

This section intentionally blank

Category I: Firearms, Close Assault Weapons and Combat Shotguns

Category II: Guns and Armament

Category III: Ammunition / Ordinance

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: Protective Personnel Equipment and Shelters

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 Systems and Associated Equipment

Category XVI: Nuclear Weapons, Design and Testing Related Items

Category XVII: Classified Articles, Technical Data and Defense Services Not Otherwise Enumerated

Category XVIII: Direct 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

2.1.2 Commodity Jurisdiction

The process of determining if an item, article, service or technical data is on the USML and subject to the requirements of the ITAR is known as the "Commodity Jurisdiction" ("CJ") process. CJ is used by the U.S. Government if doubt exists as to whether an article or service is covered by the USML or some other regulations, such as the Commerce Control List ("CCL"). Designations of defense articles and defense services are made by the Department of State with the concurrence of the Department of Defense.

Proper CJ determination is absolutely essential to avoid violations because export compliance relies upon knowing which regulatory regime governs a particular export or activity (e.g. EAR or ITAR). The ITAR only regulates items, defense articles, services and associated technical data of items specifically identified on the USML as opposed to other U.S. export regulations.

The order of review for CJ is to self-classify items, articles or services to determine if they are subject to the ITAR by being listed on the USML, or if they meet the qualifications of being considered "specially designed." "Specially designed" is used to determine if an item or service meets the criteria of a defense article or defense service, or provides the equivalent performance capabilities of a defense article on the USML. If an article is not on the USML, or if it is not "specially designed" then it may be on the CCL, or subject to a different regulatory regime. The DDTC has a web-based interactive "Order of Review Decision Tool" to assist with this process: http://www.pmddtc.state.gov/licensing/dt_OrderofReview.htm

CJ is used to determine if an item or service meets the criteria of a defense article or defense service, or provides the equivalent performance capabilities of a defense article on the USML. The effort to determine whether an activity or item is subject to the ITAR, i.e., on the USML, is known as a "Jurisdictional Analysis", while the review for the EAR is known as "Commodity Classification." Conducting either of these analyses independent of government guidance is known as "self-classification".

The Jurisdictional Analysis process begins by reviewing the general characteristics of the item, technology or proposed defense service. The general characteristics must fall within the proscribed requirements of "specially designed" to be subject to the ITAR. Commodities and software are "specially designed" if:

This section intentionally blank

(1) As a result of development, has properties peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions described in the relevant U.S. Munitions List paragraph; or

(2) Is a part (see § 121.8(d) of this subchapter), component (see § 121.8(b) of this subchapter), accessory (see § 121.8(c) of this subchapter), attachment (see § 121.8(c) of this subchapter), or software for use in or with a defense article.

(b) A part, component, accessory, attachment, or software is not controlled by a U.S. Munitions List "catch-all" or technical data control paragraph if it:

(1) Is subject to the EAR pursuant to a commodity jurisdiction determination;

(2) Is, regardless of form or fit, a fastener (e.g., screws, bolts, nuts, nut plates, studs, inserts, clips, rivets, pins), washer, spacer, insulator, grommet, bushing, spring, wire, or solder;

(3) Has the same function, performance capabilities, and the same or "equivalent" form and fit as a commodity or software used in or with a commodity that:

(i) Is or was in production (i.e., not in development); and

(ii) Is not enumerated on the U.S. Munitions List;

(4) Was or is being developed with knowledge that it is or would be for use in or with both defense articles enumerated on the U.S. Munitions List and also commodities not on the U.S. Munitions List; or

(5) Was or is being developed as a general purpose commodity or software

If the technology meets the definitional requirements of qualifying as "specially designed" and is identified within a USML Category, the characteristics and functions of an article can be matched to a specific entry found on the USML.

DDTC has a web-based interactive "Specially Designed" decision tool to assist with this process: http://www.pmddtc.state.gov/licensing/dt_SpeciallyDesigned.htm

Both the Departments of Commerce and State prefer for organizations to attempt to self-classify whenever possible; however, if a concluded jurisdictional determination cannot be made through either the Commodity Classification or Jurisdictional Analysis process, the U.S. Government will provide a definitive written determination in response to the submission of a "Commodity Jurisdiction Request." Necessary forms and processes are available at the DDTC website: http://www.pmddtc.state.gov/commodity_jurisdiction/index.html

2.1.3 Definition of Export Under the ITAR

The ITAR defines the term "export" broadly. The term applies not only to exports of tangible items from the U.S., but also to transfers of intangibles, such as technology or information. The ITAR

defines as an "export" the passing of information or technology to foreign nationals even in the United States. The following are examples of exports:

1. **Exports of articles from the U.S. territory**
   - Shipping or taking a defense article out of the United States.
   - Transferring title or ownership of a defense article to a foreign person, in or outside the United States.

2. **Extra-territorial transfers**
   - The re-export or re-transfer of defense articles from one foreign person to another, not previously authorized (i.e., transferring an article that has been exported to a foreign country from that country to a third country).
   - Transferring the registration, control, or ownership to a foreign person of any aircraft, vessel, or satellite covered by the USML, whether the transfer occurs in the United States or abroad.

3. **Export of intangibles**
   - Disclosing technical data to a foreign person, whether in the United States or abroad, through oral, visual, or other means.
   - Performing a defense service for a foreign person, whether in the United States or abroad.

2.1.4 Requirements for ITAR Export Authorization

Any person or entity who engages in the U.S. in the business of manufacturing or exporting or temporarily importing defense articles or furnishing defense services is required to register with the Department of State. Registration is a mandatory prerequisite to process license applications or invoke other approvals for an activity regulated by the ITAR, or invoke the use of an exemption to the license requirement. Once registered, licenses to export defense articles or perform defense services can be processed, including permanent and temporary export and import licenses and technical assistance agreements for complex programs for the provision of defense services. Certain licenses or exemptions or other government approvals are required to employ or allow foreign nationals to participate in activities subject to export requirements (see "deemed exports"). License applications or the invocation of other government approvals and exemptions contain additional certifications / transmittal letters, supporting documentation, and in some cases, non-transfer and use certification from the licensee and / or the foreign government of the licensee.

University research is subject to the ITAR when the research involves defense articles or technical data. Activities that involve defense articles or export-controlled technical data that involve foreign persons require a license or other government approval before the foreign person is permitted access to the articles or data. Instruction or methods involved in the ITAR-controlled research constitute the provisioning of "defense services", which is also a licensable activity. A "defense service" is equivalent to a "deemed export" under the EAR.

2.1.5 Proscribed Countries

Pursuant to U.S. policy related to arms embargoes, no ITAR exports, including license requests, exemptions and other government approvals for export may be made to countries proscribed in 22 C.F.R. § 126.1, such as China, Cuba, Iran, North Korea, Sudan, and Syria. Additional restrictions apply to other countries; a complete list of U.S. arms embargoes is available online at: http://www.pmddtc.state.gov/embargoed_countries/index.html

2.2 EXPORT ADMINISTRATION REGULATIONS

The U.S. Department of Commerce's ("DoC") Bureau of Industry and Security ("BIS") regulates all dual-use technologies, materials, items, software, and technology not administered by another agency under the authority of the Export Administration Act of 1969 ("EAA") as enumerated in the Export Administration Regulations (EAR). The export control provisions of the EAR are intended to serve the national security, foreign policy, nonproliferation and short supply interests of the US, and in some cases, to carry out its international obligations. "Dual-use" items, products, technologies, and software that have both military, or civilian and commercial applications, but were not "specially designed" for military applications are identified on the Commerce Control List ("CCL"). Certain technologies identified on the CCL may parallel those enumerated on the USML; however, the key distinguishing factor is the military application of the items.

All items of U.S.-origin, wherever located, are subject to the EAR. Foreign manufactured goods are generally exempt from the EAR re-export requirements if they contain less than a de minimis level of U.S. content by value. Such de minimis levels are set in the regulations relative to the ultimate destination of the export or re-export.

The EAR requires a license for the exportation of a wide range of items with potential "dual" commercial and military use, or otherwise of strategic value to the United States (but not made to military specifications). However, only items listed on the Commerce Control List ("CCL") require a license prior to exportation. Items not listed on the CCL are designated as EAR99 items and generally can be exported without a license, unless the export is to an embargoed country, or to a prohibited person or end-use.

2.2.1 Commerce Control List (CCL)

The EAR specifically enumerates controlled technologies on the CCL, including technical thresholds and performance parameters that distinguish various levels of controls. The CCL is divided into ten broad categories, which is further subdivided into five product groups. This scheme is the framework for a matrix-based system utilized within the EAR to categorize control, licensing and exception requirements. Every commodity on the CCL is categorized according to a "Export Control Classification Number" ("ECCN"), which is an numeric-alpha code that describes the item and indicates licensing requirements. All ECCNs are listed within the CCL.

The following are the primary ten broad categories:

Category 0:	Nuclear Materials, Facilities and Equipment & Miscellaneous
Category 1:	Materials, Chemicals, Microorganisms and Toxins
Category 2:	Material Processing
Category 3:	Electronics
Category 4:	Computers
Category 5:	Telecommunications and 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 following are the five product groups controlled under the EAR:

- **Commodities, Equipment, Assemblies and Components.** Finished or unfinished goods ranging from high-end microprocessors to airplanes, to ball bearings.

- **Test, Inspection, Production and Manufacturing Equipment**. This includes equipment specifically for manufacturing or testing controlled commodities, as well as certain generic machines, such as computer numerically controlled ("CNC") manufacturing and test equipment.

- **Materials**. This includes certain alloys and chemical compounds.

- **Software**. This includes software specifically associated with particular commodities or manufacturing equipment, as well as any software containing encryption and the applicable source code.

- **Technology**. Specific information necessary for the "development", "production", or "use" of a product. The information takes the form of "technical data" or "technical assistance".. Unlike the ITAR, there is generally no distinction between the two. However, the EAR may apply different standards to technology for "use" of a product than for the technology for the "design" or "manufacture" of the product.

2.2.2 Commodity Classification

As previously reviewed, the State Department's CJ process is the primary means to determine which regulatory requirements are subject to an export activity. The State Department has jurisdiction to decide whether an item is ITAR- or EAR-controlled. DDTC encourages exporters to self-classify the product. If doubt exists, a CJ request may be submitted to DDTC to determine whether an item

is ITAR- or EAR- controlled. Proper CJ determination is absolutely essential to avoid violations because export compliance relies upon knowing which regulatory regime governs the technology..

Once it is determined that an item is EAR-controlled, the exporter must determine its Export Control Classification Number ("ECCN"). The first digit identifies the general category within which the entry falls (e.g., 3A001). The letter immediately following this first digit identifies under which of the five groups the item is listed (e.g., 3 A001). The second digit differentiates individual entries by identifying the type of controls associated with the items contained in the entry (e.g., 3A001). Listed below are the Reasons for Control associated with this second digit.
Once the ECCN is determined all associated regulatory control requirements can be looked up using the Reasons for Control and Commerce Country Chart.

Reasons for Control

AT	Anti-Terrorism
CB	Chemical & Biological Weapons
CC	Crime Control
CW	Chemical Weapons Convention
EI	Encryption Items
FC	Firearms Convention
MT	Missile Technology
NS	National Security
NP	Nuclear Nonproliferation
RS	Regional Stability
SS	Short Supply
UN	United Nations Embargo
SI	Significant Items
SL	Surreptitious Listening

The reason for controls identified on the ECCN are cross indexed to the "Commerce Country Chart" found in Supplement No. 1 to Part 738. The chart is available at:
http://www.bis.doc.gov/index.php/forms-documents/doc_download/14-commerce-country-chart

The "Country Chart" header identifies, for each applicable Reason for Control, a column name and number (e.g., CB Column 1). These column identifiers are used to direct you from the CCL to the appropriate column identifying the countries requiring a license. A license or other export authorization is required if the Chart and Reason for Control are marked with an X.

2.2.3 Requirements for EAR Export Authorization

Once determined that a license is required, an exporter can apply for export authorization from BIS. The EAR contains a number of exceptions. Determining whether a particular exception applies requires review of the specific application as detailed in 15 C.F.R. § 740, as well as review of the

notes on applicable license exceptions following the ECCN entry on the CCL. These exceptions include:

EAR License Exceptions	
LVS	Items of limited value (value is set under each ECCN).
GBS	Items controlled for national security reasons to Group B countries.
CIV	Items controlled for national security reasons to particular countries where end-user is civilian.
TSR	Certain technology and software to certain countries.
APP	Computer exports to certain countries.
TMP	Certain temporary exports, re-exports, or imports, including items moving through the U.S. in transit.
RPL	Certain repair and replacement parts for items already exported.
GOV	Exports to certain government entities.
GFT	Certain gifts and humanitarian donations.
TSU	Certain mass-market technology and software.
BAG	Baggage exception.
AVS	Aircraft and vessels stopping in the U.S. and most exports of spare parts associated with aircraft and vessels.
APR	Allows re-export from certain countries.
ENC	Certain encryption devices and software.
AGR	Agricultural commodities.
CCD	Consumer communication devices
STA	Strategic Trade Authorization

2.2.4 Definition of Export under the EAR

The definition of export under the EAR is very broad, just as in the ITAR, and covers a broad range of products and activities. Definitions that are important and specific to the EAR include:

- **Export.** "Export" means an actual shipment or transmission of items subject to the EAR out of the United States, or release of technology or software subject to the EAR to a foreign national in the United States.

- **Export of Technology or Software ("Deemed Export").** (i) Any release of technology or software subject to the EAR in a foreign country; or (ii) Any release of technology or source code subject to the EAR to a foreign national. Such release is deemed to be an export to the home country or countries of the foreign national. Deemed exports may occur through such

means as a demonstration, oral briefing, or plant visit, as well as the electronic transmission of non-public data that will be received abroad.

- **Release of Technology or Software:** 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 United States or abroad; or (iii) The application to situations abroad of personal knowledge or technical experience acquired in the United States.

- **Re-export.** "Re-export" means an actual shipment or transmission of items subject to the EAR from one foreign country to another foreign country; or release of technology or software subject to the EAR to a foreign national outside the United States, i.e., the shipment or transfer to a third country of goods or technology originally exported from the United States.

- **Re-export of Technology or Software (Deemed Re-export)**. Any release of technology or source code subject to the EAR to a foreign national of another country is a deemed re-export to the home country or countries of the foreign national. Re-export includes the export or re-export of items subject to the EAR that will transit through a country or countries or be transshipped in a country or countries to a new country or are intended for re-export to the new country, are deemed to be exports to the new country.

The release of technology or software source code to a foreign national in the United States is regulated, as is visual inspection by foreign nationals at U.S. facilities. This concept, as defined above, is considered a "Deemed export." The Deemed export relies upon the transmission in the US of technology as follows:

- **Technology**. Specific information necessary for the "development", "production", or "use" of a product. The information takes the form of "technical data" or "technical assistance". Unlike the ITAR, there is generally no distinction between the two. However, the EAR may apply different standards to technology for "use" of a product than for the technology for the "design" or "manufacture" of the product.

- **Required Information for the Development, Production, or Use of Items on the CCL:**
    - **Required.** As applied to "technology" or "software", refers to only that portion of "technology" or "software" which is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions. Such "required" "technology" or "software" may be shared by different products.

    - **Development.** "Development" is related to all stages prior to serial production, such as: design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, layouts.

    - **Production.** Means all production stages, such as: product engineering, manufacture, integration, assembly (mounting), inspection, testing, quality assurance.

- **Use.** Operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing**.**

- **Technical Assistance.** Technical assistance—May take forms such as instruction, skills training, working knowledge, consulting services. "Technical assistance" may involve transfer of "technical data".

- **Technical Data.** May take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memory.

2.3 Foreign Assets Control Regulations (FACR)

In addition to ITAR and EAR export restrictions, The Office of Foreign Assets Control ("OFAC") in the Treasury Department administers and enforces economic and trade sanctions against targeted:

Foreign governments (e.g. Iran, Sudan, Cuba)

Individuals (e.g. terrorists, narcotics traffickers)

Entities (e.g. drug front companies, charities linked to terrorist groups)

Practices (e.g. trade in rough diamonds, proliferation of WMDs)

There are three types of sanctions programs:

Comprehensive Sanctions

- Counter Narcotics Trafficking
- Non-proliferation (WMD)
- Anti-terrorism
- Sudan
- Cuba
- Iran

Regime-Based Programs

- Former Liberian Regime of Charles Taylor
- Democratic Republic of the Congo
- Zimbabwe
- Cot D'Ivoire
- Balkans
- Belarus

Limited Program

- Burma (Myanmar)
- Diamond Trading
- North Korea
- Syria

Numerous publications and legislation encompass the spectrum of sanctions, embargoes, and financial regulations. Sanctions typically regulate:

- Transactions involving designated foreign countries or their nationals;

- Transactions with respect to securities registered or inscribed in the name of a designated national;

- Importation of and dealings in certain merchandise; and
- Holding certain types of blocked property in interest-bearing accounts.
- Transactions with specific entities or individuals known as "specially designated nationals," found in the Specially Designated Nationals List ("SDNL").

In many cases a general or specific license from OFAC is required in order to travel to sanctioned countries, or have transactions with sanctioned countries, entities, or individuals. University personnel will not engage in international collaborations with sanctioned countries, entities, or individuals without first consulting with ORC to determine if an OFAC license is required.

2.4 Anti-boycott Restrictions

U.S. Anti-boycott policies proscribe certain actions regarding the Arab League's boycott of Israel and require reporting to the Department of Commerce or the Internal Revenue Service for certain boycott related communications or identification of participation in an international boycott. U.S. anti-boycott laws require US firms and persons to refuse to participate in foreign boycotts that the U.S. government does not sanction. Any interaction, contracts, or agreements with foreign companies, entities and Governmental agencies of identified participating boycott countries may require scrutiny to ensure there are no reportable boycott issues.

Prohibited conduct includes:

- Agreements to refuse or actual refusal to do business with or in Israel or with blacklisted companies.
- Agreements to discriminate or actual discrimination against other persons based on race, religion, sex, national origin or nationality.
- Agreements to furnish or actual furnishing of information about business relationships with or in Israel or with blacklisted companies.
- Agreements to furnish or actual furnishing of information about the race, religion, sex, or national origin of another person.
- Implementing letters of credit containing prohibited boycott terms or conditions.

Arab League Members

Algeria
Bahrain
Djibouti
Egypt
Iraq
Jordan
Kuwait
Lebanon
Libya
Mauritania
Morocco
Oman
Qatar
Saudi Arabia
Sudan
Syria
Tunisia
United Arab Emirates
Yemen

Examples Include:

- **Prohibited Boycott Condition in a Purchase Order:** "In the case of overseas suppliers, this order is placed subject to the suppliers being not on the Israel boycott list published by the central Arab League."
- **Reportable boycott condition in an importer's purchase order:** "Goods of Israeli origin not acceptable."

- **Prohibited Condition in a Contract**
  "The Contractor shall comply in all respects with the requirements of the laws of the State of Bahrain relating to the boycott of Israel. Goods manufactured by companies blacklisted by the Arab Boycott of Israel Office may not be imported into the State of Bahrain and must not be supplied against this Contract."

- **Prohibited Boycott Condition in a Questionnaire**
  "1. Do you have or ever have had a branch or main company, factory or assembly plant in Israel or have sold to an Israeli?"
  "2. Do you have or ever have had general agencies or offices in Israel for your Middle Eastern or international operations?"

- **Prohibited Condition in a Trademark Application**
  "Requirement for the registration of pharmaceutical companies: Certification letter regarding the boycott of Israel (i.e., do not comprise any parts, raw materials, labor or capital of Israeli origin)."

2.5 PENALTIES FOR EXPORT VIOLATIONS

Penalties for export violations can apply to individuals and the university.

International Traffic in-Arms Regulations (ITAR)

- Maximum $1,000,000 per violation or imprisonment of up to twenty years, or both pursuant to 22 U.S.C. 2778(c)

Export Administration Regulations (EAR)

- Criminal: Maximum $1,000,000 per violation or imprisonment of up to twenty years, or both
- Administrative: Maximum $11,000 per violation or $120,000 per violation for items involving national security

- Pursuant to the International Emergency Economic Powers (IEEPA) Enhancement Act:
  - Criminal: Maximum $100,000 per violation or imprisonment of up to twenty years, or both
  - Administrative: Maximum of greater of $250,000 per violation or twice the amount of the transaction

Office of Foreign Assets Control (OFAC)
Pursuant to the Trading with the Enemy Act (TEWA) of 1917, 50 USCS Sec 5

- Criminal (Willful Violation): Maximum $1,000,000 per violation, and up to $100,000 in individual fines, per violation or imprisonment of up to ten years, or both
- Criminal (Knowing Violation): Maximum $100,000 or up to ten years in prison, or both, per violation

- Civil: Maximum of $65,000 per violation

Pursuant to the International Emergency Economic Powers (IEEPA) Act, 20 USCS Sec 1701

- Criminal: Maximum $1,000,000 per violation or imprisonment of up to twenty years, or both
- Civil: Maximum $250,000 per violation, or twice the amount of the transaction

Administrative Penalties

- **Warning Letter:** are administrative determinations that a violation has occurred, but that a "good faith effort" (mitigating factor) to comply with the law and to cooperate with an investigation has been shown with no aggravating factors.

- **Denial Order / Interim Suspension:** deny the sanctioned party any U.S. export privileges and any access to U.S.-origin goods and technology, from any source, for a specified period of time or indefinitely and may be narrow in scope, such as a restriction on the export of specific items or to specific destinations.

- **Seizure & Forfeiture:** Commodities or technical data which have been, are being, or are intended to be exported or shipped from or taken out of the U.S. in violation of the Export Administration Act (EAA) or International Traffic in Arms Regulations (ITAR) are subject to being seized and forfeited including, the vehicles carrying such commodities or technical data.

- **Debarment:** includes the exclusion from practice or the denial of export privileges, including the revocation of contracts, loss of funding, debarment from government contracts or implementation of additional compliance measures.

2.6 Voluntary Self-Disclosure of Suspected Violations

Because of the complexity of the ITAR, EAR and FACR, accidental or inadvertent violations of export control regulations are possible. In research, a university may presumably discover that a researcher or collaborator has violated the ITAR. DDTC, BIS and OFAC all have voluntary disclosure programs and procedures whereby a potential export violation may be self-disclosed. Specifically, Section 127.13 of the ITAR states that the DDTC:

> Strongly encourages the disclosure of information…by persons, firms or any organization that believes they may have violated any export control provision of the Arms Export Control Act, or any regulations, order, license, or other authorization issued under the authority of the Arms Export Control Act.

The cognizant export administration agency may consider a voluntary disclosure as a mitigating factor in determining whether to impose any penalties (including monetary penalties) or seek other enforcement action. A failure to submit a Voluntary Self-Disclosure ("VSD") may be considered as an aggravating factor, likely increasing the penalties levied upon an organization.

UCF will report all potential violations of the ITAR, EAR and FACR immediately upon discovery. A comprehensive report must be provided to the cognizant federal agency within 60 calendar days of the initial notification. A formal request for extension will be lodged with the appropriate agency if 60 days is insufficient. The procedure for detecting, investigating, reporting, and correcting suspected export violations are as follows:

The investigation of suspected export violations will be expedited. An investigation is a pre-requisite to properly evaluate whether to submit a voluntary self-disclosure. All investigations will be carried out by an Empowered Official and reported to upper management. An investigation will examine the full scope of any potential violations, to include:

- Potential violation, causes, important facts, aggravating or mitigating circumstances.

- Parties involved, dates, places, locations, methods, export jurisdictions, means by which the violation was detected, type of export violation (physical, visual, oral, electronic);

- Short term corrective actions / stops implemented upon violation discovery, including parties involved in the corrective actions.

Investigation will consist of three phases:

1. **Data preservation**
    a. Notify necessary parties of the investigation
    b. Require parties to preserve all materials related to the subject matter
    c. Categorize and review the types of information and documents relevant to the investigation
    d. Demand strict compliance with data preservation
    e. Inform parties of how information should be preserved
    f. Designate a Point of Contact

2. **Data collection and review**
    a. Document preservation and collection interviews
    b. Collection and review of paper and electronic data

3. **Interviews of relevant employees / participants**
    a. Following collection, review and organization of data, interviews with all relevant parties will be conducted.
    b. A formal memo and summary of all interviews will be prepared

Upon conclusion of data collection, interviews and evaluation, a formal report will be prepared. Facts developed during the course of the investigation are important for VSD purposes in addition to university decision-making. Contents of the report will include:

1. Description of the subject and scope of the investigation
2. Description of each phase of the investigation, including all efforts
3. A chronology of the facts developed via the investigation
4. A description of remedial measures undertaken

5. A description of proposed corrective/preventative actions

VSD's will be drafted pursuant to Section 127.12(c)(2) of the ITAR, as a baseline, which include:

(i) A precise description of the nature and extent of the violation (e.g., an unauthorized shipment, doing business with a party denied U.S. export privileges, etc.);

(ii) The exact circumstances surrounding the violation (a thorough explanation of why, when, where, and how the violation occurred);

(iii) The complete identities and addresses of all persons known or suspected to be involved in the activities giving rise to the violation (including mailing, shipping, and e-mail addresses; telephone and fax/facsimile numbers; and any other known identifying information);

(iv) Department of State license numbers, exemption citation, or description of any other authorization, if applicable;

(v) U.S. Munitions List category and subcategory, product description, quantity, and characteristics or technological capability of the hardware, technical data or defense service involved;

(vi) A description of corrective actions already undertaken that clearly identifies the new compliance initiatives implemented to address the causes of the violations set forth in the voluntary disclosure and any internal disciplinary action taken; and how these corrective actions are designed to deter those particular violations from occurring again;

(vii) The name and address of the person making the disclosure and a point of contact, if different, should further information be needed.

This section intentionally blank

3 ACTIVITIES NOT SUBJECT TO REGULATION

The EAR, ITAR and FACR only regulate certain transactions that involve controlled items, technology, defense articles or services. Articles or services not listed on the USML or CCL, or specifically excluded from the regulations are not subject to export controls, regardless of the context of university research or educational activities. Common to all regulations, although worded sufficiently different to make equivalent comparison impossible, are the concepts of general "publically available" and "public domain" information that is not subject to regulations, as follows:

- Information in the Public Domain or Publically Available, e.g. published information and software
- University Research that is neither classified, nor contains "technical data
- Marketing Information
- Educational information released in official catalogue courses and associated teaching labs of U.S. institutions of higher education
- Patent applications

A discussion of each of these generally excluded publicly available items follows.

3.1 PUBLIC DOMAIN (ITAR); PUBLICLY AVAILABLE (EAR)

- The EAR excludes publicly available technology if it is already published or will be published. Information is published when it becomes generally accessible to the interested public in any form, including:
    - publication in periodicals, books, print, etc., available for general distribution free or at cost;
    - readily available at libraries open to the public or university libraries;
    - patents and open patent applications available at any patent office; or
    - release at an open conference, meeting, seminar, trade show, or other gathering open to the public
- The ITAR does not regulate information in the "Public Domain" nor is such information subject to licensing requirements. The ITAR has a very narrow scope of what is included within "public domain":

(a) *Public domain* means information which is published and which 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 (see also § 125.4(b)(13) of this subchapter);

(8) 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 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 or 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.

3.2 Marketing Information (EAR and ITAR)

- The EAR (734.7) would include marketing information as qualifying for public release as being generally accessible and distributed to the interested public.

- The ITAR (120.10(5)) states that technical data "does not include basic marketing information on function or purpose or general system descriptions of defense articles."

3.3 Educational Information (EAR and ITAR)

Both the ITAR and the EAR address the issue of general educational information that is typically taught in schools and universities. Such information, even if it relates to items included on the USML or the CCL, does not fall under the application of export controls.

- The EAR (734.9) states that educational information is not subject to the EAR if it is "released by instruction in a catalogue course and associated teaching lab of academic institutions" (with the exception of certain encryption software and object code).

- The ITAR (120.10(5)) states that technical data "does not include information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities or information in the public domain…."

3.4 Patent Information (EAR and ITAR)

- The EAR (734.10) excludes "information contained in a patent application."

- The ITAR (120.11(5)) excludes "patents available at any patent office."

3.5 University Research

While some of UCF's projects involve applied research and may result in defense articles or technical data, UCF generally only undertakes projects that have the potential to make some contribution to the advancement of fundamental knowledge, primarily through publishable results. UCF operates under the presumption that its research activities constitute "Fundamental Research" (as defined below) and that the results of such research may be generally published freely or shared within the academic community, except to the extent that (i) UCF explicitly agrees to publication or access restrictions requested in advance by the research sponsor; or (ii) some aspect of a particular research project is otherwise inconsistent with Fundamental Research.

The EAR (734.8(a)) defines Fundamental Research to mean:

> [B]asic 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 are restricted for proprietary reasons or specific national security reasons as defined § 734.11(b) of [the EAR].

Section 734.8(b) of the EAR explicitly states that "[r]esearch conducted by scientists, engineers or students at a university normally will be considered fundamental research," provided that the university does not accept certain types of "prepublication review" requirements or "other restrictions on publication of scientific and technical information resulting from the research." Even where the university accepts prepublication review requirements or publication restrictions with respect to information provided by the sponsor (i.e., restrictions on "input" information from the sponsor), this section provides that the university still may treat information resulting from the research (i.e., the "output" information resulting from the university's research) as "Fundamental Research."

The ITAR, Section 120.11, provides an exclusion from export control restrictions for information and technology already in the public domain, including technology resulting from "Fundamental Research" at universities and other institutions of higher learning. Under Section 120.11 of the ITAR, Fundamental Research is defined to mean:

> [B]asic and applied 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 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 or 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.

Both the ITAR and the EAR provide that information published and generally accessible to the public through fundamental research is not subject to export controls. However, there are certain restrictions.

3.6 FUNDAMENTAL RESEARCH DISQUALIFIERS

- Information results must be produced as part of basic and applied research in science and engineering and must be broadly shared within the scientific community (i.e., no restrictions on publication / dissemination of the research results);

- Information generated from the research is separate and distinguishable from the conduct that occurs in performance of the research;
- Even when the results of research are not subject to export controls, government approval may be required if the performance of the research requires foreign national access to export controlled technology. This may take the form of:

    - Proprietary/restricted information released to a foreign national. Provided by a research sponsor, partner institution, or from a previous research project;

    - Operation or use of export-controlled equipment in a manner that exceeds the deemed export threshold

    - Mere access to a defense article.

- Performance location is limited to accredited U.S. institutions of higher learning in the United States. EAR allows fundamental research to occur at facilities other than accredited institutions of higher learning in the United States; however this typoe of research is considered "Corporate Research" and not fundamental research pursuant to 734.8(e).

- Research performed in the US at accredited institutions will not qualify as fundamental if the university (or the primary investigator) has accepted publication or other dissemination restrictions:

    - ITAR specifically identifies restrictions for proprietary reasons, or specific U.S. Government access and dissemination controls.

    - EAR specifies that fundamental research is 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. University-based research is not considered fundamental research if the university or its researchers accept restrictions (other than review to ensure no release of sponsor-provided proprietary or patent information) on publication of scientific and technical information resulting from the project.

    - National security controls include:

        - Prepublication review and approval by the Government, with right to withhold permission for publication;

        - Restriction on prepublication dissemination of information to non-U.S. citizens or other categories of persons;

        - Restrictions on participation of non-U.S. citizens or other categories of persons in the research

3.7 Areas of Research Impact

The availability of the Fundamental Research exemptions under the ITAR and the EAR has significant implications for universities and how they operate. Most importantly, the Fundamental Research exemptions enable universities to maintain open environments that encourage the free exchange of ideas, without having to segregate or discriminate among students and faculty on the basis of nationality or citizenship. Where the Fundamental Research exemptions are not available, universities are required to determine the export classification of the technology involved or resulting from their research activities and to comply with all applicable export licensing requirements. In instances where the research involves technologies that are controlled under the ITAR or the EAR, the "deemed export" provisions of these regulations would require universities to establish access controls to ensure that foreign national students, faculty members and visitors do not participate in or have access to the controlled research. Transfers or release of export controlled information in the university research environment may occur as a result of:

- Allowing virtual or physical access
- A demonstration, briefing or presentation
- A conversation (in-person or telephone)
- Laboratory or plant visit

- Film crew
- Faxes or letters
- Hand-carry of documents, hardware or drawings
- Design reviews
- Posting non-public data on the internet
- The exchange of electronic data or communication
- Surreptitious attempts, such as unsolicited inquiries
- Carrying a laptop or other electronic device with controlled technical information or software out of the country
- Collaborating with other universities or foreign collaborators

Because the acceptance of publication or access restrictions generally would render a university's research activities ineligible for the Fundamental Research exemptions, universities engaged in sponsored research are very cautious to determine whether the sponsor seeks to impose access or restrictions on the research results. Application of "fundamental research" to university research activities must be consistent with the UCF Policy on Export Controls. Compliance reviews are conducted by the Office of Sponsored Programs and Office of Export Controls. The final determination of whether a program qualifies for the fundamental research exclusion can only be authorized by the Office of Export Controls. This is almost exclusively done in writing to comply with federal record requirements.

It is the UCF position that "fundamental research" constitutes only the information resulting from research and not any informational inputs provided to the research or conduct performed during research. As such, the UCF approach for fundamental research is to separate out activities pursuant to Input, Conduct and Output.

3.8 Proprietary or Restricted Information Provided by Research Sponsors

The EAR and the ITAR provide that information received from government or corporate sponsors (i.e., "input" information) remains subject to the export control regulations when it is identified as proprietary or otherwise subject to access or publication restrictions. Information received from DoD that is designated as "For Official Use Only," "Sensitive But Unclassified" or otherwise restricted constitutes export controlled information and may not be released to foreign nationals, except as authorized under the ITAR or the EAR. Similarly, proprietary technical data and software applications received from corporate research sponsors or partners also would be subject to export controls.

The receipt of such controlled information, however, would not necessarily eliminate the availability of the Fundamental Research exemptions for the University's research results (i.e., "output" information). Where the university is able to conduct the research and publish the research results without disclosing the restricted input data to unauthorized persons, the research activities and results generally remain exempt from export controls under the Fundamental Research exemptions. In contrast, where it is not possible to publish research results without disclosing restricted input data or software, such research results would be subject to applicable export controls.

3.9 Exports of Controlled Hardware, Software and Related Technical Data

The Fundamental Research exemptions under the ITAR and EAR apply only to the information and technology developed through the research (i.e., "output" information). Hardware and software items produced in the course of research still may be subject to export controls when physically exported from the United States. Certain technical data relating to the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of such controlled applications also may be subject to export controls. (At the same time, "basic marketing information" or "general system descriptions" relating to the function or purpose of defense articles are exempt from controls pursuant to the Section 120.10 of the ITAR, unless specific contractual provisions state otherwise.)

In this regard, certain technologies may initially be researched for academic or commercial applications and regularly draw upon pre-contractual, UCF-developed technologies and software tools. These underlying technologies and software tools have broad research-related and commercial applications, and UCF regularly publishes its research findings in these areas. Where such underlying technologies and software tools are used or incorporated into a particular military application that is deemed to be ITAR-controlled, such usage should not subject those underlying technologies and software tools to the same ITAR controls. Thus, while UCF recognizes that it would need to restrict access to a specific military application in some cases (including the application itself and any application-specific source code and related technology), it would continue to treat its research relating to the underlying technology and software tools as Fundamental Research where appropriate.

UCF will, where appropriate, restrict access to specific military applications. Presentations, publications, facility tours and other types of disclosures do not include or otherwise result in the release of ITAR-controlled technical data.

3.10 DoD Research & Development Funding Accounts

Research funds received from Department of Defense ("DoD") agencies generally originate from one of seven accounts specified within the DoD's research and development budget for funding particular types of activities, as follows:

6.1	"Basic Research"
6.2	"Applied Research"
6.3	"Advanced Technology Development"
6.4	"Advanced Component Development and Prototypes"
6.5	"System Development and Demonstration"
6.6	"Management and Support"
6.7	"Operational Systems and Development"

While the account used to fund a particular research program may be indicative of the purpose and objectives of the research, the allocation of funding is an internal agency matter and the originating account is not necessarily determinative of the eligibility of the research for the Fundamental Research exemptions under the ITAR and the EAR. The decision as to whether the research would be subject to export controls is more properly based on the particular subject matter and research activities to be performed. UCF would expect any restrictions applicable to the research program or the research results to be identified in the contract documents.

3.11 DEFENSE SERVICES

Finally, the Fundamental Research exemptions generally apply only to basic and applied research conducted in the United States. Pursuant to the ITAR's restrictions on "defense services," research involving the provision of military or defense-related technical assistance (i.e., "conduct") to foreign persons may require authorization under the ITAR, even where there are no contractual access or publication restrictions applicable to the research. Accordingly, UCF will apply for and obtain ITAR approvals for mere access to defense articles or technical data for foreign persons.

This section intentionally blank

4 MANAGEMENT CONTROL STRUCTURE & POLICY

4.1 Institutional Commitment

As a leading academic institution on the forefront of technological development and academic research, the University of Central Florida will strive to educate and conduct research in harmony with the export control laws, regulations, and sanctions of the United States. A preponderance of activities taking place at UCF are educational in nature, consisting of basic and applied research, the fruits of which are intended for learning and open distribution among scientific and technical communities. While the University recognizes that education is based primarily on the free and open exchange of information and ideas, it consciously chooses to accept research and conduct activities subject to proprietary or national security restriction that nullify free and open exchange and subject such efforts to limitations on access and distribution. To fulfill its commitment, the University has established the Office of Export Compliance to collaborate with various academic departments and research units engaging in activities subject to export controls to:

- Support UCF's commitment to comply with U.S. export control policies, laws, regulations, and sanctions;
- Provide direction and solutions to researchers, faculty, staff, and employees in complying with export controls;
- Prevent inadvertent transfers of export controlled technologies;
- Educate, train, and foster compliance.

Most research and activities conducted on-campus are excluded from U.S. export control laws, including the Export Administration Regulations (EAR), the International Traffic in Arms Regulations (ITAR), and U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC) sanction regulations. However, certain research involving specified technologies controlled under the EAR or the ITAR, or transactions and exchanges with designated countries or sanctioned entities may require that the University of Central Florida obtain an export license or other government approval prior to providing controlled technologies to certain foreign national employees, professors, students, researchers or other foreign national collaborators. However, information generated during the course of "Fundamental Research", as defined under such laws, is exempt from export licensing requirements.

The University will 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. To this end, the University will ensure that, unless unavoidable, information generated during the performance of any university research, including sponsored contract activities, qualifies for the Fundamental Research provisions of applicable export control laws. The civil and criminal penalties associated with violating export control regulations can be severe, ranging from administrative sanctions including loss of research funding to monetary penalties to imprisonment for individuals.

The University 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: http://www.research.ucf.edu/ExportControl/ that contains university export control policies, forms, training modules and reference materials.

4.2 Export Control Policy

The University of Central Florida initially implemented export control guidelines on January 17, 2006. These guidelines were applied to all university operations when the University formally applied for registration with the DDTC on April 19, 2010. The guidelines were revised by the University Office of Compliance and Ethics on August 19, 2011. On September 17, 2014 the University policy Review committee approved revisions and implementation of the guideline under UCF Policy 4-209 "Export Control." The policy establishes roles, responsibilities, standards of conduct and procedures, including the creation of this Export Control Management Plan ("ECMP"). A copy of the current guideline and policy is included in the Appendix of this ECMP, and is available on the export compliance website at: http://www.research.ucf.edu/ExportControl/

4.3 Empowered Officials

The Provost and Executive Vice President designated the following university officers as empowered officials pursuant to 22 CFR 120.25:

- Dr. Thomas O'Neal, Associate Vice President for Research and Commercialization
- Douglas Backman, Director of Research Compliance, Office of Research and Commercialization
- Michael Miller, Assistant Director, Office of Research Compliance (Export Control Officer)

In this capacity, designated Empowered Officials:

This section intentionally blank

(1) Are directly employed by UCF in a position having authority for policy or management; and

(2) Are legally empowered in writing by the applicant to sign license applications or other requests for approval on behalf of UCF with the U.S. State Department; and

(3) Understand the provisions and requirements of the various export control statutes and regulations, and the criminal liability, civil liability and administrative penalties for violating the Arms Export Control Act and the International Traffic in Arms Regulations; and

(4) Have the independent authority to:

(i) Enquire into any aspect of a proposed export or temporary import by UCF, and

(ii) Verify the legality of the transaction and the accuracy of the information to be submitted; and

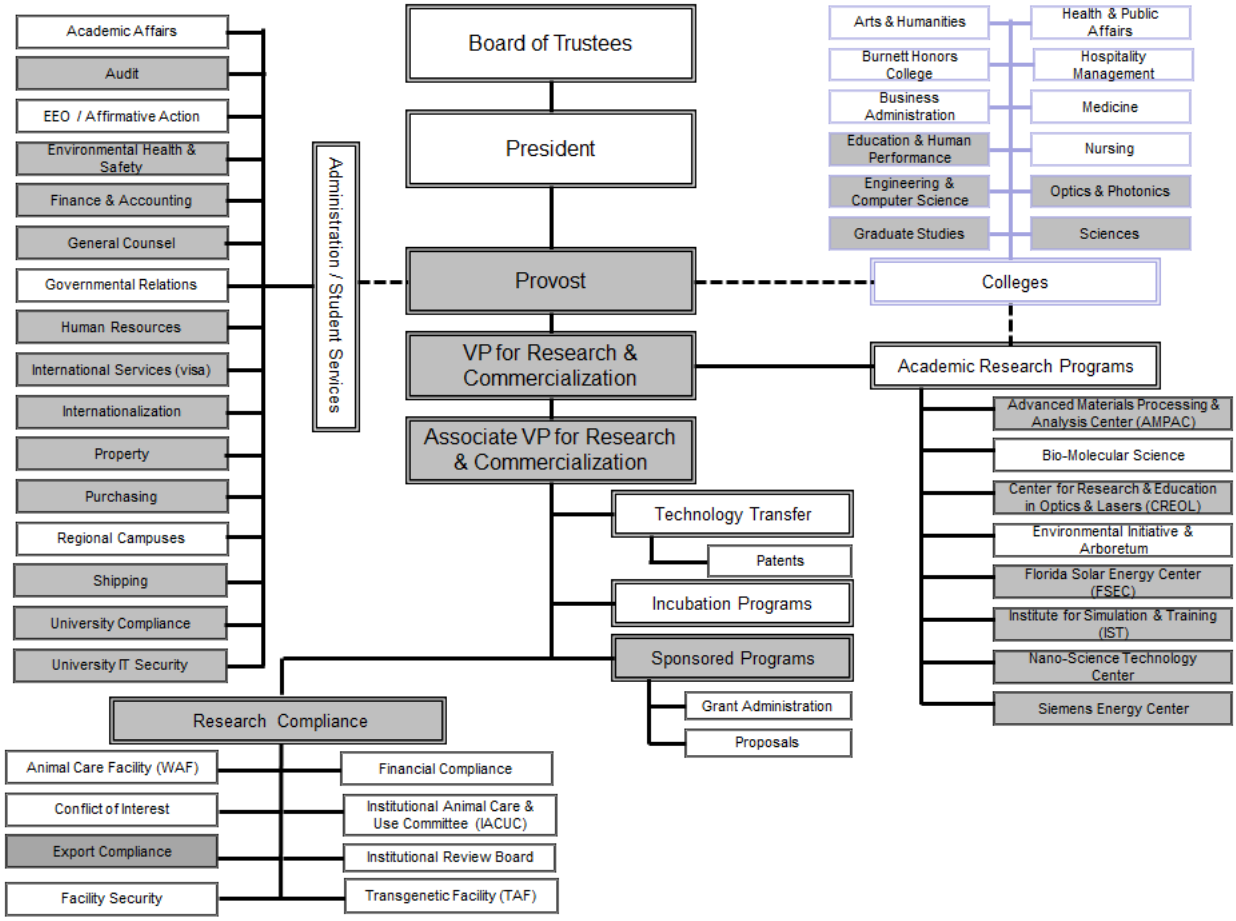
(iii) Refuse to sign any license application or other request for approval without prejudice or other adverse recourse.

4.4 Organization Structure

The UCF export control program is a distributed compliance program with certain critical functions spread across key departments and units located throughout the University. Many of these units are embedded within administrative functions located in central administration and the business offices of colleges. Overall, the "footprint" or reach of export compliance is university-wide and relies on the Office of Export Controls for coordination, information distribution, and management of the program.

This section intentionally blank

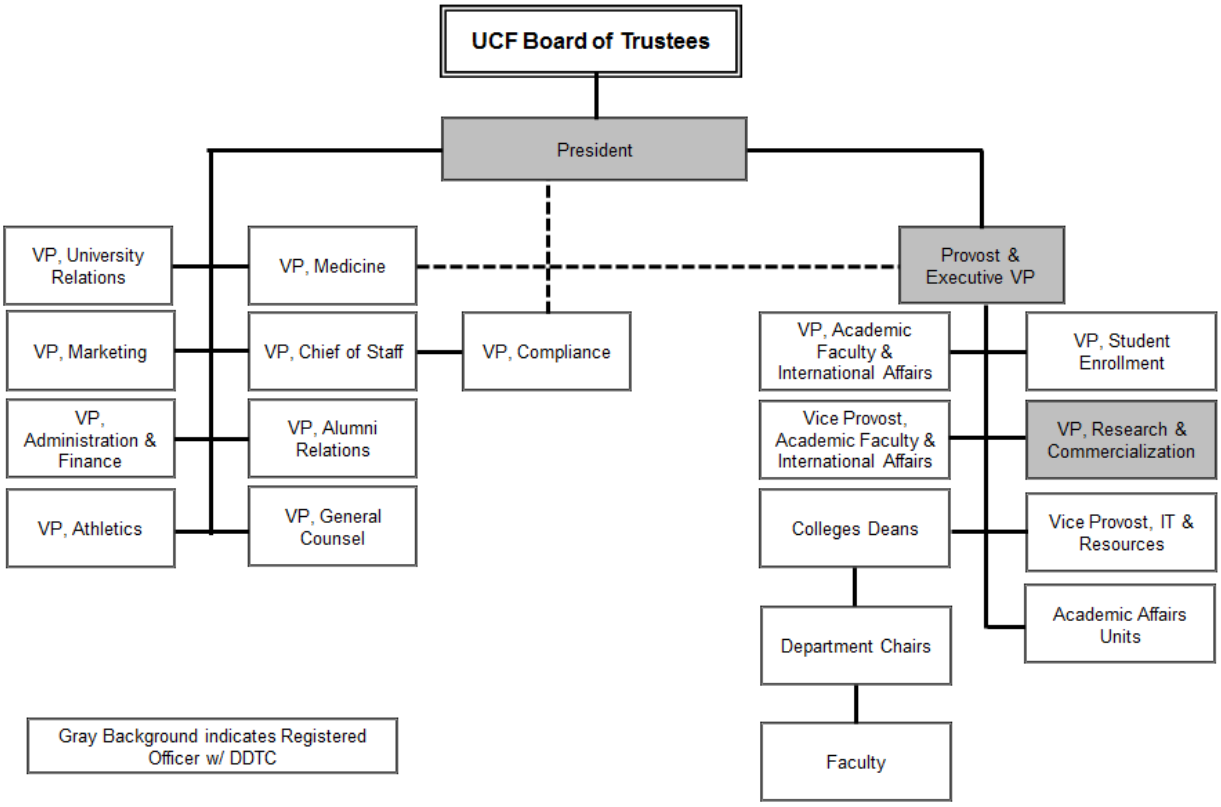
Export Control Footprint



***Note:** Shaded areas indicate the unit has an administrative, advisory or auxiliary role in the Export Control Compliance program. The role is explained in the next section.

This section intentionally blank

University Senior Management



Defense Trade Senior Management Information
As specified in the DS-2032, UCF has designated the following Senior Officers as primary administrators of the defense trade program:

Dr. John C. Hitt, President
Dr. Diane Z. Chase, Interim Provost and Vice President for Academic Affairs
Dr. Marion J. Soileau, Jr., Vice President of Research and Commercialization
Dr. Thomas P. O'Neal, Associate Vice President of Research and Commercialization

4.5 University Roles & Responsibilities for Export Control Compliance

4.5.1 Office of Export Controls

The functional administrative unit at the University of Central Florida charged with the responsibility for oversight of compliance and recordkeeping of all applicable exports and regulated transactions with sanctioned individuals, entities, and countries is the Office of Research and Commercialization, Office of Compliance, a unit under the Vice President for Research and Commercialization.

The Assistant Director of Export Controls is the principal point of contact for all export control and related activities throughout the university responsible for institutional-wide development, implementation, maintenance, management and improvement of the Office of Export Controls to ensure overall university compliance with export control laws and regulations related to international trade and technology transfer. The Assistant Director for Export Controls is the designated Empowered Official charged to oversee, administer, and coordinate all export compliance functions in concert with other departments and units as necessary, including:

- Direct the day-to-day operational, administrative, communication, database and record-keeping functions of the Office of Export Controls and all export control and related activities throughout the university, including all staff assigned to the Office.

- Manage the support functions the Office of Export Controls provides to other University departments and units, including: performing agreement reviews and analysis; conducting export assessments of international shipping, transfers and travel; prepare, review, approve and submit license applications for international exports and deemed-exports, and other requests for government agency export approval; determine the application of licensing exceptions or licensing requirements and exception/exemption certificates as applicable; and research, prepare, approve and submit advisory opinion requests or other government guidance requests.

- Lead, manage and approve the overall university approach to implementing institutional-wide export control policies, procedures and protocol by working directly with university administration, management and technical personnel. The export control standard operating procedures, policies and protocols will be enumerated in the University Export Compliance Management Plan (ECMP) to provide consistency and compliance for all departments and units involved in exports and travel matters, such as: screening end users, end use and countries for exported technology; subcontractors and visitors to controlled facilities; determining International travel requirements including those for embargoed and sanctioned countries.

- Provide subject matter expertise on University policy and procedures related to export controls. Areas of functional oversight for the Office of Export Controls include: Office of Research & Commercialization-specific and broader university-at-large.

- Perform advanced regulatory/legal research on issues related to export controls and work with functional and legal experts to represent university compliance.

- Develop and maintain the university security approach for controlling technology. Such measures include: Technology Control Plan (TCP)/ Sensitive But Unclassified plans, and other security protocols that document controls for: the secure handling, use, storage, and transmission of sensitive information; physical security controls for sensitive work and material storage areas; research activities subject to export control and activities with contractual security requirements. Provide institutional oversight of TCP implementation and monitor compliance with such plans.

- Maintain and update institutional registrations with necessary federal agencies.

- Develop and deliver export control education and awareness to the broad University community: Provide strategic consultation and guidance to faculty, staff and administration on decisions that have import/export regulatory impact. Provide training and guidance to staff in all export control-related matters. Conduct and manage initial and refresher export compliance education and awareness. Develop content and delivery methods; develop and conduct training programs on export control, including, ITAR, EAR, OFAC, DEAR, FAR, international travel and related issues, including embargoed and sanctioned countries.

- Identify project-specific sensitive material concerns. Collaborate with Principal Investigators and technical research staff to identify sensitive information and equipment. Using information from a variety of internal and external sources, determine commodity jurisdiction and self-classify equipment and technologies pursuant to ECCN or USML classifications and implement and maintain automated self-classification decision tools (Visual Compliance).

- Identify, implement and maintain an information management system for tracking and managing export controlled hardware, software, information and deliverables in accordance with Federal and State statutes and policies as well as University policies; Develop and implement automated tools for the screening of research project personnel and external recipients to determine federal export control status (Visual Compliance).

- Make immigration related export certifications and conduct technology alert investigations, as required by the U.S. Consulate. Review H-1B and other foreign national beneficiary information as it relates to deemed export and licensing needs. Work with other campus units as needed to acquire and review associated agreements and technology/data or software associated with foreign national activity at the University. Review and approve deemed export control attestations on behalf of the University. Manage federal background investigations, personnel security clearances and visit authorizations for employees, consultants, and cleared visitors.

- Liaison with federal regulatory and investigatory agencies (Commerce, State, Treasury, Energy, Defense, DSS, FBI) regarding export control matters to counteract illegal foreign intelligence gathering methods, identifying breaches/spillages, and providing intelligence for ongoing investigations. Assist federal agencies in the identification and neutralization of foreign interdiction of sensitive U.S. technology, articles, and data identified as export controlled and act as liaison and coordinator for export-related and travel matters between the various research and regulatory offices within UCF.

4.5.2 Designated Department and Units

There are four categories of departments and units with an export compliance role and responsibility:

- Research Administration: Administrative units and personnel specific to research functions, such as Sponsored Programs (Proposals, Contracts & Grants) and Technology Transfer.

- Central University Administration: Administrative units and departments that service the general university, such as General Counsel, Human Resources, Purchasing and International Student Services.

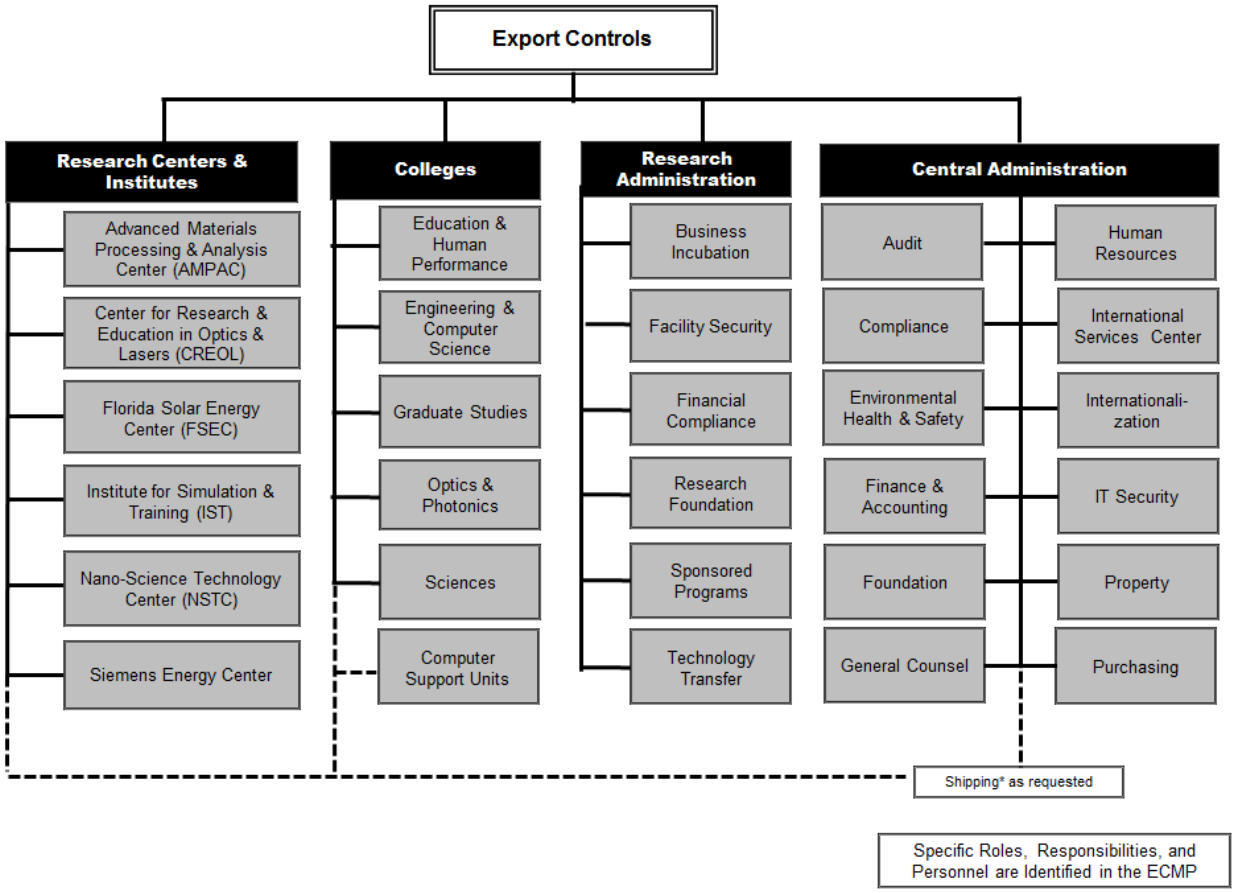
- College Administration: Technical college administration such as college deans and department chairs, faculty and associated administrative staff. Researchers are assigned to work within departments and units that report to college administration.

- Research Centers & Institutes Administration: Administration of high technology research centers that are embedded within colleges and employ department faculty and staff, such as the Siemens Energy Center and Advanced Materials Processing Center.

4.5.3 Organizational Structure of Designated Departments and Units

The organizational structure for the implementation of these policies is centered in the Office of Export Controls, and includes the following administrative, advisory, and auxiliary relationships

This section intentionally blank



4.6 Research Administration Units

4.6.1 *Office of the Vice President for Research & Commercialization*

The Vice President for Research and Commercialization and the Associate Vice President for Research and Commercialization are the university officials with final responsibility for compliance with export and sanction related regulations. The Vice President for Research assists the University President in maintaining continuing relationships with federal agencies.

4.6.2 *Business Incubation*

The Business Incubation program serves as an export control outreach conduit with local small businesses affiliated with the University. The University will provide guidance and instruction to local small businesses to ensure they are aware of U.S. export control laws and regulations. The Office of Export Compliance will provide information, guidance and training as requested to ensure small businesses affiliated with UCF are compliant. Facility Security

The Office of Export Controls collaborates with the Facility Security program to ensure there is a common approach to national security issues common to export controlled and classified programs. Suspicious contacts and other reportable events related to classified programs are forwarded to the Facility Security Officer for disposition. Exports of classified information or articles are coordinated with the Facility Security Officer pursuant to NISPOM requirements. Joint training seminars are coordinated as appropriate.

4.6.3 Financial Compliance

The Office of Financial Compliance performs Restricted Party Screening on research participants (graduate and undergraduate students, temporary workers, faculty, and other A&P personnel) who are paid from research programs. This does not include volunteers.

4.6.4 Research Foundation

The Research Foundation identifies and ensures trade sanction compliance involving international donations and international travel.

4.6.5 Sponsored Programs

In close daily coordination with the Office of Export Control, Sponsored Programs ensures that all sponsored activities are managed in accordance with the UCF Export Control Policy and ECMP. Sponsored programs personnel are trained to assess potential export control issues associated with UCF programs and route all assessments to the Export Control Officer for final disposition.

4.6.6 Technology Transfer

In coordination with the Office of Export Control, the Office of Technology Transfer ensures that all Patent applications are secured until such time as they are filed and become "publically available." Fundamental research generated technology and information contained in the patent application is not public domain until the patent is processed, typically 18 months after submission. Information about the invention that is not publically disseminated via the patent application, journal articles, or other public venues is not public domain. Information left out of the patent, patent application and other publically available documents such as know-how is not public domain. The Office coordinates with Export Controls to implement the necessary security protocols for all patent applications subject to a secrecy order.

4.7 CENTRAL UNIVERSITY ADMINISTRATION

4.7.1 Audit

University Audit provides feedback to the Office of Export Controls on compliance with export controls requirements during routine scheduled departmental and college audits. Export information necessary for these audits is shared with University Audit so that a thorough examination can be conducted. On a case-by-case basis, University Audit conducts targeted research and data collection in close coordination with the Office of Export Controls for official investigations. University Audit maintains TLO subscription used by the Office of Export Controls for certain background checks.

4.7.2 Compliance, Ethics, and Risk

University Compliance facilitates the reach of the export control program across campus by coordinating university-wide compliance activities including training, monitoring and awareness efforts. University Compliance provides additional investigation and outreach support.

4.7.3 Environmental Health & Safety (EHS)

Ensures institutional compliance with biological agents, chemicals, and other hazardous materials and maintains a register of all agents, chemicals, and other hazardous materials that are controlled both on the CCL and the USML. EHS reviews domestic and international shipping requests and ensures that all documentation and U.S. laws are followed. In this capacity, EHS coordinates international shipping with the Office of Export Controls to obtain necessary government approvals.

4.7.4 Finance & Accounting (F&A)

Finance and Accounting performs restricted party screening on international financial transactions for compliance with applicable OFAC regulations, and tracks purchase, custody, and disposal of ITAR-restricted defense articles, and other export regulated items as determined necessary by the Office of the Controller and the Office of Export Compliance. The Travel Department located within F&A reviews travel to destinations on the State Department Travel Warning List and executes approval requirements pursuant to UCF Policy 2-903 'Travel to Restricted Destinations" and ensures that all necessary reviews were conducted, and approvals obtained.

4.7.5 Foundation

In coordination with the Office of Export Compliance, develop policies and procedures to (i) screen international financial transactions for compliance with applicable OFAC regulations and entity lists, and (ii) ensure that all Foundation-funded activities are in compliance with export and sanction laws.

4.7.6 General Counsel (GC)

The General Counsel's Office employs multiple attorneys, with two of the attorneys being physically located in the Office of Research & Commercialization, who work jointly with the Office of Export Controls on legal issues associated with compliance. The General Counsel's Office prepares standardized contractual language, reviews agreements for export control issues; and forwards documents that were identified as containing possible export control issues to the Office of Export Controls for ECCN or USML jurisdictional classification.

4.7.7 Human Resources (HR)

Human Resources provide citizenship information to the Office of Export Controls to ensure international employees and foreign exchanges are in compliance with export and sanction laws.

4.7.8 Internationalization

The UCF Internationalization Office provides university-wide services related to international studies, Memoranda of Understanding ("MOU") between UCF and foreign institutions, study-abroad programs, international travel to restricted destinations, coordinating international partnerships and managing the International Services Center ("ISC") as well as the Center for Multilingual Multicultural Studies ("CMMS"). CMMS provides intensive English language courses for potential students to meet the minimum standard to successfully study at UCF. The Office of Internationalization coordinates travel approvals and international partnership arrangements between UCF and foreign educational institutions with the Office of Export Controls.

4.7.9 International Service Center (ISC)

The International Services Center processes all visa requests on behalf of the University. ISC reviews visa requests and submits all J1 DS-2019 applications related to activities taking place in technical colleges to the Office of Export Controls for compliance assessment. Sponsoring units are required to submit a Visiting Scholar Questionnaire for assessment. ISC relies upon the Office of Export Controls for I-129 (Petition for Nonimmigrant Worker) attestations. Sponsoring units are required to complete a Foreign National Employee Questionnaire. ISC coordinates with Export Controls to review employee, visiting scholar and business visitors activity for compliance with export controls. The International Taxation unit within ISC works jointly with Export Controls to review certain international collaborations and exchanges for OFAC and export compliance. ISC ensures that all international collaborations and foreign exchanges are in compliance with export and sanction laws pursuant to UCF Policy 2-901 "UCF Policy for All Foreign Nationals".

4.7.10 Information Security

The Information Security Office reviews and approves remote access requests for foreign persons requiring access to UCF IT resources. Access requests are routed to the Office of Export Control

for assessment to ensure permissions are limited only to public domain information. The Information Security Office coordinates all IT security protocols between the Office of Export Control and university IT staff embedded within operational unity across campus. The Office is instrumental in data security associated with Technology Control Plans and provides incident tracking and reporting of data breaches involving unclassified data, including export controlled data. The Office conducts university-wide training concerning threats, methods to counter-threats and other data security methods.

4.7.11 Purchasing

Purchasing assists the Export Control program by conducting Restricted Party Screens on all vendors. Purchasing ensures that the procurement of items on the CCL and/or USML are identified and assigned an ECCN number as appropriate, and the proper disposal of controlled assets. If requested, assign an administrator/responsible person to coordinate development and implementation of export compliance procedures with the Office of Export Control.

4.7.12 Property

Reserved

4.8 COLLEGES, RESEARCH CENTERS & INSTITUTES ADMINISTRATION

4.8.1 Vice Presidents, Deans, Department Heads & Directors

Academic Deans, Directors and department heads share the responsibility of overseeing export compliance in their respective departments, centers and institutes and work with the Export Control Officer to implement effective processes and controls to ensure export control compliance.

4.8.2 Faculty/Principal Investigators

Principal Investigators and department heads are responsible for ensuring that employees in their activities are properly instructed in the handling of export-controlled, or proprietary information and that they have signed the required briefing document, prior to involvement in the project, attended mandatory Export Control Training, and are cognizant of their obligations and responsibilities under the Technology Control Plan. Because faculty members have expert knowledge of the type of information involved in a research activity, their participation in the export control process is critical.

The Office of Export Controls will consult and provide assistance to faculty and Principal Investigators:

- To understand their obligations to comply with export control regulations by providing information and training
- To determine if technology involved in their research is specified in the USML or the CCL
- To review award agreements, terms and conditions for possible export control indicators

- Assist in preventing unauthorized distribution of export controlled technology
- Assist in the development Technology Control Plans (TCP) and implement research security measures, if required
- Ensure staff (students, post docs, visiting scholars) are appropriate to work on restricted programs, including when there is a change in scope of an export controlled project
- Ensure foreign nationals are excluded from access to export controlled technology or data until the availability of an exclusion has been determined, or an export license has been obtained.

4.8.3 University Personnel

Personnel, including Administrative and Professional ("A&P"), students, post docs, visiting scholars and other support staff provide critical support to export controls by:

- Identifying potentially problematic export control issues and forwarding those issues for assessment, including:
    - Deemed exports
    - Shipping
    - Import of goods
    - Reporting of suspicious incidents

5 PROCESSES & PROCEDURES

Detailed processes and procedures utilized to identify and manage export controlled activities are outlined below.

Export Control Protocols

Document No.	**Protocol**
ECO-1	Preliminary Assessment
ECO-2	Comprehensive Assessment
ECO-3	Findings & Notification
ECO-4	Technology Control and Security Compliance
ECO-5	Government Approval
ECO-6	Restricted Party Screening
ECO-7	Denied Entities
ECO-8	Deemed Export Attestation
ECO-9	Restricted Dissertations
ECO-10	International Travel
ECO-11	(Reserved) International Collaborations & Memorandums of Understanding
ECO-12	Records
	Instructions
ECO.INST-1	Instructions to Completing the Preliminary Export Control Assessment Form
ECO.INST-2	Proposals and Awards Requiring Preliminary Export Control Review
ECO.INST-3	Processing Department of State Licenses
ECO.INST-4	Processing Department of Commerce Licenses
	Forms
Form ECO-1.1	Preliminary Export Control Assessment Form
Form ECO-4.1	Technology Control Plan
Form ECO-4.2	Custody, Access & Use Agreement
Form ECO-5.1	125.4(b)(10) Bona Fide Employee Exemption Certificate
Form ECO-5.2	Initial Export Notification
Form ECO-5.3	License Return Notification
Form ECO-8.1	Visiting Scholar Questionnaire
Form ECO-8.2	Deemed Export Attestation Questionnaire
Form ECO-8.3	Attestation Email Language
Form ECO-8.4	Attestation Memo Language
Form ECO-10.1	Travel Preliminary Approval Form
Form ECO-12.1	TCP Closeout Checklist
Form ECO-12.2	TCP Participant Certification

5.1 ECO-1 PRELIMINARY ASSESSMENT

OFFICE OF RESEARCH & COMMERCIALIZATION

SUBJECT:	**Effective Date:**	**Guideline Number:**
	May 2014	ECO-1
	Supersedes:	
	Original	
Preliminary Assessment Protocol	**Responsible Authority:**	
	Export Control Officer	

APPLICABILITY
These protocols are applicable to all ORC Pre and Post Award Staff.

PURPOSE
It is the purpose of these protocols to establish clear preliminary review procedures for Sponsored Programs Pre and Post Award staff to follow for determination of applicability of export regulations to intended research that require comprehensive review by the Export Control Officer.

BACKGROUND
These protocols are intended to assist Sponsored Programs staff determine if Export Control Review and Approval is required **before** proposal submittal or award set-up by the Export Control Officer. Proposals and Awards identified as potentially problematic ("*red-flagged*") will be routed to the Export Control Officer for comprehensive assessment in accordance with Protocol ECO-2. Findings and notification will be issued by the Export Control Officer to both Pre and Post Award staff and the Principal Investigator(s) in accordance with Protocol ECO-3. Technology Control and security compliance requirements are issued by the Export Control Officer in accordance with Protocol ECO-4. Government Approval protocols are processed by the Export Control Officer in accordance with Protocol ECO-5.

GUIDELINE STATEMENT
The University of Central Florida, Office of Research & Commercialization, Office of Sponsored Programs, Pre and Post award units will conduct a preliminary export control analysis when a PI submits a proposal, receives an award, or amends the scope of an existing project in accordance with these procedures.

PROCEDURES
Sponsored Programs staff will review proposals and awards (*listed in Table 1)* for preliminary "red flags" using Form ECO1.1 "Preliminary Export Control Assessment" and mark review results on the form. All such documentation will be scanned and uploaded into ARGIS/TERA for recordkeeping purposes.

Preliminary review resulting with a "red flag" will require comprehensive review by the Export Control Officer. In the event that the comprehensive review determine that export control measures are required for project performance, then the ECO will issue written directives and implement security protocols that may need to be completed prior to account set-up. Selected project activities affected by export control requirements may not commence unless specifically directed by the ECO.

Pre-Award "Red Flag" Indicators

- Foreign sponsor(s), collaborator(s), subcontractor(s) or consultant(s)
- Foreign travel or shipping
- Proprietary information (NDA, CDA, PIA, MTA, etc.)
    - Scope of work is identified as export-controlled
    - IP, publication or dissemination restrictions are anticipated
    - Foreign sponsor or collaborators
    - Foreign performance of location, travel or shipping
- Prime Sponsor is DoD, NASA, DoE, DHS or an intelligence agency
- Funding announcement (Guideline, BAA, RFP, RFQ, etc.) reference to:
    - U.S. Government Security classification or clearance requirement
    - *Specific* reference that research is subject to Export Control Regulations (e.g. statements indicating the research is subject to the International Traffic in Arms Regulations)
    - Access or participation prohibitions based upon citizenship
    - Sponsor *approval* of foreign nationals personnel or prohibition of foreign persons
    - Publication or dissemination restrictions (sponsor approval required to publish or dissemination, or UCF is prohibited from publishing, disseminating results)
    - Information / data protection requirements (Personally Identifiable Information), IT security standards, or other identifiers

Post-Award "Red Flag" Indicators

- Agreement/Contract/Terms & Conditions requirements:
    - U.S. Government Security classification, clearance requirement, or DD 2345 Militarily Critical Technical Data Agreement
    - *Specific* reference that research is subject to Export Control Regulations (e.g. statements indicating the research is subject to the International Traffic in Arms Regulations)
    - Access or participation prohibitions based upon citizenship
    - Sponsor *approval* of foreign nationals personnel or prohibition of foreign persons
    - Publication and dissemination restrictions (sponsor approval required to publish or dissemination, or UCF is prohibited from publishing, disseminating results)
    - Information / data protection requirements

    - Budget Activity is or includes 6.2 (*applied*) or 6.3 (*advanced technology development*) or greater
- Prime Sponsor:
    - DoD, NASA, DoE, DHS or an intelligence agency
    - SBIR/ STTR flow-thru
    - Foreign sponsor, military or government

Information Required for Comprehensive Export Control Review

Sponsored Programs proposals and awards positively identified as requiring comprehensive review shall be forwarded to the Export Control Officer and will include the following informational materials:

1. Completed Form ECO1.1 "Preliminary Export Control Assessment Form"
2. A summary of the following information in the email sent to the ECO:

    a. Principal Investigator (Full Name)
    b. College / Department
    c. Research ID (*if assigned*)
    d. Project Title
    e. Sponsor Name
    f. Prime Sponsor
    g. Listing of Problematic "Red flags", export clauses or other issues
    h. Documents
        i. Guidelines / Request for Proposal
        ii. Draft Agreement / Contract
        iii. Terms & Conditions /Flow-down provisions
        iv. Statement of Work

Communication Required with PI

Sponsored Program staff will inform the PI(s) in writing of such proposals and awards that are suspect and require comprehensive review by the Export Control Officer for final determination. The ECO will be cc'd on this formal notification. The notification will include:

1. A copy of the completed ECO1.1 "Preliminary Export Control Assessment"
2. A copy of the "Information Required for Export Control Review" (*above*), and
3. A statement that the proposal or award requires comprehensive review by the ECO and that PI assistance will be required in this review. Project commence cannot be performed on the project until comprehensive compliance review has been conducted and approved or authorized by the Export Control Officer,

- PI assistance will include:
    - Providing a list identifying all foreign national participants, including faculty, staff, students, visiting scholars, collaborators, volunteers, etc., prior to proposal submittal (*if known*) or award,
    - Assisting the ECO in determining if the technology involved in the research is specified in the ITAR USML or the EAR CCL, when requested,
    - Assisting in the development of a Technology Control Plan and implement research security measures when required,

- Notify the Export Control Officer when new staff are added (students, post docs, visiting scholars) or there is a change in scope of the export controlled project,
- Prevent unauthorized access to export controlled technology or data until the availability of an exclusion has been determined, or an export license has been obtained.

- Sponsored programs staff will include a statement that that the ECO has been informed and will contact the PI in the near future.

Table 1: Proposals & Awards Requiring Preliminary Export Control Review by Sponsored Programs Pre and Post-Award Staff (not an exhaustive list)

	Proposal & Awards Requiring Preliminary Export Control Review	Preliminary Review Required?
1.	Sponsor identified as the Department of Defense (DoD) or related military agency (including, but not limited to the MDA, DARPA, NGIA, DTRA) and other military-related or intelligence agencies or any affiliated research lab (AFOSR, AFRL, ARL, ONR, HEL-JTO, etc): Military, Space, Intelligence	
a)	Contracts	Yes
b)	Grant, DURIP or Cooperative Agreement	Yes
c)	BAA with reference to foreign national restriction if invoked by contract clause	Yes
d)	*See SBIR/STTR Subcontracts below*	*See below*
e)	All other Agreement Types	No
2.	Sponsor Identified as NASA, DHS, NRC, DoE, Sandia, NNSA or NETL, or other federal energy-related labs	
a)	Grant / Cooperative Agreement	Yes
b)	Contracts	Yes
c)	BAA with reference to to foreign national restriction if invoked by contract clause	Yes
d)	*See SBIR/STTR Subcontracts below*	*See below*
e)	All other agreement types	No
3.	Subcontract w/ DoD as Prime	Yes
4.	Subcontract w/ NASA as Prime	Yes
5.	SBIR / STTR Subcontracts	
a)	DoD/NASA/DoE Other National Security Prime (CIA/DHS, MDA, DTRA, NNSA etc.)	Yes
b)	All other Primes	No
6.	Projects requiring access to restricted technical information or defense articles	Yes
7.	Projects with specific assess, dissemination, publication or participation restrictions	Yes
a)	Clauses, Reference to ECCN or USML Category, Section H, other references or statements	Yes
8.	Industry	
a)	If technology is subject to an NDA, PIA, CDA, MTA or similar agreement	Yes
b)	If technology or technical information is proprietary to the sponsor and provided to or generated by UCF	Yes
9.	International Sponsor	
a)	Sponsor identified as a foreign government, military, space or intelligence agency (including NATO, UN, ADD, IMOD, etc.)	Yes
b)	Projects requiring access to restricted technical information or defense articles	Yes

c)	If technology is subject to an NDA, PIA, CDA, MTA or similar agreement	Yes
d)	Foreign Universities that are not Denied Entities	No
9.	Project involves International Shipments / Hand-carry	Yes
10.	Project is restricted and a thesis or dissertation will be published	Yes

Other Activities Requiring Export Control Review that may involve Sponsored Programs		ECO Approval Required before Finalization?
11.	I-129 Certifications for Technical Colleges & Departments, including J-1 Visiting Scholars	Yes
a)	Visitors from State Sponsors of Terror: Iran, Sudan, Syria, North Korea, Cuba	Yes
12.	MOU's with international organizations	
a)	Universities	Yes
b)	Military or military-related organizations	Yes
13	$25K procurements / sole source General Counsel Requests	Yes
14	International Travel:	
a)	Any destination on a travel warning: http://travel.state.gov/travel/cis_pa_tw/tw/tw_1764.html	Yes
b)	International travel to non-restricted destination if in conjunction with a sponsored activity identified in 1-10 above	Yes
15	International collaborations	Yes
16	International Shipments	Yes
17	Imports	Yes
18	Proposals / Awards with a NASA China Assurance requirement	Yes
19	Export Compliance certification certificates	Yes

OFFICE OF EXPORT CONTROLS
PRELIMINARY EXPORT CONTROL ASSESSMENT

(The instructions ORC ECO.INST-1 and ORC ECO.INST-2 apply to this effort.)

DATE OF REVIEW:

1. REVIEWER

2. REVIEW TYPE PRE-AWARD ☐ POST-AWARD ☐

3. INVESTIGATOR INFORMATION

a. RESEARCH I.D. / ACCOUNT

b. PRINCIPAL INVESTIGATOR / CO PRINCIPAL INVESTIGATOR

c. COLLEGE / DEPARTMENT

d. TITLE

4. SPONSOR INFORMATION

a. SPONSOR / COMPANY (check if foreign sponsor ☐)

b. PRIME SPONSOR (federal only)

c. FEDERAL AGENCY

5. OTHER AMPLIFYING DATA

	YES	NO
a. Is the sponsor the DoD, DoE, NASA, NNSA, MDA, DHS, DARPA, NGIA, DRTA or other military-related or intelligence agencies or any affiliated research lab (AFOSR, AFRL, ARL, ONR, HEL-JTO, etc.) or foreign government?	☐	☐
b. Is the project a SBIR / STTR flow-thru?	☐	☐
If yes, do the Guidelines indicate the topic is subject to the ITAR or export controls? Or does the award contain any restrictive flow-thru?	☐	☐
c. Does the Announcement (Guideline, BAA, RFP, RFQ, etc.) or the Award documents (Contract, Grant, Terms & Conditions, etc.) contain any problematic clause or provision that would preclude the program from qualifying as "fundamental research"?	☐	☐

6. FOREIGN COMPONENTS	YES	NO	N/A
a. INTERNATIONAL TRAVEL			
b. INTERNATIONAL SHIPPING			
c. FOREIGN SPONSOR			
d. FOREIGN COLLABORATOR			
e. FOREIGN SUBCONTRACTOR / CONSULTANT			
f. FOREIGN PERFORMANCE LOCATION			
7. PROJECT INPUTS			
g. REQUIRES NON-PUBLIC DOMAIN DATA			
h. PROPRIETARY INFORMATION			
(1) NDA, CDA, PIA, MTA			
(2) SCOPE OF WORK POSSIBLY EXPORT CONTROLLED			
i. RECEIVE EXPORT CONTROLLED EQUIPMENT OR MATERIALS			
j. RECEIVE RESTRICTED OR EXPORT CONTROLLED DATA			
RESERVED			
8. TECHNOLOGY Not all inclusive			
k. MILITARY, INTELLIGENCE, SPACE, ENERGY, DEFENSE			
l. SPACE, SATELLITE, MISSILE, OR ROCKET TECHNOLOGY			
m. PATHOGENS, TOXINS, SELECT AGENTS, BIOLOGICAL, CHEMICAL			
n. NUCLEAR, PROPULSION, ENERGY, TURBINES			
o. UAV, SIMULATION, HIGH POWER LASER, OPTICS, CERAMICS			

9. ANNOUNCEMENT / AGREEMENT	YES	NO	N/A
p. SPONSOR APPROVAL OF FOREIGN NATIONAL PERSONNEL			
q. U.S. GOVERNMENT SECURITY CLASSIFICATION			
r. PUBLICATION OR DISSEMINATION RESTRICTIONS OR APPROVAL			
s. DD 2345 MILITARILY CRITICAL TECHNICAL DATA AGREEMENT			
t. SPECIFIC REFERENCE TO EXPORT CONTROLS			
u. PERFORMANCE WILL GENERATE RESTRICTED INFORMATION DURING CONDUCT			
10. PROJECT CONDUCT			
v. PROJECT OR FACILITY ACCESS OR PARTICIPATION PROHIBITION BASED ON CITIZENSHIP			
w. TECHNICAL DATA OR I.T. PROTECTION REQUIREMENT			
x. BUDGET ACTIVITY CATEGORY / TECHNOLOGY READINESS LEVEL (TRL)			
6.3 ADVANCED TECHNOLOGY DEVELOPMENT OR GREATER			
y. UTILIZE NON-UCF EXPORT CONTROLLED EQUIPMENT / MATERIALS/ PROPRIETARY INFO.			
aa. WILL PERFORM AN EXPORT CONTROLLED SERVICE			
11. PROJECT OUTPUT			
bb. WILL GENERATE, FABRICATE OR MODIFY EXPORT CONTROLLED MATERIALS			
cc. WILL RESULT IN AN EXPORT CONTROLLED SERVICE			
dd. RESULTS SUBJECT TO DISTRIBUTION LIMITATION OTHER THAN "A"			
(1) DISTRIBUTION B, C, D, E, F, OR X STATEMENTS TO BE PLACED ON RESULTS			
(2) CUI CATEGORIES & SUBCATEGORIES DESIGNATION ON RESEARCH RESULTS			

12. PRE / POST AWARD EXPORT ASSESSMENT

All "positive" responses require an explanation. Indicators for "Comprehensive Export Assessment" are identified below and must include specific reference suspect red flags, including citation to the document and page number. ***Comprehensive Assessment is required for YES responses in Sections, 7, 9, 10, and 11.***

13. ASSESSMENT DETERMINATION & CERTIFICATION **Export Control Assessment stated herein are complete and will be forwarded to the PI.**

Based upon Preliminary Review, the above referenced activity does ☐ , does not ☐ require comprehensive assessment before submittal or award set-up.

Initial assessments resulting in a possible "red flag" will be routed electronically to the Export Control Officer for comprehensive review and must, at a minimum, include a copy of the guidelines / RFP; draft agreement or contract; terms & conditions / flow-down provisions; statement of work and any other applicable documentation. See "ORC ECO-1 "Export Control Preliminary Review Protocol" for additional information.

FORM ECO 1.1 OCTOBER 2013 PREVIOUS EDITIONS OBSOLETE

Print Form Clear Form

5.2 ECO-2 COMPREHENSIVE ASSESSMENT

OFFICE OF RESEARCH & COMMERCIALIZATION

SUBJECT:	**Effective Date:** October 2013	**Guideline Number:** ECO-2
Comprehensive Assessment Protocol	**Supersedes:** July 2010	
	Responsible Authority: Export Control Officer	

APPLICABILITY
These protocols are applicable to the Office of Export Controls.

PURPOSE
It is the purpose of these protocols to establish clear comprehensive review procedures for Office of Export Controls staff to follow for determination of applicability of export regulations.

BACKGROUND
Sponsored Programs staff determine if Comprehensive Export Control Assessment is required **before** proposal submittal or award set-up by the Export Control Officer. Proposals and Awards identified as potentially problematic ("*red-flagged*") are routed to the Export Control Officer for comprehensive assessment in accordance with Protocol ECO-2. The Export Control Officer will conduct the assessment and consult the PI and Sponsored Programs as required to conclude that the research program either is subject to export controls or qualifies for an exemption or other government approval. Findings and notification will be issued by the Export Control Officer to both Pre and Post Award staff and the Principal Investigator(s) in accordance with Protocol ECO-3. If subject to export controls, a Technology Control and security compliance requirements are issued by the Export Control Officer in accordance with Protocol ECO-4. Government Approval protocols are processed by the Export Control Officer in accordance with Protocol ECO-5.

GUIDELINE STATEMENT
The University of Central Florida, Office of Research & Commercialization, Office of Export Controls, Export Controls Officer will conduct a comprehensive export control analysis when a doubt exists as to the applicability of the program as "fundamental research."

PROCEDURES
Export Controls staff will review proposals, awards, agreements or other activities and assess whether the activity is impacted by export controls laws or regulations. Comprehensive assessment

methodology will rely upon the CIRAC format: Conclusion, Issue, Rule, Analysis, Conclusion. The Export Control Officer will (1) examine the activity, (2) examine all relevant documentation pertaining to the activity, (3) conduct legal and regulatory research concerning federal compliance requirements related to the activity, (4) apply the research to the university activity, (5) issue a conclusion, (6) and concisely summarize the conclusion in writing to formally document the compliance effort.

In the event that the assessment determines export control measures are required, the Export Control Officer will issue written directives and implement security protocols pursuant to Protocol ECO-4.

Comprehensive Assessment Procedure

1. Gather Data
Gather all programmatic data concerning a project: participants / collaborators and their nationality, proposal, Statement of Work / Terms and Conditions / contract**,** type of technology involved (EAR, ITAR, or neither) and deliverables.

2. Jurisdictional Analysis
Agency jurisdiction and proper commodity/technology classification (i.e. military or non-military) should be made when reviewing all data for obvious restrictions or subjects that may be controlled if awarded (i.e. DoD contracted research, pass-thru, proprietary, or restrictions on participation or publication).

If it is difficult to determine the commodity/technology classification, an opinion may be requested from the government (commodity jurisdiction).

3. Participant Review

Restricted Parties Screen: Screen for restricted parties/entities using Visual Compliance.

Foreign National Participants: Foreign nationals (students) permitted to work on research projects are only a concern if the research does not qualify for an exclusion.

4. Review program for export control indicators pursuant to check sheet (Appendix 1)

5. Applicability of Exclusionary Rules
Research qualifying for an exclusion is not subject to export controls. Most research (particularly grants) will qualify for the FRE. Some sponsored research (usually government contracts) may contain restrictions that nullify the FRE and thereby subject the research to export controls.

To qualify for FRE, the agreement cannot contain restrictions typically found in proposal request / award clauses. Such clauses must be negotiated out of the agreement in order to qualify. The research must also be conducted within the U.S. at an institution of higher learning. Defense research is regulated under ITAR and is funded from 3 areas of the Defense's budget (e.g. 6.1 Basic Research, 6.2 Applied Research, 6.3 Advanced Technology Department). Defense research may or

may not qualify for an exclusion, depending upon contract requirements. The "use" of ITAR articles by foreign nationals (the USML word for "item") requires licensing. International shipments of tangible items do not qualify for FRE.

If the project does not qualify as FRE, review the technologies with the PI to determine if they are controlled under EAR CCL or ITAR USML. If they are not on either control list, the project may be proprietary, but not otherwise subject to export controls.

As the individual most knowledgeable about the technologies the researcher is responsible for assisting the Export Control Officer in ascertaining whether or not the technology is on the EAR/ITAR list. The Office of Export Controls will rely on this certification to determine whether the research falls within export controlled areas.

- **EAR CCL**
  The "use" of EAR items in research subject to Export Control Regulations are negated if the research qualifies as FRE. Therefore, it is imperative to qualify the research for FRE (if possible) and ensure that all items or data are within the EAR.

  Research not qualifying as FRE or Public Doman may require a "deemed export" license if all of the following criteria of the controlled technology are released (the "deemed export" threshold): operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing.

- **ITAR USML**
  Defense articles do not qualify for FRE; however, technical data may if it is already in the "Public Domain" or comprises general science and mathematics. Defense articles on campus require a Technology Control Plan, and only licensed foreign nationals are permitted access. Bona Fide Employees qualify for an ITAR exemption, and are permitted access to defense articles so long as they are not from an ITAR Proscribed country.

6. Negotiation of Contracts and Grants

A careful review of the contractual terms must be done in order to determine whether export controls apply and if so, which sets of regulations the project falls under. This determination requires a detailed understanding of the statement of work and the commodities and technology involved in the research as well as a thorough understanding of the project plan (e.g., project participants, citizenship of all involved, end users, and end use). Problematic clauses should be negotiated out on the basis of institutional policy. Defense research can be negotiated. Also, negotiation of an agreement may result in the removal of T&Cs, contractual clauses or change in scope of the SOW that otherwise would have subjected the research to export controls. If subject to export controls, the Office of Export Compliance, in consultation with the Sponsored Programs, will take further required action.

7. Determine if there are any other General Areas of Concern:

- Physical exports (International Shipments/Deliverables)
- Deemed exports (if not FRE) Remember, FRE nullifies the deemed export rule
  - Foreign sponsors or collaborations
  - Hosting visiting scientists

    - Foreign Collaborations
- Foreign travel (to sanctioned countries or with equipment)

Restricted Research

In those situations where the University approves an award that is affected by export controls, the Office of Export Compliance will coordinate with the PI and Sponsored Programs on the development and implementation of a Technology Control Plan. This may involve issuing notices, applying for licenses, restricting access and participation, compartmentalizing aspects of the project, or modifying the scope of the research.

Restricted Access

In awards not qualifying for an exclusion or with technologies or equipment listed on the ITAR USML, it may be necessary to restrict foreign national involvement (including access to stored data or information on computer networks) until:

- Identification of these research personnel and their country of nationality is verified by the Office of Export Compliance as not subject to controls or until approval by the Government Contracting Officer is received; or
- The foreign nationals are licensed by the appropriate Government agency.

Publication Restriction

In rare instances where certain projects may include technology listed in the EAR/ITAR identified as sensitive material or critical end use, the award document may impose a publication restriction to the extent any proposed publication may require advance approval by the Government even if 1) no foreign nationals are appointed to the project or 2) an Export License is not required.

Appendix 1:
Comprehensive Assessment

Guideline, terms, contractual documents, and national security restrictions

- Foreign Person Participation or identification of participants by nationality
- Access to information or facilities
- Dissemination of the results of information, pre-pub approval, no attribution, no presentation at conferences
- Other SBIR and STTR award specific requirements

INPUT ISSUES

Sponsor Provided:

- Non-public domain technical data or information, such as:
    - For Official Use Only (FOUO), Controlled Unclassified Information (CUI), Sensitive But Unclassified (SBU), Law Enforcement Sensitive (LES)?
    - Proprietary Information (CDA, PIA, NDA, MTA)
- Hardware, software or technical data subject to other restrictions (e.g. user agreements)?
- Procurement of defense articles

Arms Export Control Act & Security Classification
Will security classification or restriction be imposed on the project, including but not limited to:

- DD Form 2345, Military Critical Technical Data Agreement
- DD Form 254 DoD Contract Security Classification Specification
- Personally Identifiable Information,
- Other type of federal security classification or restriction
- NASA Awards: NASA Assurance for Funding Restrictions with China? http://www.research.ucf.edu/ExportControl/nasa.html

CONDUCT ISSUES

Participants:

- Are any foreign persons anticipated to participate in this program?
- International collaboration
- Foreign Travel
- Sanctioned country or entity list involvement?

Research Instruments

- Does the conduct of the research involve access or operation of any EAR or ITAR research instruments, equipment or software?
- Access, use or operation or transmittal of defense article(s)?
- Deemed exports?

Application:

Commercial Applications

- Designed, developed for commercial use or involves commercial commodities?

Military Application

- Sponsored by or involve: NASA, DoD, DARPA, MDA, Energy, DHS, Intel, DoD flow-thru, defense contractors or associated research lab (such as the Office of Naval Research or Air Force Office of Scientific Research) including flow-thru awards?
- Indications of that research is not basic (6.1) or applied (6.2)?
    - Advanced Technological Development (6.3),
    - Demonstration & Validation (6.4),
    - Engineering & Manufacturing Development (6.5),
    - Management Support (6.6), or
    - Operational Systems Development (6.7)?
- Specially designed, developed, configured or adapted for a military application
- Activities related to chem/bio weapons, missiles, encryption, HHS or USDA Select Agents, pathogens, or toxins?
- Access, use or operation or transmittal of defense article(s)?

OUTPUT ISSUES

Federal Government Specific Distribution Limitations

- Generation of any technical data or information identified as:
  - For Official Use Only (FOUO), Controlled Unclassified Information (CUI), Sensitive But Unclassified (SBU), Law Enforcement Sensitive (LES)?
  - Limited Distribution Information requiring distribution statements to be placed on unclassified scientific technical documents (e.g. Contract Data Requirements List (CDRL's)) such as:
    - Distribution B: Authorized to U.S. Government Agencies Only
    - Distribution C: Authorized to U.S. Government Agencies and their Contractors
    - Distribution D: Authorized to the DoD and U.S. DoD Contractors only
    - Distribution E: Distribution authorized to DoD components only
    - Distribution F: Further distribution only as directed
    - Distribution X: Distribution authorized to U.S. Government agencies

Fundamental Research (EAR)

All information or software involved published or planned to be published or released and made generally accessible to the public:

- Periodicals, books, print, electronic, or any other general distribution media;
- Subscriptions available without restriction for purchase;
- Websites available to the public free of charge or at a cost not exceed the cost of reproduction;
- Public Libraries;
- Patents and open (published) patent applications;
- Release at an "open" conference, meeting, seminar, trade show in the U.S., accessible by the public for a fee where attendees may take notes and leave with notes.

Information Results (ITAR)

Does the information and software results meet all of the following criteria?

- Results from basic and applied research in science and engineering conducted at an accredited institution of higher education located in the U.S.;
- Is ordinarily published and shared broadly within the scientific community

Educational Instruction

Instruction in general science, math and engineering principles commonly taught at schools, colleges and universities, and conveying information through courses listed in course catalogues and in associated teaching laboratories of academic institutions

Other International Components

- Involve any international visiting scholar(s) (including researchers, post docs and visiting scientists)?
- Involve training of foreign persons in the "operation" of equipment?

- Have any other type of international component, including but not limited to:
    - Sponsorship by a:
        - foreign-owned company
        - foreign government
        - foreign research institutions
        - foreign military / Law enforcement
        - foreign military affiliated contractor

- MOU between UCF and a foreign institution
- Other type of international collaboration

OFAC

- Collaboration with foreign scientist(s), researcher(s) or institution(s) outside of the U.S.?
- Performance of research in a foreign country?
- Payment to any individual, entity or organization (i.e. subcontractors) in a foreign destination for performance or will any U.S. researchers be paid abroad?

International travel

- Travel to sanctioned or embargoed countries for purposes of teaching or performing research?
- Travel to a destination currently under a State Department Travel Warning?
- Travel out of the U.S. with tangible articles, items samples or technical data associated with a UCF project including UCF equipment?
- Transfer or hand-carry of research data or information out of the U.S. (including on a PDA/flash-drive , laptop, or log-in remotely to a UCF server)? **If yes,**
    - Is any of the data or information proprietary, or subject to export control?

Shipping

- Shipping of items, samples or technical data to foreign countries (e.g., sample shipments for analysis)?
- Will materials be transferred to UCF from an outside entity or from an outside entity to UCF?

Importation

- Importation of any items or materials

Final Export Control Compliance Determinations:

Restricted Research Under:

- EAR
- ITAR
- DEAR
- OFAC

Required Protocols:

- Export Compliance Standard Terms & Conditions, Form ECO-3.1

- Technology Control Plan, Form ECO-4.1
- Custody, Access & Use Agreement, Form ECO-4.2
- Export Compliance Training
- Other

5.3 ECO-3 Assessment Findings & Notification

OFFICE OF RESEARCH & COMMERCIALIZATION

SUBJECT:	**Effective Date:** October 2013	**Guideline Number:** ECO-3
Assessment Findings & Notifications Protocol	**Supersedes:** July 2010	Page Of
	Responsible Authority: Export Control Officer	

APPLICABILITY
These protocols are applicable to the Office of Export Controls.

PURPOSE
This protocol establishes consistent practices to document assessment findings and provide notification of the results to PIs and other applicable personnel.

BACKGROUND
Preliminary (ECO-1) and Comprehensive (ECO-2) assessment may involve face-to-face meetings, legal and regulatory research, and contract negotiations and will conclude with an official determination. Personnel will be notified of the results of the findings of assessment by the Export Control Officer in accordance with the Assessment Finding and Notification Protocol (ECO-3). Activities subject to export controls may require implementation of TCPs (Form ECO-4.1), CAUs (Form ECO-4.1), or other government approvals in accordance with protocol Technology Control and Security Compliance Requirements Protocol (ECO-4) and Government Approval Protocol (ECO-5).

GUIDELINE STATEMENT
Principal Investigators ("PI"), faculty, staff, and other critical personnel must be informed when sponsored and non-sponsored activities are found not to meet the legal qualifications of "fundamental research" or "educational activities" to ensure that performance is executed in accordance with federal regulatory requirements.

PROCEDURES
Export Controls staff will issue a conclusion, summary, and guidance in writing to formally document compliance efforts. The documentation is a summary of the methods used to:

1. Identify activities subject to export controls
    a. Proposal / Contract identification
    b. Hardware, software identification

    c. Services identification
    d. Other activity type identification (collaboration, travel, etc).
2. Identify license requirements associated with restricted activities, to include:
    a. Deemed export licenses(Commerce)
    b. Foreign national worker licenses (State)
    c. Tangible export license requirements for shipping of items
    d. Applicability of other U.S. Government Approvals (exemption, exception, exclusions)
    e. Import requirements
3. Plan license requirements, to include:
    a. Identifying foreign persons involved in restricted activities
4. Plan Security Requirements
    a. Notifying all parties of restrictions
    b. Implementing Technology Control Plans, or other access and use plans
    c. Indoctrination and training of personnel

Findings & Notification Procedure

Notification of Unrestricted Activities
The PI or other staff shall be notified via email if an activity, proposal or award is found to qualify under the Fundamental Research Exemption ("FRE") or for another exclusionary rule pursuant to Protocol ECO-2. The notification may include guidance to ensure the activities do not exceed the requirements of the exemption. Documentation, correspondence and all other records pertaining to the assessment will be retained in the project file.

Commodity Jurisdiction / Commodity Classification / Advisory Opinion Requests
If an activity cannot be determined to be subject to export control laws and regulations then UCF will seek guidance from cognizant federal agency:

- 22 CFR 126.9(a) "Advisory opinion"
- 22 CFR 120.4 and 120.4 'Commodity Jurisdiction"
- 15 CFR 748..3 "Classifications and Advisory Opinions"

Notification of Restricted Activities
Sponsored Programs and Export Control Staff will notify a PI and other involved personnel in writing of activities found to be subject to export controls, including instructions pertaining to compliance activities the University will require.

Notification may apply to:

- Proposed research activities.
- Awarded research activities
- Procurement activities
- Agreements
- Travel
- Hosting visiting scholars

Initial notification will include:

- A summary of the noted restrictions,
- Regulatory jurisdiction (if available) applicable to the activity and the technology control requirements that UCF will need to implement to be compliant. This will include relevant copies of the USML and CCL as appropriate.
- Statement regarding licensing, in addition to any other instructions deemed necessary by the Export Control Officer.
- Scheduling a verbal inquiry regarding the activity, if necessary.
- A request for a listing of all intended activity participants and/or clarification of any programmatic issues.
- Notification that foreign persons cannot participate in the activity without prior government approval or other broad-ranging regulatory requirements subject to an activity, such as travel restriction requirements.

Documentation will be processed to confirm PI and Co-PI acknowledgement of program restrictions in accordance with ECO-12 "Records."

For restricted research activities, a summary of restrictions will be provided to the PI via Form ECO-3.1 "Export Compliance Terms & Conditions." A memo detailing instructions, including a copy of a draft version of the Technology Control Plan will accompany the initial notification.

Initial Notification Sample Email

EMAIL:

Subject Line: Notification of Federal Restrictions for "[insert program name]" – RESPONSE REQUIRED

First Notice

Dear [Name],

This email is to inform you that the [program name] project is subject to federal restrictions on foreign national access and performance pursuant to the International Traffic In Arms Regulations ("ITAR"), 22 C.F.R., Chapter I, Subchapter M, Parts 120-130, because the technologies involved in the program are specifically identified in the US Munitions List, ("USML") [USML Category].

Due to the restricted nature of this technology, UCF is providing you notice of the restriction. You are required to implement a Technology Control Plan ("TCP") containing operational security requirements and procedures. TCP protocols ensure foreign persons do not inadvertently access program equipment or data, participate in the program, or that the research team does not publish research results or otherwise disseminate restricted information. Access, dissemination, publication

and participation prohibitions apply to all foreign national UCF faculty, staff, students, visiting scholars and volunteers.

Only trained "U.S. Persons" may collaborate, participate, access or perform on a program subject to the ITAR. Activities allowable only for a trained U.S. Person include: accessing any prototypes, materials, substances or other devices related to the research, accessing anything provided by a sponsor subject to non-disclosure arrangement, program participation including training, and reviewing any preliminary or final research results, publications or data.

"Export Control Training for Researchers" is administered on the 1st and 3rd Tuesday of each Month from 3:00pm until 4:30pm in Engineering 2, Room 202A. All participants will receive a separate notification to schedule mandatory training.

For purposes of the ITAR, U.S. persons include all U.S. Citizens and Permanent Residents refugees or asylees. Trained participants with a green card can work on a restricted program. All program activities must be compartmentalized in accordance with the TCP from graduate students, UCF employees, faculty, visiting scholars, etc. or others who are not "U.S. persons" unless the foreign person has prior U.S. Government approval in the form of a licensed or meet the requirements of an exemption and has been trained.

Accompanying this notification are instructions that list the compliance forms that are required to be completed prior to engaging in any restricted activity. **Please sign and return the attached export compliance terms as soon as possible.** Also attached is a draft Technology Control Plan that you will need to work with my office to complete. The TCP contains a listing of the USML Category pertaining to this activity and any associated restrictions. **This Plan must be completed before any work on the activity can commence.** I would like to have it completed no later than [date].

Please make sure you carefully read the Instructions and the export terms and TCP as these documents require your input.

Please let me know if you have any questions.

Sincerely,

University of Central Florida

Export Controls Compliance Special Terms & Conditions

Office of Research & Commercialization, 12201 Research Parkway, Suite 501
Orlando, FL 32826-3246 – (407) 882-0660

THIS FORM IS FOR INTERNAL USE ONLY AND SHOULD NOT BE FORWARDED TO THE SPONSOR

Principal Investigator: _____

Project Sponsor: _____

Proposal Number: _____

Proposal Title: _____

Please note the following Special Terms & Conditions applicable to your project. Complying with the following Special Terms & Conditions is the responsibility of the Principal Investigator. Failure to comply with these terms & conditions could result in severe civil and/or criminal fines and imprisonment.

If checked, the following Special Terms & Conditions are applicable to this project:

☐ **Publication Restrictions** – You may not publish the results of this research without the prior written consent of the sponsor (including presentations at conferences, proceedings, journals, discussions, or any other disseminations of the research).

☐ **No Foreign Person(s) on Project** – Only U.S. citizens and valid Permanent Residents (Green Card holders) may be allowed access to technical data, items or materials generated or provided by the sponsor or other participants in this research.

☐ **Pre-Approval Required for Foreign Person(s)** – Sponsor requires notification of all persons other than U.S. Citizens and valid U.S. Permanent Residents to be pre-approved by the sponsor prior to having access to any generated or sponsor provided technical data, materials or items.

☐ **International Traffic In Arms Regulations** – Items, materials, or technical data generated or provided are subject to the International Traffic In Arms Regulations (ITAR) and a Technology Control Plan **will be required** to restrict access to generated or sponsor provided items, materials, technical data, defense articles, or software (including source code).

☐ **Export Administration Regulations** – Items, materials, or technical data generated or to be provided are subject to the Export Administration Regulations (EAR) and a Technology Control Plan **may be required** to restrict access to sponsor provided items, materials, technical data, or software (including source code) that are subject to the EAR. An Export Control Classification Number (ECCN) must be either provided from the sponsor or be "self determined" through cooperation between the Office of Research & Commercialization and the Principal Investigator.

☐ **Technology Control Plan Required** – A Technology Control Plan (TCP) is required for this project. The TCP is a plan developed jointly between the PI and the ORC Export Control Officer (ECO) detailing the extra security and special handling required to protect the export restricted materials generated or provided by the sponsor. The PI is the party responsible for compliance with the TCP and requires approval of the Department Head or Dean of the College.

By signing below I hereby certify that I have read and understand the above checked Special Terms & Conditions applicable to my research project. Furthermore, I understand that by accepting this research project with the above restrictions:

- I may not be able to publish the results of the research in any manner without the express written consent of the sponsor, and that any students involved in this research may not be able to publish their thesis or dissertation that could result from the research.
- I may be restricted as to who I may employ, including foreign researchers, students, and collaborators.
- I am personally responsible for violations resulting from research activities that exceed the approved Scope of Work. No activities should be performed outside the Scope of Work without prior approval from the ORC, Office of Compliance.
- I shall ensure all subcontractors and consultants are made aware of these Special Terms & Conditions.
- I am aware that I am responsible for compliance with the security, training, and other requirements in the Technology Control Plan if a plan is required for this project.

By accepting restrictions on this research project I understand that this research is likely subject to one or more U.S. Export regulations and laws, and violations of these laws could result in severe civil and/or criminal fines and imprisonment. If you DO NOT want to accept these restrictions on your project, please contact your pre-Award Administrator or Contract Manager.

Returned the signed form to the Office of Research & Commercialization, ATTN: Mike Miller, or call (407) 882-0660. Additional information is available on the Export Compliance website at: http://www.research.ucf.edu/ExportControl/

Signed _____ **Date** _____

Rev.-2, 12/06/2012

5.4 ECO-4 TECHNOLOGY CONTROL AND SECURITY REQUIREMENTS

OFFICE OF RESEARCH & COMMERCIALIZATION

SUBJECT:	**Effective Date:** June 2013	**Guideline Number:** ECO-4
Technology Control and Security Compliance Requirements Protocol	**Supersedes:** July 2010	
	Responsible Authority: Export Control Officer	

APPLICABILITY

These protocols are applicable to all UCF faculty, staff, students, volunteers and other individuals who possess or may possess export controlled information, classified or unclassified, as defined in and governed by the National Industrial Security Program Operating Manual ('NISPOM"), the International Traffic in Arms Regulations ("ITAR"), the Export Administration Regulations ("EAR"), Office of Foreign Assets Control ("OFAC") Foreign Assets Control Regulations ('FACR") or the Department of Energy Acquisition Regulations ("DEAR"), or other regulations as appropriate that require security protocols

PURPOSE

This procedure delineates the protocols to create and implement a Technology Control Plan ("TCP") (see Form ECO-4.1) and other security protocols to ensure that no information, governed by the NISPOM, ITAR, EAR or DEAR is disclosed intentionally or inadvertently (including oral or visual disclosure) to any Foreign person; whether he or she is an employee of UCF, a visitor, a customer, a vendor, a contractor, or a service representative, unless an export license or other form of government approval has been issues, which authorizes such disclosure.

BACKGROUND

Programs are reviewed to identify those that require Technology Control from those that require no control measures through two processes; Protocol ECO-1 "Preliminary Assessment" and Protocol ECO-2 "Comprehensive Assessment." Following assessment, programs requiring Technology Control are further reviewed, documented, and formal notification is provided to the Principal Investigator, or custodian in accordance with Protocol ECO-3 "Findings & Notification." This protocol, ECO-4 "Technology Control and Security Requirements" document specific procedures taken to create a TCP, Custody, Access and Use ("CAU") Agreement, or other safeguarding plan.

GUIDELINE STATEMENT

The University of Central Florida, Office of Export Control, is the single unit within UCF empowered to implement Technology Control Plans and other security protocols for programs subject to export control regulations.

PROCEDURES

Determining What Type and Level of Security Measures

The Export Control Officer is responsible for:

(1) Identifying export-controlled input, conduct, and output activities related to research
(2) Identifying contractual security requirements, including Operational Security requirements ("OPSEC")
(3) Identifying the security resources available within a particular department, and, based upon resources,
(4) determining the most appropriate security measures to implement to ensure compliance with export controls:

Appropriate Security Measures

Determining the appropriateness, level, and severity of technology controls is largely subjective; however, the following chart provides a baseline. The Export Control Officer will issue an Export Terms notification to the PI and co-PI's followed by a TCP that is customized for each laboratory.

	Level 1		Level 2		Level 3	
Restrictions	**EAR (Proprietary)**	**ITAR**	**EAR (Proprietary)**	**ITAR**	**EAR (Proprietary)**	**ITAR**
Input	CAU	CAU	CAU	CAU	CAU	CAU
Conduct	ST&C	ST&C/ TCP	ST&C	ST&C/ TCP	ST&C	ST&C/ TCP
Output	ST&C	TCP	ST&C	TCP	ST&C	TCP
Input, Conduct, Output	TCP	TCP	TCP	TCP	ST&C	TCP
hdwr, sftwr, other	CAU	CAU	CAU	CAU	CAU	CAU

Level 1:

- No prior TCP experience
- Foreign nationals in proximity to Research
- Co-mingled Lab

Level 2:

- Prior TCP Experience / Assessed Risk
- No Foreign persons in proximity to Research
- Lab Compartmentalizable

Level 3:

- Prior TCP Experience w/o assessed Risk
- Cleared Staff
- Lab Compartmentalizable

Certain programs may only require notification and a more simplistic TCP based upon:

- Overall security, security education, training, awareness or other security variables pre-existing in the department
- The nature of the restricted activity
- Proximity of foreign persons to restricted activity
- Export Controlled inputs (whether procured, loaned or provided by a sponsor)
- Export-controlled conduct, including operation of restricted instruments.
- Export-controlled generated outputs resulting from the research.

I. **Standard Export Terms & Conditions ("ST&C")** Form is UCF's official notice to the PI and Co-PI(s) that the indicated project is subject to the federal restriction(s) checked on the form. It is used to confirm PI acceptance of access, dissemination, publication or participation restrictions associated with a research program. The form serves as official acknowledgement that the program is subject to either the EAR or the ITAR, or both, and indicates whether a TCP will be required for the activity.

II. **Technology Control Plan** is appropriate for multi-faceted programs with several participants and a combination of different restricted inputs, conduct, and outputs. A TCP is required for certain research work involving an ITAR export issue or other restrictions (publication, foreign national restrictions) that remove the work from qualification of the Fundamental Research Exclusion. A TCP identifies the restricted information/item is, who will have access to it, how access will be monitored and controlled, how the information/item will be physically and electronically stored, what information about it can be shared or presented and what will be done with the information/item once the project is complete.

III. **Custody, Access & Use Agreement** is a standardized security protocol primarily used to manage defense articles, technical data or software that are independent of restricted programs. Custodians of such items must acknowledge 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.

Completing the Selected Security Measure

I. Technology Control Plan

A boilerplate TCP (Form ECO-4.1) will be sent to the PI as part of the initial notification (Protocol ECP-3). The Export Control Officer is responsible to initially evaluate the proposed work and input preliminary information into the TCP for PI review, as follows:

- Assigned Export control file No. (Pursuant to ECO-12 "Records Protocol" using the Master Index)
- PI and Co-PI
- Title
- Account
- Sponsor and Government Agency

- Jurisdiction, USML / CCL Category and Subcategory descriptions
- Identification of contractual and publication restrictions
- Identification of publication restrictions
- Identification of IT system security by coordinating TCP protocols with department IT staff

The PI is responsible to provide:

- Initial list of proposed participants, including their nationality.
- Identification of the areas where the research will take place
- A Physical Security plan to control the work area.
- A IT Security plan to control access to IT data
- Proposed international travel
- Proposed method to manage personnel changes

Physical security measures may include:

- Laboratory Compartmentalization: Quarantine specified research areas from observation or access by unauthorized persons and ensure the research team is trained and aware of their responsibilities. Do not distribute keys or other access to a lab with export controlled items or data to foreign nationals.
- Time Blocking: Project operation may be restricted to secure time blocks when unauthorized individuals cannot observe or access export controlled materials or project data.
- Marking: Export controlled information must be clearly identified to ensure it is not inadvertently distributed.
- Locked Storage: Tangible items such as equipment, operating manuals, external hard drives, hardcopy data and research journals should be secured in a locked storage container when not in the personal possession of approved project personnel.
- Electronic Security: Project computers, networks, and electronic transmissions should be secured and monitored through User ID's, password controls, and encryption. Research data should be saved on encrypted flash drives or external hard drives that can be locked in a storage container.
- Confidential Communications: Discussions about the project must be limited to authorized project participants, in areas where unauthorized individuals are not present.

Access control measures may include:

- Locking data, hardware, software using the "one-lock" principal
- Escorting foreign visitors within research facilities
- Establishing classified work areas
- Data storing restrictions for Information Systems
- Marking all export-controlled materials
- Sanitizing information systems after use
- Project completion controls (i.e. disposal of hardware)

I**nformation Technology security** measures may include:

- Standard computer security (passwords, transmission of data, etc).
- Implementation of computers not on the network, or laptops

- Segregated electronic storage, or limited folder access privileges
- Use of encryption
- Removal of data upon completion of program

Upon completion of the draft TCP, the Export Control Officer will:

- Review the plan for compliance with the contract terms and conditions
- Contact Human Resources to verify the citizenship of proposed participants
- Add the IT server information to the IT Security Officer List for intrusion monitoring
- Coordinate any training appropriate for participants

Once finalized, the TCP will be signed by all listed parties. The original document is required to be returned to the Export Control Officer for inclusion into the export project file.

II. Custody, Access & Use Agreement

A boilerplate CAU Agreement Form (Form ECO-4.2) will be sent to the PI. This may be part of a sponsored activity (Protocol ECP-3), or unrelated to research whereon a PI may be obtaining items, equipment, material or software subject to the ITAR that require a specific custody and access plan to ensure foreign persons do not have access. The Export Control Officer is responsible to initially evaluate the proposed activity and input preliminary information into the CAU for PI review, as follows:

- Jurisdictional analysis and USML identification of the material, equipment or software.
- Verification of personnel list proposed by the PI
- Verification that the proposed location and method of storage is adequate

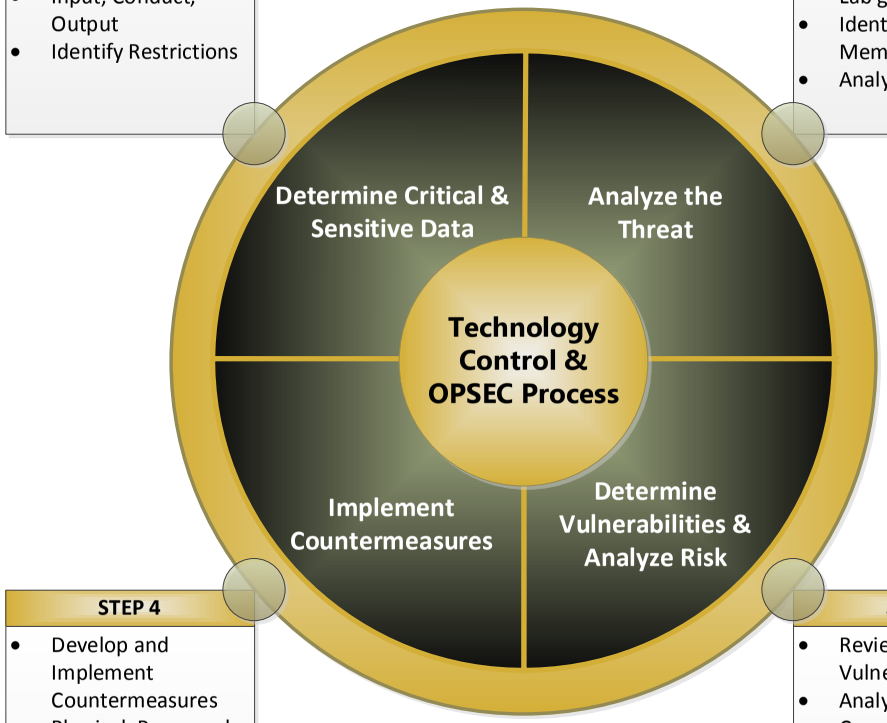
The "Custodian" is responsible to provide:

- A list of personnel requiring access
- Location and method of storage

Once finalized, the CAU will be signed by all listed parties. The original document is required to be returned to the Export Control Officer for inclusion into the export project file.

ECO-4 "Technology Control and Security Compliance Requirements Protocol"

- Preliminary Assessment — ECO-1
- Comprehensive Assessment — ECO-2
- Notification — ECO-3
- **Technology Control — ECO-4**
- U.S. Government Approval — ECO-5



STEP 1

- Determine level of security requirements
- Determine Critical and Sensitive Data
- Input, Conduct, Output
- Identify Restrictions

STEP 2

- Gather Lab and Resource Data
- Screen Research Locations
- Identify Participating Lab groups
- Identify Team Members
- Analyze Threats

STEP 3

- Review Areas for Vulnerabilities
- Analyze Risk of Compromise

STEP 4

- Develop and Implement Countermeasures
- Physical, Personnel, Access Controls, IT Security
- Train Participants
- Acknowledge TCP
- Report Suspicious Contacts

TECHNOLOGY CONTROL PLAN

DATE:
[Fill In]

PM/DDTC APPLICANT CODE:
[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]

REVISION HISTORY

Revision	Date	Title or Brief Description	Entered By
Original		Initial Release	

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.

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 International Traffic in Arms Regulations ("ITAR") codified at 22 Code of Federal Regulations (CFR) §§ 120-130, and the Export Administration Regulations ("EAR") codified at 15 Code of Federal Regulations (CFR) §§ 300 – 799 and the National Industrial Security program operating Manual ("NISPOM"). A TCP is a roadmap of how UCF will control restricted technology to ensure compliance with the ITAR, EAR 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 UCF 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.

Defense Article: "Defense article means any item or technical data designated in § 121.1 of this subchapter. The policy described in § 120.3 is applicable to designations of additional items. This term includes technical data recorded or stored in any physical form, models, mockups or other items that reveal technical data directly relating to items designated in § 121.1 of this subchapter. It does not include basic marketing information on function or purpose or general system descriptions."

Defense Services: "Defense service means: (1) The furnishing of assistance (including training) to foreign persons, 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 (2) The furnishing to foreign persons of any technical data controlled under this subchapter (see § 120.10), whether in the United States or abroad."

Foreign person: Any persons or entities (including businesses) that are ***not*** a citizen or Permanent Resident Alien (green card visa holder) of the United States (8 USC § 1101(a)(20)) or protected individuals as defined in 8 USC § 1324b(a)(3) (refugees, asylees, or persons in the U.S. under an amnesty program).

Technical data (22 CFR § 120.10):

1. "Information ... required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of [United States Munitions List regulated] defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions and documentation;... software directly relating to defense articles...include[ing] but...not limited to the system functional design, logic, flow, algorithms, application programs, operating systems and support software for design, implementation, test, operation, diagnosis and repair.
2. Classified information relating to defense articles and defense services;
3. Information covered by an invention secrecy order;
4. Software ... directly related to defense articles;
5. 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."

Technology or source code (15 CFR §§ 734.2.b.ii, 772.1): 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."

UCF Statement of Commitment

The University will 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. As a cleared defense contractor, UCF 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: http://www.research.ucf.edu/ExportControl/ that contains university export control policies, forms, training modules and reference materials.

Export Control Jurisdiction, Classification and Categorization

UCF will create, generate, require access, or receive technical data or defense articles regulated by the Arms Export Control Act ("AECA") and subject to the federal restrictions specified in the

ITAR in performance of this program. This TCP details the mitigation techniques UCF will implement to comply with the ITAR requirements. The Principal Investigator (PI) and Approved Project Personnel are required by law to conform to the minimum security requirements to ensure that controlled defense services, articles, and technical data or controlled commodities are adequately protected from disclosure. The applicable United States Munitions List ("USML") Category and subcategory classifications are:

US Munitions List, ("USML") Category XXXX: Title, Subparts (b), (h), (i), (j).

Insert USML Category

Foreign National, Publication, Contractual Restrictions and Compliance Guidance

This program involves information and data subject to contractual, publication and foreign person restrictions as follows[1]: [The Export Compliance Officer will Select the Applicable Contractual Restrictions]

- **1852.204-76 "Security Requirements for Unclassified Information Technology Resources"**
  Guidance – requires contractor to submit a plan for managing program data to ensure the methods meet the minimum IT security requirements pursuant to NIST SP800-19 & FIPS 199; acceptable if campus conducts own screening of campus personnel.

- **1852.225-70 "Export Licenses" (FEB 2000)**
  Guidance - If satellite technology is involved, contact the ORC Export Compliance Officer for guidance. ALT. I used when technical data is to be exchanged with a NASA foreign partner.

- **1852.225-71 "Restriction on Funding Activity with China" (FEB 2012)**
  Guidance -- Foreign national scholars and students who are citizens of China and affiliated with the Government of China (including having tuition paid by the Government of China) and all others affiliated with the Government of China (including non-Chinese Citizens) are not eligible to participate in this program, nor is collaboration allowable without specific NASA approval. The PI is required to complete the UCF questionnaire regarding Chinese affiliation.

- **1852.235-71 "Key Personnel and Facilities" (MAR 1989)**
  Guidance - Identifies key personnel and requires NASA approval to remove, replace or divert any of the listed people. In addition, indicative of no foreign national access to NASA facilities, compounded with other clauses.

- **1852.237-73 "Release of Sensitive Information" (JUN 2005)**
  Guidance – This program will access and/or generate sensitive information subject to national security restriction. All such data, including hardware, software and technical information, will be subject to export control laws. All data must be marked appropriately and maintained IAW federal law. Contractor must identify all information provided to NASA. All service providers must follow safeguards.

- **Section H: Additional Reports of Work, - SBIR Phase II**
  Guidance – Requires a final summary without restriction or proprietary and export controlled information for NASA publication.

- **52.225-25 "Prohibition on Contracting with Entities Engaging in Sanctioned Activities Relation to Iran – Representations and Certification (NOV 2011)**
  Guidance – Foreign national scholars and students who are citizens of Iran or others affiliated with the Government of Iran and not eligible to participate in this program, nor is collaboration allowable.

- **52.227-14 "Rights in Data – General (DEC 2007) – Alternate II (DEC 2007)**
  Guidance – Release, publication and use of data indicates contractor is unable to reproduce, distribute or publish any export –controlled or national security data. All such data must be properly marked and maintained IAW federal law.

- **Section C-5: Distribution Statement B**

[1] Any restriction voids the ability to conduct project activities as "fundamental research."

Guidance – Requires restriction of information, including export controlled information generated in furtherance of the contract, to be distributed only to authorized U.S. Government Agencies. Foreign national access during or upon completion of work subject to this distribution requirement requires compliance with federal laws. Topics falling under USML categories are subject to the International Traffic in Arms Regulations (ITAR). Contractors must follow proscribed federal safeguard measures including prohibiting access or participation by foreign nationals and dissemination or publication without required licensing or exemptions in addition to Sponsor approval.

- **Export Control Warning**
  Guidance – All technical documents that are determined to contain export-controlled technical data shall be marked "WARNING - This document contains 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." When it is technically not feasible to use the entire statement, an abbreviated marking may be used, and a copy of the full statement added to the "Notice To Accompany Release of Export Controlled Data"

- **Section H-6: Foreign Nationals Performing Under Contract**
  Guidance – Limits foreign national participation to State Department licensed foreign nationals only who are approved by the Sponsor.

- **252.204-7000 "Disclosure of Information" (AUG 2013)**
  Guidance – All articles, Information, datum, and services provided to and generated, created or originating by the Contractor under this agreement are "sensitive" and "Critical Information" subject to national security restriction. Topics falling under USML categories are subject to the International Traffic in Arms Regulations (ITAR). Contractors must follow proscribed federal safeguard measures including prohibiting access or participation by foreign nationals and dissemination or publication without required licensing or exemptions in addition to Sponsor approval. Certain information may be qualified as fundamental research if approved in writing by the U.S. Government contracting officer.

- **252.204.7012: "Safeguarding of Unclassified Controlled Technical Information (NOV 2013)**
  Guidance – Technical data residing on IT systems must comply with NIST requirements. All suspicious interdiction attempts must be reported to the federal government within 72 hours of discovery.

- **252.227-7017: "Identification and Assertions of Use, Release, or Disclosure of Technical Data or Computer Software (JAN 2011)**
  Guidance – Technical data and software resulting from this project is subject to restriction, which requires notification and identification to all recipients. Topics falling under USML categories are subject to the International Traffic in Arms Regulations (ITAR). Contractors must follow proscribed federal safeguard measures including prohibiting access or participation by foreign nationals and dissemination or publication without required licensing or exemptions in addition to Sponsor approval.

- **252.227-7025: "Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends (MAR 2011)**
  Guidance – Information, informational materials, documents, or other mediums marked with restrictive identification are subject to various federal laws requiring restriction due to national security. Such restrictive markings include any variety of acronyms which vary among federal agencies, including: FOUO, ITAR, AECA, EAR, Export Controlled, Sensitive, CUI, SBI, Critical Information, etc. All information identified with any marking other than "Distribution Unlimited" or "Approved for Public Release" is subject to internal restriction. Topics falling under USML categories are subject to the International Traffic in Arms Regulations (ITAR). Contractors must follow proscribed federal safeguard measures including prohibiting access or participation by foreign nationals and dissemination or publication without required licensing or exemptions in addition to Sponsor approval.

- **DEAR 970.5225-1 Compliance with export control laws, regulations and directives**

- **OPSEC Requirements Pursuant to NSDD-298**
  Guidance – Information generally available to the public as well as certain detectable activities reveal the existence of, and sometimes details about, classified or sensitive information or undertakings. Such indicators may assist those seeking to neutralize or exploit U.S. Government actions in the area of national security. Application of the operations security (OPSEC) process promotes operational effectiveness by helping prevent the inadvertent compromise of sensitive or classified U.S. Government activities, capabilities, or intentions. The operations security process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures. The process begins with an examination of the totality of an activity to determine what exploitable but unclassified evidence of classified activity could be acquired in light of the known collection capabilities of

potential adverseries. Such evidence usually derives from openly available data. Certain indicators may be pieced together or interpreted to discern critical information. Indicators most often stem from the routine administrative, physical, or technical actions taken to prepare for or execute a plan or activity. Once identified, they are analyzed against the threat to determine the extent to which they may reveal critical information. Commanders and managers then use these threat and vulnerability analyses in risk assessments to assist in the selection and adoption of countermeasures.

- **1052.209-96 "Protection of Information and Non-Disclosure Agreement" (MAR 2010)**
  Guidance – All information, including IT systems and computer software, used in the course of performing work under this program, or generated as a result of this program, must be used and protected and not disclosed or used for any other program or purpose. This includes technical data. Upon conclusion of the work, all items, technical data and software will be returned to the Government.

- **1052.209-93 "Disclosure of Information – RFP" (DEC 2008)**
  Guidance – Reciepient is not allowed to disclose information concerning the RFP or its sponsorship to anyone..

- **1052.215-93 "Contractor Personnel Resumes and Clearances" (DEC 2008)**
  Guidance – All program participants must be disclosed and their clearance status provided to the Government.

Program / Project Site Address and Contact Information

Describe the physical location of each sensitive technology/item include building and room numbers. A schematic of the immediate location is highly recommended

The PI must provide the following information

- PI Primary Phone
- PI Primary Email
- Research Group Name (if applicable)
- Laboratory Name (if applicable)
- Building, Office, Room Number (as applicable) (identify multiple locations separately)
- Primary location of where controlled items and data will be stored while the research is being conducted
- Location(s) of all project computers that will contain controlled data

Project Personnel

Approved Project Personnel and Technical Data Custodians

All personnel and participants authorized to work on the project are required to be U.S. persons pursuant to proof of citizenship verification. Acceptable documentation includes:

- Birth Certificate
- Passport
- Naturalization Certificate
- Certificate of Citizenship
- Permanent Resident Alien Card

[Laboratory Name] (PI Name)

- [PI to specify project members and Citizenship, e.g. First Name, Last Name, U.S. Citizen]

[Laboratory Name] (PI Name)

- [PI to specify project members and Citizenship, e.g. First Name, Last Name, U.S. Citizen]

All project personnel are responsible for reviewing and signing this TCP. All project personnel have attended or will attend training provided by ORC. All project personnel are made aware of their responsibilities to prevent either active or inadvertent disclosure of controlled items and of the criminal and civil penalties (including prison sentences of up to 10 years and fines of up to $1M) for failure to comply with U.S. export control rules or other federal regulations. All project personnel will be screened against the applicable restricted parties' access lists and will have their nationality screened by the ORC. The PI will notify ORC before adding additional personnel to a project having access to export controlled items.

Project Personnel Screening Procedures
Prior to commencement of any work and access to any controlled or other sensitive data all project personnel must:

1. Be a U.S. Citizen or Permanent Resident formally designated in writing
2. Receive a copy of this TCP, and
3. Sign a copy of this TCP in which the employee acknowledges understanding of the Plan.

Personnel Foreign Person Screening Procedures
Students, visitors, conference participants, etc., or employees of the university who are defined as "foreign persons" or "foreign nationals" may not participate in this program or have access, in any capacity, to export controlled technical data unless license authority has been granted by DDTC, the BIS or other authorized federal agency. The supervisor, to whom the foreign national reports, will control access to the export controlled data. When applicable and pertinent to their activities, foreign nationals will be briefed by their supervisor and/or the ECO, in those areas of export control and export licensing, as set forth in the guidelines provided by the DDTC and BIS. Provisos and limitations included in the approval must be implemented prior to the transfer of any export of data, materials, etc. Foreign nationals will be informed as to their responsibility to protect export controlled data and the treatment of export controlled technical information obtained during their employment or visitation. Foreign nationals are required to adhere to facility security rules, policies, and procedures relating to on-campus regulations for personnel.

Foreign National Exemptions
[The Export Compliance Officer will Complete this Section]
125.4(b)(10) Exemption: Exports by Accredited U.S. Institutions of Higher Learning to Full-time Bona Fide Employees
123.16(b)(10) Exemption: Exports by Accredited U.S. Institutions of Higher Learning of Category XV Spacecraft Systems and Associated Equipment

Personnel Changes
The PI and department shall notify the ECO (1) each time an additional person is added to the project so that they can be screened and trained, and (2) when the scope of the project changes. The only authorized individual allowable to access any restricted information will be the PI. All other access requires approval by an empowered official.

Personnel changes in the case of terminated employees, or the departure of individuals working on the program will be reported as soon as possible.

Protection Guidelines

Physical Security
The PI and all Co-PI's are responsible for creating and implementing compliant security solutions within all areas (offices, labs, analysis areas, classrooms, etc.) as identified in Section XX and other areas where restricted program research will take place in accordance with the following parameters.

Classified Work Area
UCF does not have facilities or authorization to conduct classified activities in furtherance of this program.

Unclassified Segregated Work Area
The PI is responsible to make provisions for foreign persons to have an enclosed work area, where possible. Foreign persons performing duties in open work areas, co-mingled labs, or shared areas containing export-controlled information will be escorted and monitored by Authorized Personnel unless other provisions have been arranged to ensure no access to restricted information is possible.

Access Controls in Unclassified Work Area
Export controlled technical data and articles (including mock-ups and prototypes) must always be secured from unauthorized access by foreign persons. Computer rooms/areas that process export controlled data must be secure during business hours and locked after close of business. Only users listed as Approved Project Personnel may have key access to the secure project office.

Escorts
The PI and approved project personnel will ensure that foreign nationals are escorted within the lab area when applicable and that foreign nationals are not given keys, combinations, passwords or other access to enter the secured inner lab area where securing For Official Use Only ("FOUO") and Controlled Unclassified Information ("CUI") and other ITAR-restricted technical data is stored. Foreign nationals are not permitted independent, unescorted 24 hour access to a work area until such time as all export controlled activity has ceased.

Foreign persons must be granted a U.S. Government approval, including a possible license to access restricted program data, articles, or export controlled information resulting from research.

Project data and / or materials must be physically shielded from observation by unauthorized individuals by operating in a secured laboratory, space or other area during secure time blocks when observation by unauthorized persons is prevented. This includes laboratory management of "works in progress."

Electronic Countermeasures for Unclassified Work Area
Personnel are not authorized to discuss sensitive or critical information where disclosure to foreign nationals is possible. All cell phones or similar devices must be kept a minimum of 2 meters from all experimental equipment, computers or any other electronic device containing Critical Information at all times.

Release of Technical Data from Unclassified Work Area

No employee or other person acting on behalf of UCF 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), and non-UCF managed IT services (e.g. Yahoo.mail or Gmail), is strictly prohibited.**

No posters, information postings or other summary regarding program work is authorized to be disseminated either within the research facility or on any website, blog or other communication medium.

Information Display:

Windows on the inner secure area will blackened to prevent viewing from outside. If necessary, dividers will be positioned so that the inner area is not viewable from outside the work center. The inner secure lab area contains no access to outer windows or sightlines viewable from a distance.

Physical Security Plan for Unclassified Work Area.

The PI must provide a detailed narrative of each phase of the project and any physical security plans you will implement to protect the restricted item / technology from unauthorized access, i.e. secured doors, limited access, security badges, etc. The PI will need to specify the research location and measures to ensure foreign nationals do not have access to the program, (e.g. a secure inner room where FOUO, CUI, and other ITAR-restricted technical data is stored). Only approved project team members will be issued keys in order to restrict who has access to the secured inner room.

Materials testing will take place in the Engineering building, in the [PI] lab 1234, and the {PI} labs (room #100 and 101) or in the {PI} labs within. Additionally, work related to spectroscopy will be carried out in xxxxxxx). The doors to these labs will be locked during data collection periods, with notification clearly posted on doors. Surfaces (bench tops, desk tops, walls) will remain free of project technical data in order to avoid accidental visual disclosures to unauthorized persons. Physical property data will be acquired and analyzed on the [specify instrument] located in Room 100. This characterization system has dedicated computer control (and is not connected to a network). All sensitive data will be stored on a separate, password protected external hard drive which will remain stored and locked when not in use in a secured office. Lab 100 is a shared lab with keycard (therefore limited) access to which foreign persons do have access. Where possible, data analysis runs using xxxxx instruments will be scheduled to take place when only project participants are present in the lab. In those rare circumstances where others may be present, the [Instrument] computer will be configured to allow access during run time only to project participants and the computer monitor will be completely covered and marked as "private" to prevent disclosure. Run results will be collected on an encrypted, removable hard drive for storage and analysis in room 100 or the (room number 101).

Program experiments will be conducted in Engineering with data being stored in 100 as discussed above. Additional experiments will be carried out in the [Specify Laboratories] (room 201) located in Suite 1000 of Engineering 1. Experimentation will occur in a secure inner room where FOUO,

CUI, and other ITAR-restricted technical data is stored. Where exclusive use is possible, approved project team members will be issued keys in order to restrict who has access to the secured inner room.

Storage of Defense Articles and Technical Data

Storage:
Research material, samples, prototypes, mock-ups and data including lab notebooks, hard and softcopy of data, reports, research materials must be stored in a locked room, drawer, filing cabinet, briefcase, or other storage device, so that access to the material by unauthorized individuals (i.e. anyone not an approved member of the project team) is prevented whenever unattended. This includes FOUO or CUI data provided by the sponsor or generated by the university.

It is the responsibility of the project personnel to safeguard the controlled items at all times by having "one lock" in place, such as:

(1) Controlled items will be secured in a locked storage container when not in the personal possession of the approved project personnel.
(2) Critical Information such as configuration processes, listings of materials/chemicals or other characteristics will be locked-up in physical form or encrypted on a stand-alone computer system.
(3) Electronic data will be stored on hard drives of a stand-alone non-networked computer. Media will be saved on CD-roms which will be locked up in the secured area.

Location:
Data (soft and hardcopy) must be limited to storage within the secure room that is physically safe from access by unauthorized persons at all times. No copies will be made available except to Approved Project Personnel.

Printed Material:
Printed material containing FOUO, CUI, or ITAR-restricted technical data shall always be secured from unauthorized access (e.g., locked in a secure cabinet within the secure project office when not in use).

Electronic Media:
Machine-readable media storage devices will be CD-ROMs or DVD-ROMS. **Thumb-drives/flash Drives are unallowable and are not permitted as a storage device for data.** Subject data on machine-readable media shall always be secured from unauthorized access (e.g., locked in a secure cabinet within secure project office when not in use, only one backup copy can be made.

Marking.
Portable electronic storage devices and hard copies that contain controlled technical data will be marked with the following warning:

> WARNING - *This contains 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, as amended, Title 50, U.S.C., App. 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.*

Information Technology Security[2]

Appropriate measures must be taken to secure controlled electronic information, including User ID's, password control, SSL or other approved encryption technology. Database access must be managed via a Virtual Private Network (VPN), allowing only Approved Project Personnel access to data over the internet if the transmission is secured using 128-bit Secured Sockets Layer (SSL) or other advances, federally approved encryption technology.

Authorized Personnel and Custodians
Approved project personnel are the only designated users of the computers. Designated computer custodians are identified as:

- [PI to specify project members and Citizenship, e.g. First Name, Last Name, U.S. Citizen]

Unclassified Stand Alone Desktop Computer.[3]
A standalone desktop computer is any single-user PC (e.g., running a Windows operating system). Laptop computers are discouraged and may be strictly prohibited unless specific security safeguarding measures are implemented. Computer systems must be hardened using federal standards.[4]

---

[2] DoD Information Security Program, Volumes 1-4 is available at: http://www.dss.mil/seta/news/2012-03-01a.html

[3] Unclassified Computer Information Security program requirements is available at: http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf

Minimum Security Requirements

The following are minimum security measures for standalone computers processing ITAR, FOUO or CI-restricted data:

- Laptop computers cannot be used
- Limit access to room/area to License users only
- Passwords-unique, 6-8 characters with one non-alphanumeric
- Change password at least every 3 months
- Notification (warning statement)
- Read-only access to original data
- Shut down any connections to other computers prior to loading data on the system
- Lock computer and/or room when away from computer, or
- Enable automatic "shutdown" after 3-5 minutes of inactivity
- No routine backups of restricted-use data
- Change staff passwords accordingly when staff changes
- Remove data by overwriting at the end of the project or prior to the computer needing repair

Passwords: Passwords must be unique, 6-8 characters in length, contain at least one non-alphanumeric character (e.g., ?, &, +), and be changed at least every three months. See subparagraphs "Lock Computer and/or Room" and "Automatic 'Shutdown' of Inactive Computer" for other password requirements. In the absence of an automated password generator, user-selected passwords should be unique, memorizable, and NOT dictionary words.

No Connections to Another Computer: Prior to placing any subject data (export controlled technical data) on a standalone desktop computer, shut down any connections to another computer (e.g., via modem, LAN, cable, wireless).

Lock Computer and/or Room: When the authorized user is away from the computer, protect the subject data by locking the computer and/or the room. For example, physically lock the computer with its exterior keylock, shut down the computer and enable its power-on password, or lock the room to prevent an unauthorized individual from gaining access to the computer.

Automatic "Shutdown" of Inactive Computer: Some computers can automatically shut down, logout, or lockup (e.g., password-protected screen-savers) when a period of defined inactivity is detected. If available, this feature may be used in place of or in addition to locking the computer and/or room. When used, the defined period of inactivity shall be three to five minutes.

Do Not Backup Restricted-Use Data: Routine or system backups (e.g., daily, weekly, incremental, partial, full) of restricted-use data is not allowable, except for the one backup copy that must be physically locked and encrypted. This restriction does not apply to backing up statistical computer syntax code used to analyze the restricted data.

Data Storage. Dedicated external portable drives are acceptable only if encrypted and password protected that are kept within a secure inner lab area. The controlled technical data must be secured by encryption or password protection. Emails shall not contain controlled technical data files unless both send and receive email locations are encrypted.

Data Transmission. All data transmissions of CUI, FOUO, or ITAR-restricted technical data must be in accordance with "DoD Information Security Program: Controlled Unclassified Information (CUI), Volume 4, Enclosure 3" available at: http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf The standard requires PKI Encryption[5] for all data transmissions, including email transmissions, which contain CUI, FOUO, or ITAR-Restricted technical data. Encryption technology meeting the federal standard can be found at: http://iase.disa.mil/pki/eca/certificate.html

Data transmissions in furtherance of this project will comply with contract requirements via electronic mail in Microsoft compatible formats.

Structure of IT Security and Security Plan

---

[4] FIPS 200, Minimum Security Requirements for Federal Information and Information Systems http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf and NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems available at: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf

[5] Theses encryption products (in addition to all "National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) 140-2 Validated products" listed at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm) are subject to Federal Export Control Regulations and require licensing for export outside of the United States, including hand-carrying such commodities on business travel (e.g. hand-carrying a laptop with encryption pre-loaded on the device).

Structure of IT Security and Security Plan

Describe the information technology set-up / system and detail the security plan (i.e. password access, firewall protection plan, encryption, onsite communication methods between Approved Project Personnel, servers to be used, etc). Describe how you will manage IT resources that contain export controlled data in the case of personnel changes (e.g. how will you ensure a student does not mistakenly use one device on an uncontrolled project when the device was previously used on a controlled project).

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. Should an employee or student depart while the project is ongoing, screens 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.

Secured Storage for Fiber Design and Fabrication (Dr. Rodrigo Amezcua)

1. All files related to these projects are stored in folders on the CREOL file server at the following location: \\net.ucf.edu\College\Home\Shared\project name
2. Read and write access is granted using Active Directory security group called "Program".
3. The file server is a virtual machine (file server number.net.ucf.edu) in the UCF data center joined to the UCF NET domain, secured behind the UCF firewall as well as the server's own Windows firewall.
4. Users' NET domain credentials provide authentication.
5. The UCF VPN provides secure remote access.
6. All files related to this project stay in this folder on the college server. Files and folders are not copied to local desktop or laptop computers, nor are they copied to any other media such as CDs or thumb drives.
7. After the completion of the project, the folder and its contents will be encrypted, written to a DVD, and erased from the server.

Secure Computing

1. All Computers used for this project are all joined to the UCF NET domain. The domain security group (2. above) is used to grant local login and remote desktop access. All other users, except college computer administrators, are explicitly denied access.
2. No data related to the project are stored on these computers. After the completion of the project the hard-drives will be removed from the computers and either destroyed or securely erased.

DISCLOSURE

Dissemination

Approved project personnel are not authorized disseminate, in any form (such as publication, visual or oral disclosure, posting on a social network) any FOUO, CUI, or ITAR-restricted technical data, including the nature of this research, involved collaborators, and technical capability. This includes listing this project and other associated information on

any website, resume, publication, professional document, annotation or disclosure in any other manner or form. All such disclosures require the prior written permission by the Sponsor.

Verbal:
Discussions in person or via telephone concerning the project or work product are limited to the Approved Project Personnel and contributing investigators and may not be held in a location that may disclose information to unauthorized persons. Discussions with third-party subcontractors, volunteers, or any arrangement with no exchange of funds require a Non-Disclosure Agreement.

Graduate Student Thesis / Dissertation:
You are required to contact the College of Graduate Studies before allowing a student to conduct a thesis or dissertation subject to the ITAR. Contact Max Poole for additional information.

Proprietary Information

UCF Proprietary Information. UCF's proprietary information is protected by confidential disclosures and nondisclosure agreements as necessary. Release of UCF's proprietary information occurs only after a nondisclosure agreement is executed between the party releasing and the party receiving the information.

Proprietary Information Received by UCF. This information is protected under the terms of each nondisclosure agreement as negotiated and executed by the parties involved.

International Travel

International travel with restricted information is not permitted. If international travel is anticipated, all data relating to this project requires licensing before such data can be transported out of the United States.

PROJECT COMPLETION & REPORTING

Project Completion Requirements

Information Security Procedures.
Upon completion of a restricted research project, all controlled items will be disposed of or stored properly. The secure storage requirements set forth in the previous sections remain the same after completion of the project. Hard copies will be disposed of by shredding. Electronic files will be disposed of by using current "wiping" software.[6] Contact ORC or your department IS administrator for information on effective solutions for wiping. Hardware and equipment can be disposed of properly by contacting ORC. The information security data associated with this project will be disposed of by either shredding or using a U.S. Government approved media sanitization package.

Employee / Student Certification.
Upon completion of this project or a planned permanent departure from the university while actively involved in this project, employee and students must certify that they have not given or disclosed to any unauthorized person any documents, reports, or other data, which is considered to be export controlled information pursuant to this Plan.

Deviation

Any deviation or waiver from or exception to this procedure requires the prior approval of the UCF Empowered Official within ORC, who are:

- Tom O'Neal, Associate Vice President, Office of Research & Commercialization
- Douglas Backman, Director of Compliance, Office of Research & Commercialization
- Michael Miller. Export Compliance Officer, Office of Research & Commercialization

Reporting

[6] pursuant to *NIST 800-88 Guidelines for Media Sanitization* available at: http//csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

Any legal, investigatory, or other demand for disclosure of subject data, including any request or requirement to provide subject must be immediately reported to the Export Control Officer, Michael Miller or Nino Frederico at 407-882-0660 or by email at Michael.Miller@ucf.edu or Nino.Frederico@ucf.edu Time is of the essence in notifying UCF of any such request or requirement. UCF must also immediately inform the requestor or enforcer of the request or requirement that subject data are protected under the law of the United States.

Reporting is mandatory for:

- Suspect or confirmed breaches or compromise ("spillages") of data
- Access by unauthorized persons or employees not listed as "Approved Project Personnel"
- Access of data at an offsite location or on an IT system unapproved for use
- Inadvertent disclosure of data by any means (including uploading to the internet)
- Hacking attempts or breach of IT system(s) by illicit means
- Any other suspicious interdiction attempt or success

Recordkeeping Requirements

Each of the relevant export control regulations contain specific recordkeeping requirements that must be satisfied. In addition, the university maintains its own recordkeeping requirements in order to document its commitment to, and compliance with, export control regulations generally. Departments or programs must keep soft or hard copies of all export documentation, including financial records, shipping documentation (Commercial Invoices, Shipper's Export Declarations), and appropriate UCF paperwork in their research project files for a period of five years from the date of the export, re-export or controlled deemed export.

Submitted:

Signature:

_____ Date: _____

Dr. [Name], [Title] Professor
[Laboratory]
[Department]
[College]
University of Central Florida

Approved Personnel to Access and Use Defense Articles, Software and Technical Data

By signing below, I affirm that I have been provided a copy of the Technology Control Plan and that I agree to the provisions therein.

Signature:_____ Date: _____
[Project Team Member]

Signature:_____ Date: _____
[Project Team Member]

Signature:_____ Date: _____
[Project Team Member]

ATTESTATION MEMORANDUM FOR RECORD

SUBJECT: Attestation of Understanding and Compliance Agreement with the Technology Control Plan

Section 1: To be completed after initial ITAR Training

I, [Project Team Member], having read the subject Technology Control Plan, attest to my understanding of the following responsibilities:

a. I will refrain from sharing the research project's Critical Information (CI) with personnel who are not part of the contract or university research teams performing under contract Number [Number]

b. I will notify my Principal Investigator (PI) of any inadvertent disclosures

c. I will comply with the management controls and Te3chnology Control Plan countermeasures prescribed in the Plan.

_____ _____ _____

[Project Team Member] Date Dr. [Name], Professor

Date

Section 2: To be completed upon exit from the research project

I attest to my understanding that my obligation to protect the project's Critical Information (CI) and Export Controlled technical data continues past my association with the project. I acknowledge that I am required to follow the same countermeasures to protect that information after my association with this project has concluded.

_____ _____ _____

[Project Team Member] Date Dr. [Name], Professor

Date

University of Central Florida

Office of Research & Commercialization

INSTRUCTIONS FOR CUSTODY, ACCESS AND USE AGREEMENT FOR EXPORT CONTROLLED DEFENSE ARTICLES, TECHNOLOGY, INFORMATION OR SOFTWARE

This form is for internal use only and should not be forwarded to the sponsor

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, technical data or software, you become personally liable (civil and criminal) for failing to prevent improper disclosure, even if in the academic setting. This requirement is applicable to the provision, procurement, acceptance or loan of USML defense articles or Commerce Control List (CCL) items, articles, technical data or software that enter onto Campus for use in research or academics that are in the care, custody, access or use of UCF employees and students.

Allowing a foreign person (including a foreign person here in the U.S., e.g. on UCF's campus) to access defense articles, software or technical data, or providing instruction to the foreign person regarding "operation" , "use" or know-how of any defense article may require a federal license before the access or instruction described above (called the "export") is allowed to occur. Failure to obtain a such a license prior to the export may be illegal and could subject both the university and the violator to crimes and penalties up to and including imprisonment.

Definitions: The following definitions clarify the terminology used throughout this Agreement.

Defense Article (22 CFR §120.6): "Defense article means any item or technical data designated in § 121.1 of this subchapter. The policy described in § 120.3 is applicable to designations of additional items. This term includes technical data recorded or stored in any physical form, models, mockups or other items that reveal technical data directly relating to items designated in § 121.1 of this subchapter. It does not include basic marketing information on function or purpose or general system descriptions."

Defense Services (22 CFR § 120.9): "Defense service means: (1) The furnishing of assistance (including training) to foreign persons, 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 (2) The furnishing to foreign persons of any technical data controlled under this subchapter (see § 120.10), whether in the United States or abroad."

Foreign Person (22 CFR § 120.16): Any persons or entities (including businesses) that are ***not*** a citizen or Permanent Resident Alien (green card visa holder) of the United States (8 USC § 1101(a)(20)) or protected individuals as defined in 8 USC § 1324b(a)(3) (refugees, asylees, or persons in the U.S. under an amnesty program).

Release (15 CFR § 734.2.b.ii): 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 data (22 CFR § 120.10):

6. "Information ... required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of [United States Munitions List regulated] defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions and documentation;... software directly relating to defense articles...includ[ing] but...not limited to the system functional design, logic, flow, algorithms, application programs, operating systems and support software for design, implementation, test, operation, diagnosis and repair.
7. Classified information relating to defense articles and defense services;
8. Information covered by an invention secrecy order;
9. Software ... directly related to defense articles;

10. 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."

Technical Assistance (15 CFR § 772.1): Instruction, skills training, working knowledge, consulting services and other similar forms.

Technical Data: (15 CFR § 772.1): Forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories.

Technology or source code (15 CFR §§ 734.2.b.ii, 772.1): Specific information (or source) code necessary for the "development", "production", or "use" of a product. The information takes the form of "technical data" or "technical assistance". Release of technology on the Commerce Control List requires an export license or other government approval.

Use (15 CFR § 722,1): "Operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing."

CUSTODY, ACCESS AND USE AGREEMENT

Introduction: Although academic research normally is conducted openly and most research activities are not subject to export control regulations, there are certain conditions under which the export of critical technologies, which include certain technical and scientific data, software, or tangible items, is either prohibited by law or requires an export license or other government approval. Such "export control" laws regulate certain transfers of technology and technical data to foreign nationals, either in the U.S. or abroad as well as the physical export of hardware and software.

Controlled Technology: This document establishes guidelines to ensure compliance by the University of Central Florida with federal laws associated with the handling of [quantity, list items, USML category, etc].

Technology Control Statement: [Name], ("Custodian") an employee of the University of Central Florida, is [procuring, on-loan, describe action] [list items, USML category, etc]. To facilitate this activity, the Custodian acknowledges that these defense articles, and all associated technical data and technology, including provisioning or instructing in methods of "use" are export controlled technology, and that all such controlled technologies and related data will require the execution of the attached Custody, Access and Use Agreement to ensure proper handling and safeguarding of everything subject to that Agreement. The defense articles will be in the exclusive possession of the Custodian, and at no time will these [list items, USML category, etc] (as they are controlled defense articles), or technology or data related thereto [list items, USML category, etc] be intentionally or inadvertently transferred from the University of Central Florida, its facilities, labs, staff, researchers, or students to any foreign country or to any foreign person whether at the University of Central Florida or abroad.

Technology Control Requirements:
Custody: Custodians must be official full-time bona fide employees (e.g. faculty members or staff) of the University and cannot be Post Docs, students or visiting scientists. In addition, Custodians must be either a U.S. Citizen, a U.S. Permanent Resident, or a foreign person, who is not a citizen of a country under U.S. Arms Embargo (info pertaining thereto is available at: http://www.pmddtc.state.gov/embargoed_countries/index.html) and such foreign person must possess a Exemption Certificate issued by the UCF Office of Compliance pursuant to 22 CFR § 125.4(b)(10). Defense articles, software and technical data, regardless of medium or whether generated, purchased, obtained or loaned, require special custody measures while on campus due to the presence of foreign persons throughout the academic environment. A Custodian inherently accepts all compliance requirements associated with the defense article.

Access: Defense articles, software, and technical data (including mock-ups and prototypes) must always be secured from unauthorized access. Access must be limited to only U.S. Citizens or U.S. Permanent Residents. Foreign persons are not permitted to visually inspect, operate, use, or access defense articles, software or technical data without a

federally issued license. Rooms/areas that contain export controlled articles or process controlled data must be secure during business hours and locked after close of business. Only users listed as Approved Project Personnel may have key access to the secure project office. Foreign persons are not permitted to access such areas. Access is allowed only to Approved Project Personnel as identified below.

Use: Operation or use of a defense article, even for research or academic purposes, can only be performed by U.S Citizens, U.S. Permanent Residents or full-time regular bona fide UCF employees who are not a citizen of a country under U.S. Arms Embargo who have been issues an exemption certificate by the Office of Compliance pursuant to 22 CFR § 125.4(b)(10). Use includes data analysis, generation, interpretation, or access. Use or operation is allowed only by Approved Personnel for Access and Use as identified below.

Storage. All controlled articles, software, technology and technical data must be secured in a locked room (i.e. secured project office), preferably in a locked storage container therein, when not in the personal possession of the Approved Personnel for Access and Use. Data (soft and hardcopy) must be limited to storage at a single location that is physically safe from access by unauthorized persons at all times. Electronic data must be encrypted. No copies of data or controlled articles, software or technology will be made available except to Approved Project Personnel as identified below. The primary locked storage container location of controlled items is located at: [_____].

Printed Material: Printed material containing export controlled information shall always be secured from unauthorized access (e.g., locked in a secure cabinet within the secure project office when not in use).

Electronic Media: Machine-readable media storage devices will be CD-ROMs or DVD-ROMS. Thumb-drives/flash drives are unallowable and are not permitted as a storage device for technical data relating to a defense article, which may include blueprints, drawings, formulas, lab notebooks, etc. Subject data on machine-readable media shall always be secured from unauthorized access (e.g., locked in a secure cabinet within a secure project office when not in use and only one backup copy thereof can be made).

Marking. Information provided to the university may contain disclaimers or markings. Information, including hard copies generated at the university subject to the ITAR that are not otherwise marked, must be identified and maintained by the Custodian with the following warning:

> WARNING - *This contains 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, as amended, Title 50, U.S.C., App. 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.*

Standalone Desktop Computer: A standalone desktop computer is any single-user PC (e.g., running a Windows operating system). Laptop computers are strictly prohibited. See "No Connections to Another Computer" below for further information. The following are appropriate and suggested security measures for standalone computers processing ITAR-restricted data. Minimum Security Requirements include:

- Laptop computers and thumb drives cannot be used
- Limit access to room/area to approved personnel for access and use
- Passwords must be unique, 6-8 characters with one non-alphanumeric
- Change password at least every 3 months
- Provide read-only access to original data
- Shut down any connections to other computers prior to loading data onto your standalone desktop computer
- Lock your computer and/or the room when away from your computer, or
- Enable automatic "shutdown" on your computer after 3-5 minutes of inactivity
- No routine backups of restricted-use data shall be performed
- Change staff passwords accordingly when staff changes
- Remove data by overwriting at the end of the project or prior to the computer needing repair

Lock Computer and/or Room: When the authorized user is away from the computer, protect the subject data by locking the computer and/or the room. For example, physically lock the computer with its exterior keylock, shut down

the computer and enable its power-on password, or lock the room to prevent an unauthorized individual from gaining access to the computer.

Project Personnel Screening Procedures: Prior to commencement of any work and access to any controlled or other sensitive data all Approved Personnel for Access and Use must:

1. Be formally designated in writing
2. Receive a copy of the attached Custody, Access and Use Agreement, and
3. Sign a copy of the attached Custody, Access and Use Agreement in which the employee acknowledges understanding of the confidential nature of the defense articles, technology and technical data and the safeguards identified in this Agreement to avoid improper disclosure.

Approved Personnel for Access and Use should be limited to only articles and data necessary for performance of duties.

ALL PERSONNEL WITH ACCESS TO DEFENSE ARTICLES, SOFTWARE, TECHOLOGY, AND TECHNICAL DATA MUST SIGN THE "CUSTODY, ACCESS & USE AGREEMENT" found on the last page of this document.

Approved Personnel for Access and Use: This project requires that UCF personnel authorized to access or use defense articles be limited to U.S. Citizens or Permanent Residents or full-time regular bona fide UCF employees who are not a citizen of a country under U.S. Arms Embargo who have been issues an exemption certificate by the Office of Compliance pursuant to 22 CFR § 125.4(b)(10) as follows:

- [Name (Last, First), Employee I.D., Nationality, Citizenship Status]

Custody, Access and Use Agreement: I, [Name], (hereinafter "Custodian") acknowledge and understand that in my capacity as an employee of the University of Central Florida, I am facilitating the transfer of [state nature of controlled articles, i.e. USML defense articles] onto the campus which will be in my care and custody and that such articles and technical data, including "know-how" related thereto (termed a "defense service") are subject to federal laws and regulations, which include without limitation the Export Administration Regulations ("EAR"), the International Traffic in Arms Regulations ("ITAR"), and regulations and orders administered by the Treasury Department's Office of Foreign Assets Control (collectively, "Export Control Laws"). Operation and use of United States Munitions List (USML) defense articles, even in furtherance of academic coursework and research qualifying as "Fundamental Research" by a foreign person, requires federal licensing before access or use pursuant to the ITAR, 22 CFR §120-130.

1. I understand and acknowledge that the data and defense articles involved in this program are subject to United States laws and regulations relating to export control. These defense articles, items, technical data or software will be in the exclusive possession of the Custodian and will not be made available to any foreign person.

2. I understand and acknowledge that export controlled defense articles and technical data are confidential in nature and cannot be disclosed to any person outside of "Approved Personnel to Access and Use Defense Articles, Software and Technical Data" in any manner, (e.g., oral disclosure, electronic, visual access, facsimile message, telephone) whether in its original form, modified, or incorporated in any other form, to any unauthorized person including any third-person without first obtaining the necessary governmental approvals, up to and including licensing

3. I understand and acknowledge that any release of:
   a. "defense article(s)" as that term is defined in 22 C.F.R. § 120.6 of the ITAR,
   b. "technical data" as that term is defined in 22 C.F.R. § 120.10 of the ITAR, or
   c. "defense services" as that term is defined in 22 C.F.R. § 120.9 of the ITAR

   to a foreign person (including a foreign person here in the U.S., e.g. on UCF's campus) is an "export" requiring a federally- issued license or qualification and invocation of a license exception before release and that I will not allow such release unless such release is approved by the UCF Office of Research & Commercialization.

4. I understand and acknowledge that violations of section 38 or 39 of the Arms Export Control Act (AECA), of which the USML is a subpart, are punishable by civil and criminal penalties, including monetary fines and imprisonment. Violations of the ITAR may result in civil fines up to $1,000,000.00 per violation and/or

criminal penalties of up to 10 years imprisonment per violation, or both, pursuant to 22 U.S.C. 2778(c). I understand that I may be personally liable if there is an unlawful release of defense articles, information or software subject to this Agreement to a foreign person without an appropriate export license or other government approval, including allowing a foreign person to operate, visually inspect, or use the defense articles, technology or technical data.

5. I also acknowledge and understand that should I inadvertently receive restricted data for which I have not been granted access authorization or release restricted data to an unauthorized recipient, I will report such unauthorized access or release and acknowledge the transfer to be a violation of U.S. Government regulations.

Acknowledgements:

Custodian:

_____ Date: _____
[Employee Name]
Designated Custodian
[Department]
[University of Central Florida]

Supervisor:

_____ Date: _____
[Supervisor Name]
[Chair or Dean]
[Department/College]
[University of Central Florida]

Approved Personnel to Access and Use Defense Articles, Software and Technical Data
By signing below, I affirm that I have been provided a copy of the Custody, Access and Use Agreement and that I agree to the provisions therein.

Signature: _____ Date: _____
[Type Name of Personnel Authorized Access and Use]

Signature: _____ Date: _____
[Type Name of Personnel Authorized Access and Use]

Signature: _____ Date: _____
[Type Name of Personnel Authorized Access and Use]

Signature: _____ Date: _____
[Type Name of Personnel Authorized Access and Use]

5.5 ECO-5 GOVERNMENT APPROVAL

OFFICE OF RESEARCH & COMMERCIALIZATION

SUBJECT:	**Effective Date:** June 2013	**Guideline Number:** ECO-5
Government Approval Protocol	**Supersedes:** July 2010	
	Responsible Authority: Export Control Officer	

APPLICABILITY
These protocols are applicable to all UCF faculty, staff, students, volunteers and other individuals who possess or may possess export controlled information, classified or unclassified, as defined in and governed by the National Industrial Security Program Operating Manual ('NISPOM"), the International Traffic in Arms Regulations ("ITAR"), the Export Administration Regulations ("EAR"), Office of Foreign Assets Control ("OFAC") Foreign Assets Control Regulations ('FACR") or the Department of Energy Acquisition Regulations ("DEAR"), or other regulations as appropriate that require security protocols

PURPOSE
It is the purpose of these protocols to establish clear government approval procedures for the Office of Export Controls staff to follow to process licenses and other government approvals from the Departments of State and Commerce, including use of certain exemptions and exceptions.

BACKGROUND
Export regulations require that only US persons may be provided with export-controlled items, software code or information without having to obtain an export license. Under certain conditions, an exemption, exception, or exclusion supersedes licensing requirements. Certain exemptions (ITAR) and license exceptions (EAR) available only to higher academic institutions.

The determination of applicability of a license exemption, exception, or exclusion can only be performed by the Export Control Officer ("ECO"), to include application of the "Fundamental Research Exclusion." All license or applications of exemptions are investigated, research, analyzed and concluded by the ECO.

GUIDELINE STATEMENT
The University of Central Florida, Office of Export Control, is the only unit within UCF empowered to process license applications, or qualify an activity for an exemption, exception, or

exclusion pursuant to the ITAR, the EAR, the FACR or the DEAR. Licensing and use of other government must be made in accordance with these procedures.

PROCEDURES

Procedures under this protocol are divided into the following sections:

Department of State:

1. DSP-5 Foreign Person Employee Licenses
2. TAA
3. Exemptions of General Applicability
    a. 125.4(b)(10) Full-time Bona Fide Regular Employee Exemption
    b. Other ITAR Exemptions
4. Initial Notification of Export
5. Return to ODTC of Licenses

Department of Commerce:

6. "Tool of Trade" Exception for Business Travel
7. BIS 748-P

Determination of License

If it is determined that a project or activity requires an export authorization from the cognizant U.S. government agency for international shipments (tangible exports) or foreign national participation (deemed exports) (including faculty, graduate students or foreign entity sponsors) export license applications will be processed pursuant to these guidelines:

1. The ECO will examine the activity and determine if it:
    a. Requires a license, including the jurisdictional analysis, and license type:
        i. State Department License Types:
            1. **DSP 5** Application for Permanent Export of Unclassified Defense Articles.
            2. **DSP 73** Application for Temporary Export of Unclassified Defense Articles.
            3. **DSP 61** Application for Temporary Import of Unclassified Defense Articles
            4. **DSP 85** Classified Defense Articles/Technical Data
            5. **DSP 119** License Amendments
        ii. Commerce Department License:
            1. **BIS 748P** General Export License for the Department of Commerce
    b. Meets the requirements for an exemption (ITAR) or exception (EAR)

License Process (ITAR)

The ITAR controls export of defense articles which are enumerated on the U.S. Munitions List ("USML"). The USML identified technologies that are specially designed for military purposes.

Defense articles include items, components, subcomponents, assemblies, models, mock-ups, technical data and technical information that may reveal technical details about the item. Exports of defense articles require licensing or application of an exemption.

All U.S. persons engaged in the manufacturing or exporting of defense articles, technical data or provisioning of defense services are required to register with the Directorate of Defense Trade Controls. Registration is a precondition to approval of any license application, or utilization of exemptions. UCF is registered with DDTC as a defense manufacturer.

License applications, including exemption certificates must be signed by a university officer who has been empowered by the intended registrant to approve documents. Thomas O'Neal, Doug Backman and Mike Miller have been designated as the empowered officials for UCF and must sign all applications and official correspondence relating to exports under ITAR. The empowered official may refuse to sign any export license or other request for approval without prejudice or any other adverse recourse.

An empowered official will review the proposed scope of work of an activity and make the following determinations:

1. If an activity requires a license, the ECO will furnish the PI with a list of required information needed to begin the application process.

2. If the license is for a foreign person employee/student, Visual Compliance will be used to ensure the person is not a denied entity.

3. The ECO will draft an agreement or license application and review the content material with the PI.

4. If necessary, relevant foreign parties will be consulted for additional information and comments.

5. A TCP will be implemented.

6. The ECO will submit the necessary documentation to the cognizant U.S. government agency

7. License status will be tracked using the U.S. Government Agency system

I. Department of State, Initial Notification of Export License Use

Upon initial use, DDTC requires license notification be furnished. The following memo will accompany the initial use of a license.

PM/DDTC Applicant Code: M25125

[Date]

U.S. Department of State
Directorate of Defense Trade Controls
Office of Defense Trade Controls Licensing
ATTN: Mr. Kevin Maloney, Director
2401 E Street N.W., SA-1, Room H1200
Washington, DC 20522-0112

Subject: Initial Export Notification for DSP-5 License No. [123456789]

Dear Mr. Maloney:

Pursuant to 123.22(b)(3), this letter serves as notification to DDTC of the initial export of technical data against the above referenced DSP-5 license for the operation of a Category [XXX] defense article.

Upon completion of operation of the defense article, the original license will be returned to the ODTC.

Under penalty according to federal law (22 CFR 127.2; 22 USC 2278; 28 USC 1001) I, Michael Miller, as authorized by the University of Central Florida, warrant the truth of the statements made herein.

If you have any questions or concerns regarding this letter, please contact the undersigned at (407) 882-0660 or by email at Michael.Miller@ucf.edu

Sincerely,

Michael Miller
Export Control Officer
Empowered Official

II. Department of State, Return of Licenses

Upon use or expiration, DDTC requires licenses be decremented and returned. The following memo will accompany the license.

[Date]

Kevin Maloney, Acting Director
Office of Defense Trade Controls Licensing

Directorate of Defense Trade Controls
2401 E St., N.W., 12th Floor
Washington, DC 20037

PM/DDTC Code: M25125

Subject: Return of DSP-5 License Number [123456789]

Dear Mr. Maloney:

Pursuant to 123.22(c)(3) Enclosed please find the above referenced DSP 5 license. Then explain why you are returning the license. Use any that apply:

This license is no longer needed because (explain).

This license has expired.

And if the license was never decremented, then make that statement as well. "This license was never used".

If you have any questions or concerns regarding this letter, please contact the undersigned at……

Under penalty according to federal law (22 CFR 127.2; 22 USC 2278; 28 USC 1001) I, Michael Miller, as authorized by the University of Central Florida, warrant the truth of the statements made herein.

If you have any questions or concerns regarding this letter, please contact the undersigned at 407-882-0660, or by email at Michael.Miller@ucf.edu

Sincerely,

Name
Empowered Official

Attachments:
1. License

III. Exemptions of General Applicability

As a general policy, UCF will utilize exemptions only on a very limited basis. Applicability and use of all ITAR exemptions will only be made by the Export Control Officer. Use of exemptions must comply with all requirements specified in the ITAR, to include Sections 125.4:

- Eligibility to use exemptions is conditional upon UCF's continued registration with DDTC

- Exemptions cannot be used to allow export, including the provisioning of defense services, to any foreign person who is a citizen of, or was born in a Proscribed Destination: http://www.pmddtc.state.gov/embargoed_countries/index.html
- The following use of exemptions are unallowable: classified transmissions, offshore procurement arrangements (e.g. international collaborations)
- Use of exemptions must be documented

1) 125.4(b)(10) Exemption for Full-time Bona Fide Employees of U.S. Institutions of Higher Learning for Disclosures of Unclassified Technical Data

(10) 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:

> (i) The employee's permanent abode throughout the period of employment is in the United States;
>
> (ii) The employee is not a national of a country to which exports are prohibited pursuant to § 126.1 of this subchapter; and
>
> (iii) 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 Directorate of Defense Trade Controls;

ITAR 125.4(b)(10) Explanation:
This exemption exempts from ITAR licensing requirements the disclosure 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 if the person's permanent abode through the period of employment is in the U.S., the person is not a national of a country to which exports are prohibited, 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 ODTC.

Regular employee is defined in the ITAR as:

> (1) An individual permanently and directly employed by the company, or
>
> (2) An individual in a long term contractual relationship with the company where the individual works at the company's facilities, works under the company's direction and control, works full time and exclusively for the company, and executes nondisclosure certifications for the company, and where the staffing agency that has seconded the individual has no role in the work the individual performs (other than providing that individual for that work) and the staffing agency would not have access to any controlled technology (other than where specifically authorized by a license).

Applicability of Exemption:

UCF will only use this exemption under very specific conditions.

- This exemption is only available for university employees
- This exemption is not available for any of the following:
    - Students, including Graduate Research Assistants and Graduate Teaching Assistants,
    - Volunteers,
    - Part-time employees,
    - Other employees not receiving benefits, as these are not "regular" employees
    - Appointed faculty that are not being paid
    - Any foreign person attending UCF on a F-1 or J-1 visa, regardless of tax withholdings
- This exemption is specific to release/disclosure of unclassified technical data. It does not allow the transfer of defense services. Defense services require a separate license.
- The exemption does not allow for access to tangible defense articles.
- Supervisors of employees utilizing this exemption must be informed of the use. If necessary, the supervisor may be a signatory on the exemption certificate

Documentation of Invocation of Exemption (Exemption Certificate)

The following record shall be used to record provisioning of the 125.4(b)(10) exemption:

BONA FIDE EMPLOYEE LETTER

Applicable to UCF employees who are exempt from ITAR export control restrictions as a Bona Fide Employee of the University

PM/DDTC Applicant Code: M25125
USML Category: [enter category]

Dear [Foreign National Employee Name]:

This is a certification of the exemption claim to provide United States Munitions List (USML) unclassified technical data in the U.S. by a U.S. institution of higher learning to a foreign person (you as the employee) without a license pursuant to the International Traffic in Arms Regulations (ITAR) codified at 22 Code of Federal Regulations (CFR) §§ 120-130. Pursuant to 22 CFR § 125.4(b):

> "The following exports are exempt from the licensing requirements of this subchapter …(10) 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."

Pursuant to 22 CFR § 125.4(b)(10), as a bona fide employee of the University of Central Florida, whose permanent abode throughout the period of employment is in the United States and who is not a national of a country to which exports are prohibited pursuant to 22 CFR § 126.1, you are hereby exempt from the requirement of obtaining a Department of State Publication (DSP) foreign national worker license. Although you, as a bona fide

employee are exempt from licensing, all non-bona fide foreign national employees, researchers, collaborators and students **require** licensing.

You are hereby notified that as _____ (participant/principal investigator) in the Sponsored Project for _____(name of project) you will be producing ITAR export control restricted experimental or developmental electronic equipment or equipment specifically designed or modified for military application or specifically designed or modified for use with a military system and associated technical data. The date, time, and method of transmission to you is as follows:_____. The description of the unclassified technical data is as follows:_____ _____.

In accordance with 22 CFR § 125.4(b)(10)(iii), ITAR-restricted defense articles or technical data may not be transferred to foreign persons without the prior written approval of the Directorate of Defense Trade Controls. Prohibited technical transfer includes oral, visual, written or electronic disclosure, as well as transfer of physical custody. Pursuant to 22 United States Code (USC) § 2778(c) and (e), violations of ITAR can result in criminal penalties of up to 10 years in prison and/or up to $1 Million in fines per violation, and civil penalties of up to $500,000 in fines and forfeiture per violation. Therefore, this exemption does not permit you to transfer any ITAR-restricted defense articles or technical data to **any** foreign national within or outside of the United States.

Under penalty according to federal law (22 CFR § 127.2; 22 USC § 2778; 18 USC § 1001) I, Michael J. Miller Jr., as authorized by the University of Central Florida, warrant the truth of the statements made herein.

If you have questions about this export control restriction, please contact Michael Miller (407) 882-0660 from our office.

This certificate will be retained for five years pursuant to ITAR 22 CFR § 122.5(a) and § 123.26. Additional information is available on the Export Compliance website at: http://www.research.ucf.edu/ExportControl/

Sincerely,

_____

Michael J. Miller Jr.
Export Controls Officer
Office of Research & Commercialization

Acknowledgement:

[Name]

Rev-2, 1/29/2010

IV. Use of Other ITAR Exemptions

The ITAR employs various other exemptions to the licensing requirements that permit the export and import of articles, technical data, and defense services pursuant to specific conditions. Final determination with respect to the applicability of these exemptions must be made on a case-by case basis by the Export Control Officer pursuant to examination of the Issue, Rule, Analysis of Situation to Rule, Conclusion ("IRAC").

V. Use of EAR Exceptions

The most common EAR exception used is the "Tool of Trade" exception, which is used for travel or transmissions to destinations outside the U.S. of commodities required to conduct routine business, such as a laptop, certain software, cellphone, etc.

The exception requires:

- The destination cannot be to a sanctioned country (Cuba, Iran, Sudan, Syria, North Korea)
- Use of the "Tool of Trade" exception must be documented on a certificate,
- Equipment and data cannot be on the International Traffic in-Arms (ITAR) U.S. Munitions List (USML) (e.g. DoD Sponsored project articles or data not in the public domain),
- Equipment and data must be in the "effective control" of the traveler for the duration of the trip and cannot be released,
- Equipment and data cannot be out of the U.S. for longer than 12 months.

Equipment not Qualifying:

- Agents, toxins, microorganisms, pathogens, chemicals or nuclear technologies,
- High end GPS units,
- Defense articles listed on the ITAR U.S. Munitions List (USML).
- Non-standard cryptography technology and software, (non-mass market software), "open cryptographic interface" technology or "cryptanalytic (code-breaking)" technology

Data

Remove the following types of data from a laptop before departure as they do not qualify for the "Tool of Trade" exception:

- Proprietary technical data not intended for public distribution, such as sponsored research with access, publication, or participation restrictions,
- Technical data relating to the development, production, or use of a commodity listed on the EAR Commerce Control List (CCL),
- Data relating to any military sponsored project or defense articles on the ITAR U.S. Munitions List (USML).

Traveling with Non-University Equipment

License Exception BAG (Baggage) allows US citizens to carry family-owned retail-level items including laptops, personal digital assistants (PDAs), and cell phones as personal baggage. The items and software must be for their personal use.

Tool of Trade Certificate

"TOOL OF TRADE" EXPORT LICENSE EXCEPTION (TMP) CERTIFICATION for Export Administration Regulations (EAR) controlled Items, Technology, and Software

To: Mike Miller, Export Controls Officer, Office of Research & Commercialization
From: [*Insert Name of PI or Employee*]
Date: [*Insert Date*]
Re: **Export License Exception for Temporary Exports/Reexports* per 15 CFR 740.9(a)(2)(i)**

The export of items, technology, commercial software, and encryption code is subject to export control regulations (this includes laptops, PDAs and digital storage devices). The Export Administration Regulations (EAR) makes an exception to licensing requirements for the temporary export or reexport of certain items, technology, or software for professional use as long as the criteria to which you are certifying below are met. The exception does not apply to any EAR satellite or space-related equipment, components, or software, or to any technology associated with high-level encryption products. In addition, this exception does not apply to items, technology, data, or software regulated by the Department of State's International Traffic in Arms Regulations (ITAR).

Detailed Description of Items, Technology or Software to which this Certification applies:
[*Insert description of items you will be carrying abroad here*]

By my signature below, I certify that:

1. I will ship or hand-carry the items, technology, or software to [*insert country(s)traveling to*] as a "tool of the trade" to conduct official university business only;

2. **I will return the items, technology, or software to the US on** [*insert return date*] **which is no later than 12 months from the date of leaving the US** unless the items, technology, or software are certified by me to have been consumed or destroyed abroad during this 12 month period;

3. I will keep the items, technology, or software under my "effective control" while abroad (defined as retaining physical possession of item or keeping it secured in a place such as a hotel safe, a bonded warehouse, or a locked or guarded exhibition facility);

4. I will take security precautions to protect against unauthorized release of the technology while the technology is being shipped or transmitted and used abroad such as:
    a. use of secure connections when accessing e-mail and other business activities that involve the transmission and use of the technology,
    b. use of password systems on electronic devices that store technology, and
    c. use of personal firewalls on electronic devices that store the technology;

5. **I will not ship or hand-carry the items, technology or software to Iran, Syria, Cuba, North Korea, or Sudan without consulting with the Office of Research & Commercialization, Export Control Officer.**

6. I will consult with the Office of Research and Commercialization before taking/sending other University of Central Florida equipment or specialty software abroad (other than my laptop computer and its operating system software, PDA, or cell phone).

Signed: _____

[*Name of PI/Employee*]

Keep a signed copy with you when traveling abroad

5.6 ECO-6 RESTRICTED PARTY SCREENING

OFFICE OF RESEARCH & COMMERCIALIZATION

SUBJECT:	**Effective Date:** October 2013	**Guideline Number:** ECO-6
Restricted Party Screening Protocol	**Supersedes:** October 2012	
	Responsible Authority: Export Control Officer	

APPLICABILITY
These protocols are applicable to all UCF faculty, staff, students, volunteers and other individuals.

PURPOSE
It is the purpose of these protocols to establish procedures for the Office of Export Controls staff, and other UCF personnel, to follow to conduct Restricted Party Screens ("RPS"). Restricted Party Screening ensures UCF does not engage in an unlawful transaction or restrictive trade practice with a debarred or restricted entity prior to and during the duration of any type of business transaction, including providing services or collaboration.[7]

U.S. exporters are prohibited from conducting export related business with parties subject to denial orders (i.e., parties listed on the Department of Commerce, Denied Persons List ("DPL"), parties specified on the Department of Treasury, Specially Designated Nationals List ("SDN") or Specially Designated Terrorists List ("SDT"), or parties subject to Department of State proscription, suspensions or debarments). This prohibition includes intra-country transfers abroad of U.S. origin goods and technology and the servicing of a denied party's U.S. origin items. In order to prevent business with such denied parties, UCF uses a current list of these parties against which it screens customers, suppliers, consultants, and other business partners. An auditable record indicating that the DPL screening has been performed is maintained by the ECO on any document, database or list that is screened.

BACKGROUND
Various U.S. Government agencies maintain a number of lists (Appendix 1) of individuals, parties, corporations, entities institutions, governments, etc. that are debarred, suspended, blocked, declared ineligible or otherwise restricted from entering into certain types of transactions with U.S.

[7] Business transaction includes all type of business arrangement, whether procurement or non-procurement based, charitable, non-financial, volunteer, collaboration, service of value or any other type of transaction where one party does something on an official basis with the university or a representative thereof.

persons, including universities. A party or entity designated on a federal list may be subject to a variety of federal prohibitions or other regulatory requirements of which UCF is obligated to comply.

UCF utilizes the e-Customs "Visual Compliance" system to conduct mandatory restricted party screening of over 50+ US government restricted party lists. These lists include export-related restricted, denied and blocked persons and munitions export-related restricted, denied and blocked persons, and sanctioned countries.

Screening involves database searches for key words, specifically, names, organizations, vendors, suppliers, etc. to ensure that no foreign nationals on any government "watch" lists, sanctioned or embargoed country are associated with a UCF research contract.

All potential RPS alerts are investigated, research, analyzed and concluded by the ECO.

GUIDELINE STATEMENT

Various units throughout UCF conduct RPS to ensure UCF does not engage in a transaction with an unallowable entity. All companies, entities, affiliates or persons (etc.) are required to be screened before the commencement or continuation of the business relationship. Parties are added to and removed from various restriction lists daily. Should an entity with whom the university has an existing relationship be added to a federal list, UCF is required to comply with the regulatory requirements imposed on the entity regardless of the type, value or duration of the relationship.

PROCEDURES

UCF must "qualify" and annually review entities with a business affiliation to ensure they are not "enumerated "on any restricted list at this or any future time. UCF, under a statewide license, uses Visual Compliance to expedite screening of multiple federal lists. This software consolidates the multiple lists including daily updates while simultaneously re-screening previously screened entities.

I. Identification of Business Relations:

Sponsored Programs, Purchasing, Finance and Accounting and Export Control personnel should screen all organizations or companies (including any subcontractors or independent contractors) as well as any individuals (internal or external to UCF) that will be involved in the transaction or collaboration or otherwise working on the research project. The following are representative examples of a "business relationship" that require screening:

- Parties involved in a business relationship with the university, for example: individual, corporation, partnership, firm, association, trust, estate, public or private institution, Nation, State, political entity or subdivision, foreign government, national agency, instrumentality, End-user, sub-recipient, parent, subsidiary, affiliate, individual, company, government or department (e.g. Ministry of Energy, Atomic Energy Commission, etc).
- Specially Designated Nationals: individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-

specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs."

- Practices: Any transaction involving petroleum, diamonds, human trafficking.
- Foreign involvement and collaborations, including involvement of any country listed as a state sponsor of terrorism or on a State Department Warning list.

II. Visual Compliance (Access, Use)

Account Request and Set-up

New accounts and modifications are managed by the Export Compliance Officer. User training and instructions are provided by E-Customs in the document titled "RPS Guide."

III. Visual Compliance (Restricted Party Screening)

Step 1. Enter the Name, company or person information on the party being screened (obtained from the Subaward Commitment Form). Include as much information as possible, including the address. If key pieces of information are not available, contact the party to request additional information that will enable a search. For domestic and international transactions, select the appropriate Country. **NEVER CONDUCT A SINGLE WORD SEARCH!!!!!**

Note: for foreign research institutions, enter the university, lab, or institution name in the "Company" field. All positive alerts require resolution by the Export Compliance Officer. A listing of these institutions is available at:
http://www.bis.doc.gov/policiesandregulations/ear/744_supp4.pdf

Step 2. In the "Comment" section, enter in the applicable reference information. A unique identifier that allows the master file or record to be obtained in the long-term future is required. This should be the Research ID Number, Account Number, Vendor ID, Number, etc. Examples:

- Reference No. (Research ID / PI / College)
- Consultant (Vendor ID / PI / College)

Step 3. For US parties, use the "Exact" match. For Non-US parties, use the "Fuzzy Level 3" match.

IV. Negative Match

Screens resulting in a negative match will read in red "No Matching Records Found." Print this page as a PDF and hardcopy. The PDF is uploaded into ARGIS / Tera as a "Restricted Party Screen – No Match." The hardcopy goes into the project file.

V. Positive Alert / Suspect

Screens resulting in anything other than a "No Matching Records Found" require additional due-diligence. Forward all screens to the Export Compliance Officer for guidance if any of the following conditions apply:

- Unknown match
- Conflicting match
- Possible positive match / alert

It is better to treat potential matches as a "red-flag" and either resolve the question, refrain from the transaction, or seek a federal license, depending upon the nature of the debarment.

Individual / Corporate / Consultant / Affiliate / Collaborative Matches from a GSA list are verified using the Excluded Party Listing Service / System for Award Management verification process. These are the only matches Sponsored Programs can independently verify without seeking assistance from the Export Compliance Officer.

Using EPLS, conduct a basic or advanced search. Obtain all applicable information (i.e. Cause / Treatment Codes, Reciprocal Codes, Procurement / Non-Procurement Codes, Agency Contact information, etc.). If necessary, contact the designated federal official for the listing agency to obtain additional information that enables UCF to independently verify if the party involved in the UCF transaction is the excluded party listed in EPLS. If the match is not verified, print all documents and proceed with the transaction.

Logging into SAM at: https://www.sam.gov/portal/public/SAM/ conduct a records search using the DUNS Number, CAGE Code or Business Name, obtained from the Subaward Commitment Form. Conduct a search using the system. Obtain all applicable information (i.e. Debarred status, Agency Contact information, etc.). If necessary, contact the designated federal official for the listing agency to obtain additional information that enables UCF to independently verify if the party involved in the UCF transaction is the excluded party listed in SAM. If the match is not verified, print all documents and proceed with the transaction.

If EPLS or SAM cannot be used to verify a person / company/ entity, etc. contact the Export Compliance Officer for a TLO search.

If there is a positive match, please contact the Export Compliance Officer for a TLO search.

Prior to taking any further actions, users are to consult the requirements of the specific list on which the company, entity or person is identified by reviewing the webpage of the agency responsible for such list.

Print and PDF a copy of the search for the file.

Appendix 1
Federal Screening List Authorities

Export-related Restricted, Denied, and Blocked Persons Lists

- Department of Commerce Denied Persons [BIS]
- Department of Commerce Entity List [BIS]
- Department of Commerce "Unverified" List [BIS]
- Department of State Arms Export Control Act Debarred Parties [DDTC]
- Department of State Nonproliferation Orders

    - Executive Order 13382
    - Iran and Syria Nonproliferation Act
    - Executive Order 12938, as amended
    - Missile Sanctions Laws
    - Chemical and Biological Weapons Sanctions Laws
    - Sanctions for the Transfer of Lethal Military Equipment
    - Iran, North Korea, and Syria Nonproliferation Act Sanctions (INKSNA)
- Department of State Munitions Export Control Orders [DDTC]
- Weapons of Mass Destruction Trade Control Designations [OFAC]
- Department of State Designated Terrorist Organizations
- Department of State Terrorist Exclusion List
- U.S. Treasury Department Palestinian Legislative Council List [OFAC]
- U.S. Federal Register General Orders

Sanction Programs-related Blocked Persons Lists

- U.S. Treasury Department Specially Designated Nationals and Blocked Persons, including Cuba and Merchant Vessels, Iran, Iraq and Merchant Vessels, Sudan Blocked Vessels [OFAC]
    - Department of Treasury Specially Designated Terrorist Organizations and Individuals
    - Department of Treasury Specially Designated Narcotic Traffickers and Narcotics Kingpins
    - Department of Treasury Foreign Narcotics Kingpins
- United Nations Consolidated List
    - U.N. sanctions measures (assets freeze, travel ban, or arms embargo) imposed by the Security Council on individuals and entities under Security Council Resolutions 751 (1992) and 1907 (2009) concerning Somalia and Eritrea, 1267 (1999) and 1989 (2011) concerning Al-Qaida and associated individuals and entities, 1518 (2003), 1521 (2003) concerning Liberia, 1533 (2004) concerning The Democratic Republic of the Congo, 1572 (2004) concerning Côte d'Ivoire, 1591 (2005) concerning The Sudan, 1718 (2006), 1737 (2006), 1970 (2011) concerning Libya, 1988 (2011), and 2048 (2012) concerning Guinea-Bissau.

General Services Administration

- U.S. General Services Administration List of Parties Excluded from Federal Procurement Programs [SAM/EPLS]
- U.S. General Services Administration List of Parties Excluded from Federal Nonprocurement Programs [SAM/EPLS]
- U.S. General Services Administration List of Parties Excluded from Federal Reciprocal Programs [SAM/EPLS]

Law Enforcement-related Wanted Persons Lists

- Air Force Office of Special Investigations - Top Ten Fugitives

    - Focuses on four priorities: to exploit counterintelligence activities for force protection, to resolve violent crime impacting the Air Force, to combat threats to Air Force information systems and technologies, and to defeat and deter acquisition fraud.
- Bureau of Alcohol, Tobacco, Firearms and Explosives Most Wanted
    - Enforces U.S. federal laws and regulations relating to alcohol, tobacco products, firearms, explosives, and arson.
- FBI Ten Most Wanted Fugitives
    - Investigative functions fall into the categories of applicant matters, civil rights, counterterrorism, foreign counterintelligence, organized crime/drugs, violent crimes and major offenders, and financial crime.
- FBI Most Wanted Terrorists
    - Lists alleged terrorists that have been indicted by sitting Federal Grand Juries in various jurisdictions in the United States for the crimes reflected on their wanted posters.
- FBI Wanted Fugitives
- FBI Crime Alert
- FBI Seeking Information
- Food and Drug Administration – Clinical Investigators
- Food and Drug Administration – Disqualified and Restricted
- Food and Drug Administration – Debarment List
    - Individuals that have had various restrictions placed against them by the Food and Drug Administration (FDA) for scientific misconduct.
- Department of Homeland Security Most Wanted Fugitive Criminal Aliens
    - Persons wanted on Administrative Orders of Removal from the United States.
- Naval Criminal Investigative Service - Wanted Fugitives
    - Conducts felony criminal investigations and counterintelligence for the Department of the Navy, and managing Navy security programs.
- Immigration and Customs Enforcement Most Wanted Fugitives
    - Investigates fugitive matters involving escaped federal prisoners, probation, parole, and bond default violators, and warrants generated DEA investigations and certain other related felony cases.
- U.S. Drug Enforcement Administration - Major International Fugitives
    - Enforces controlled substances laws and regulations of the United States and brings to the criminal and civil justice system of the United States those entities and individuals involved in the growing, manufacture, or distribution of controlled substances appearing in or destined for illicit traffic in the United States.
- U.S. Marshals Service - Top 15 Most Wanted
- U.S. Marshals Service - Major Fugitive Cases
    - Involved in most every federal law enforcement initiative. U.S. Marshals major cases and top 15 most wanted consist of individuals with a history of violent crimes who may be considered armed and dangerous.
- Office of Research Integrity Administrative Actions
    - The names of individuals that have had administrative actions imposed against them by the Office of Research Integrity (ORI), maintained by the Public Health Service (PHS). The Assistant Secretary for Health (ASH) makes the final PHS decision on

findings of research misconduct and the imposition of administration actions after reviewing the recommendations made by ORI.

- U.S. Postal Inspection Service - Most Wanted
    - Important areas of jurisdictions include: assaults, bombs, controlled substances, electronic crimes, mail fraud, and money laundering.
- U.S. Secret Service - Most Wanted
    - The United States Secret Service is mandated to carry out two missions: protection and criminal investigations. In criminal investigation, the Secret Service is responsible for the enforcement of laws relating to counterfeiting of obligations and securities of the United States, investigation of financial crimes including, but not limited to access device fraud, financial institution fraud, identity theft, computer fraud, telecommunications fraud, and computer based attacks on our nation's financial, banking, and telecommunications infrastructure.

Politically Exposed Persons and Office of Inspector General

- Chiefs of State and Cabinet Members of Foreign Governments [Central Intelligence Agency]
- Office of Inspector General List of Individuals/Entities Excluded from Federal Health and Medicare Programs

International Terrorist, Blocked Person, Wanted, and Entity Lists

- European Union Consolidated List
- Interpol Recently Wanted
    - Lists persons that are wanted by national jurisdictions.
- Japan Foreign End-Users of Concern
- Kingdom of Saudi Arabia Wanted Militants
- Canada Public Safety and Emergency Preparedness Listed Entities
- Australia Foreign Affairs Consolidated List
- Bank of England [HM Treasury] Consolidated List
- Canadian Border Services Agency Wanted List
    - Violations of human or international rights under the Crimes Against Humanity and War Crimes Act or under international law.
- RCMP Wanted Fugitives
    - Enforces laws made by, or under, the authority of the Parliament of Canada.
- World Bank Listing of Ineligible Firms
    - Lists names of firms and individuals that are ineligible to be awarded a World Bank-financed contract for the periods indicated because they were found to have violated the fraud and corruption provisions of the Procurement Guidelines or the Consultants Guidelines.
- OSFI Consolidated List - Entities
- OSFI Consolidated List - Individuals
    - Office of the Superintendent of Financial Institutions (OSFI) issues names subject to the regulations establishing a list of entities made under the Canada Criminal Code or the United Nations suppression of terrorism regulations. OSFI is the sole regulator

of banks, and the primary regulator of insurance companies, trust companies, loan companies and pension plans in Canada.

- OSFI Warning List
    - Issues entity names that may be of concern to the business community and the public.

Export Risk Country Alerts

- Department of Commerce, EAR Part 736 General Prohibition Three (Foreign-produced direct product re-exports)
- Department of Commerce, EAR Part 736 General Prohibition Eight (In transit shipments and items to be unladen from vessels or aircraft)
- Department of Commerce, EAR Part 740, Country Group E:1, Terrorist Supporting Countries
- Department of Commerce, EAR Part 744, Subject to military end-user and end-use based control policy for specified ECCN dual-use items
- Department of Commerce, EAR Part 746, Embargoes and Other Special Controls (embargoes, sanctions, or special controls on specified items)
- Department of State, U.S. Arms Embargoes
- Department of State, Restricted export destinations under the ITAR (126.1) including denial policy
- Department of State, DDTC policy restrictions, limitations, or delays on license applications for the export of USML items
- Department of State, State Sponsors of Terrorism
- Department of State, Countries Not Cooperating Fully with United States Antiterrorism Efforts
- Department of Treasury Office of Foreign Assets Control (OFAC) Sanctions
- United Nations (UN) Sanctions
- BIS India and Pakistan Export Restrictions, including Atomic Energy blocked entities
- Exports and reexports under restriction to Afghanistan
- Countries that may require participation in, or cooperation with, an international boycott [Section 999(b)(3) of the Internal Revenue Code of 1986]

RPS List Reference Acronyms

- AFA · Australia Foreign Affairs Consolidated List
- AFI · AFOSI – Top Ten Fugitives
- ATF · ATF Most Wanted
- BEC · Bank of England Consolidated List
- CBS · Canadian Border Services Agency Wanted List
- CPS · CPSEP Listed Entities
- DBP · AECA Debarred Parties [DDTC]
- DEA · U.S. DEA Major Fugitives

- DOR · U.S. Federal Register General Orders
- DPL · Denied Persons List [BIS]
- DTO · Designated Terrorist Organizations
- ELT · Entity List [BIS]
- EUC · European Union Consolidated List
- FCA · FBI Crime Alert
- FDA · FDA – Clinical Investigators
- FDL · FDA – Debarment List
- FDR · FDA – Disqualified and Restricted
- FSI · FBI Seeking Information
- FTF · FBI Ten Most Wanted Fugitives
- FWF · FBI Wanted Fugitives
- FWT · FBI Most Wanted Terrorists
- ICE · ICE Most Wanted Fugitives
- IRW · Interpol Recently Wanted
- JFE · Japan Foreign End-Users of Concern
- MEO · Munitions Export Control Order [DDTC]
- MSF · U.S. Marshals Service – Fugitives
- MSW · U.S. Marshals Service Most Wanted
- MWC · Homeland Security Most Wanted Fugitives
- NEL · GSA Excluded Parties – Nonprocurement
- NPO · Nonproliferation Orders
- NWF · NCIS Wanted Fugitives
- OCE · OSFI Consolidated List – Entities
- OCI · OSFI Consolidated List – Individuals
- OIG · OIG List of Excluded Individuals/Entities
- OWL · OSFI Warning List
- PEL · GSA Excluded Parties – Procurement
- PEP · Chiefs of State and Cabinet Members of Foreign Governments
- PHS · PHS Administrative Actions Listing
- PIS · U.S. Postal Inspection Service
- PLC · Palestinian Legislative Council List [OFAC]
- REL · GSA Excluded Parties – Reciprocal
- RWF · RCMP Wanted Fugitives
- SDN · Specially Designated Nationals and Blocked Persons [OFAC]
- SSW · U.S. Secret Service Most Wanted
- SWM · Kingdom of Saudi Arabia Wanted Militants
- TEL · Terrorist Exclusion List
- UNC · United Nations Consolidated List
- UNV · Unverified List [BIS]
- WBL · World Bank Listing of Ineligible Firms
- WMD · WMD Trade Control Designations [OFAC]

5.7 ECO-7 DENIED ENTITY

OFFICE OF RESEARCH & COMMERCIALIZATION

SUBJECT:	**Effective Date:** October 2013	**Guideline Number:** ECO-7
Denied Entity Protocol	**Supersedes:** June 2012	
	Responsible Authority: Export Control Officer	

APPLICABILITY
These protocols are applicable to all UCF faculty, staff, students, visiting scholars, volunteers and other individuals.

PURPOSE
It is the purpose of these protocols to establish procedures for the Office of Export Controls staff, and other UCF personnel, to follow to distinguish allowable conduct with denied entities from unallowable conduct, based upon U.S. regulations.

U.S. exporters and entities within the U.S. are prohibited from conducting export related business with parties subject to denial orders (i.e., parties listed on the Department of Commerce, Entity List). Export-related business includes, but is not limited to:

- International travel to entity institutions or meeting with persons on the entity list, whether in the US or abroad
- International recruitment of faculty, staff, students or researchers affiliated with an entity
- Hosting visiting Scholars, including furnishing a visa, or hosting someone in the US on a tourist visa
- Research or educational collaborations, in the U.S. or abroad
- Financial transactions
- Commercial consulting or provisioning of services
- Providing assistance or know-how related to technologies subject to the EAR or the ITAR

BACKGROUND

Sponsoring or Collaborating with a Foreign Person Affiliated with a Listed Entity:
Certain foreign persons – including businesses, research institutions, universities, government and private organizations and other types of legal persons –may be subject to specific federal prohibitions, including prohibitions on research collaborations, for a variety of reasons and require

specific licensing, even for educational exchange and are specified on the Entity List available at: http://www.bis.doc.gov/policiesandregulations/ear/744_supp4.pdf A complete list of all entities on the Entity List is available at: http://www.bis.doc.gov/index.php/forms-documents/doc_download/15-entity-list

License requirements and federal review policies vary for each university on the Entity List, some permit the export of certain technologies, while others require licensing for all technologies. The federal government has a policy of denial for certain entities. It is important for you to review the Entity List and understand compliance responsibilities and limitations before collaborating, or sponsoring an employee, visiting scholar or student of a university listed therein. In certain circumstances, UCF has no alternative but to prohibit certain activities or deny a visa request. The government has issued specific guidance pertaining to such activities at: http://www.bis.doc.gov/entities/entitylistfaq.html#28

All potential collaborations with Denied Entities are investigated, research, analyzed and concluded by the ECO.

GUIDELINE STATEMENT

Colleges and Departments throughout UCF conduct international fundamental research and pursue research collaborations with a variety of scientists throughout the world. UCF will not engage in transactions with a denied entity in any manner not allowable by law. UCF should make no attempt to travel to, collaborate with, or internationally recruit at any entity on the Entity List. UCF is required to comply with the regulatory requirements imposed on the entity regardless of the type, value or duration of the relationship.

PROCEDURES

All entities involved in all transactions, whether research collaborations, international exchange programs, or other activities must (1) be allowable entities, and (2) must meet export requirements as detailed in the International Traffic in Arms Regulations ("ITAR"), the Export Administration Regulations ("EAR"), Office of Foreign Assets Control ("OFAC") Foreign Assets Control Regulations ('FACR") or the Department of Energy Acquisition Regulations ("DEAR"), or other regulations as appropriate that require security protocols.

Certain collaborations, based upon the field of specialization and research portfolio of a UCF employee, may require U.S. Government export approvals for transfer of any item, material, technical know-how or technology in any manner to any denied entity, comprehensively embargoed country, or other prohibited party or individual.

"Entities" are placed on the Commerce Department's Entity List based on a review by the Departments of Commerce, Defense, and State when determined that "there is reasonable cause to believe, based on specific and articulable facts, that the entity has been involved, is involved, or poses a significant risk of being or becoming involved in activities that are contrary to the national security or foreign policy interests of the United States and those acting on behalf of such entities

may be added to the Entity List pursuant to this section." (15CFR 744.11(b)) Denied entities include targeted foreign countries, governments, regimes, businesses, persons, denied parties and other entities that engage in activities contrary to the national security or foreign policy interests of the U.S. Government.

Any entity, including its faculty, employees, or students is ineligible to receive any items subject to the EAR without a specific export license to the extent specified in the Entity List supplement. The embargo is comprehensive for most entities. UCF is prohibited from exporting any items, software, or technology subject to the EAR to a denied entity subject to Export Administration Regulations (EAR) without an export license- licenses will be evaluated on a case by case basis by the Commerce Department. *See* 15 CFR 744.1(c).

Certain foreign civilian universities and research institutes have a direct partnership with foreign militaries and defense industries to improve the development of foreign military technologies. Such entities are enumerated in the Entity List. Examples of educational institutions on the Entity List include, but are not limited to:

- Sichuan University (China)
- Northwestern Polytechnical University (China)
- Beihang University / Beijing University of Aeronautics and Astronautics (China)
- University of Electronic Science and Technology of China (China)
- Chinese Academy of Engineering Physics (China)
- Ben Gurion University (Israel)
- Pakistan Atomic Energy Commission, National Development Centre (Pakistan)

Analysis of Proposed Activities
Proposed activities that involve entities on the Denied Entity List will be reviewed for the following:

Employees:
Commercial Item and Data Access An **employee or Post doc** of a university listed on the Denied Entity List would require licensing for participation on sponsored programs that involve technologies on the USML or CCL, and the license may be denied. Employees of denied entities also require licenses for a UCF employee to instruct how to maintain, repair, operate, integrate, overhaul and refurbish any items subject to the EAR, including unspecified (EAR99) items and all associated technical data. Therefore, all employees, officers, trustees or other persons in a similar position representing a denied entity are prohibited from accessing any items, technology, and data subject to the EAR including items generated as a result of (1) fundamental research that involve equipment subject to the EAR, or (2) proprietary research, or (3) any research that is not intended to be placed in the public domain (such as sponsored research with trade secret information or any information not in a patent).

Defense Article Item and Data Access Federal law prohibits any export of a defense article and any associated technical data, including "mere operation" or "visual inspection" of a defense article by any foreign person (employee or student or visitor) without a license or qualification for an exemption. This is regardless of the setting (i.e. in a laboratory). All foreign persons who were born

in any country subject to a U.S. Arms Embargo are prohibited from obtaining licenses or qualifying for exemptions (see http://www.pmddtc.state.gov/embargoed_countries/index.html). This is applicable to any military research subject to restriction (i.e. access, publication, dissemination or participation restrictions) or restricted research.

Students:
Former and Current Students from an entity list university are considered a "red flag" requiring additional due diligence. The federal government states that a student (as opposed to employee) is not an integral part of a university and are therefore excluded from the licensing requirements and policy specific to the "denied entity." Therefore, unlike employees and post docs, students are permitted to participate in research activities not subject to the EAR (such as fundamental research) that utilize or require the "operation" of export controlled devices providing that the overall sponsored research:

1. is not subject to access, publication, participation or dissemination restrictions pursuant to 15 CFR § 734.8 or otherwise involve any proprietary or trade secrets as any of these elements corrupt the "fundamental research exclusion";

2. does not support (including providing any educational assistance including classroom instruction) in any nuclear, missile, chemical or biological weapons activities;

3. does not involve the transfer of know-how or providing a service that will directly assist in the design, development, production or use of any type of missile technology, such as machine tools used to develop parts for missiles or unmanned aerial vehicles;

4. requires only "operation" of research equipment without releasing required information for the development, production, or use of any equipment subject to the EAR;

5. does not involve U.S. Munitions' List (USML) defense articles, technical data or defense services including instruction.

Former Students Foreign persons who were once students at an entity list university, when no longer affiliated with the university are permitted to collaborate so long as the collaboration qualifies as fundamental research or public domain in accordance with the above guidance.

Current Students Foreign persons who are currently from an entity list university are considered a "red flag" requiring additional due diligence, but are allowed to come to UCF as a student and work on fundamental research projects that do not include anything "proprietary" in accordance with the above guidance. There may be other restrictions on the type of research work they can perform. This must be reviewed on a case-by-case basis upon the time of the filing of the visa by the ECO.

Pertaining to overseas research collaborations: Educational exchange for research that is intended to be published, or that is not proprietary or restricted is allowable if it does not involve a

listed entity. Such research is subject to the "Corporate Research" requirements of the EAR (*See* 15 CFR 744.11).

> (1) Research conducted by scientists or engineers working for a business entity will be considered "fundamental research" at such time and to the extent that the researchers are free to make scientific and technical information resulting from the research publicly available without restriction or delay based on proprietary concerns or specific national security controls as defined in §734.11(b) of this part.
>
> (2) Prepublication review by the company solely to ensure that the publication would compromise no proprietary information provided by the company to the researchers is not considered to be a proprietary restriction under paragraph (d)(1) of this section. However, paragraph (d)(1) of this section does not authorize the release of information to university researchers where the research results are subject to prepublication review. (See Supplement No. 1 to this part, Questions D(8), D(9), and D(10).)
>
> (3) Prepublication review by the company solely to ensure that prepublication would compromise no patent rights will not be considered a proprietary restriction for this purpose, so long as the review causes no more than a temporary delay in publication of the research results.
>
> (4) However, the initial transfer of information from a business entity to researchers is not authorized under the "fundamental research" provision where the parties have agreed that the business entity may withhold from publication some or all of the information so provided.
>
> (e) Research based elsewhere. Research conducted by scientists or engineers who are not working for any of the institutions described in paragraphs (b) through (d) of this section will be treated as corporate research, as described in paragraph (d) of this section. (See Supplement No. 1 to this part, Question D(8).)

International research involving a denied entity requires additional due-diligence. Collaboration, including travel to collaborate with a denied entity outside of the U.S. has specific license requirements and exclusions typically do not apply. The government has a policy of denial for licensing many of these entities.

Violations

Presently, violations of the EAR may be subject to both criminal and administrative fines and penalties pursuant to the International Emergency Economic Powers ("IEEPA") Enhancement Act 50 U.S.C. §§1701 - 1706 (2000) and include up to $1,000.000 and 20 years imprisonment for criminal acts and $250,000 per violation in administrative penalties. In May 2013, the University of Massachusetts at Lowell was fined $100,000 in connection with an unlicensed export to a denied entity. See http://www.dlexports.com/pdfs/UMass-Lowell-violation.pdf

INTENTIONALLY BLANK

5.8 ECO-8 DEEMED EXPORT ATTESTATION

OFFICE OF RESEARCH & COMMERCIALIZATION

SUBJECT:	**Effective Date:** October 2013	**Guideline Number:** ECO-8
Deemed Export Attestation Protocol	**Supersedes:** June 2011	
	Responsible Authority: Export Control Officer	

APPLICABILITY
These protocols are applicable to all UCF faculty, staff, students, visiting scholars, volunteers and other individuals.

PURPOSE
Although academic research and scholar activities are normally conducted openly and are not subject to federal limitations on performance, there are certain conditions under which the sharing, transmission or the "export" of critical technologies with a foreign person whether in the U.S. or abroad may be either prohibited by law or require a federally-issued export license or other U.S. government approval. Such "export control" laws regulate certain transfers of technology, technical and scientific data, know-how, software or tangible items to foreign nationals, either in the U.S. or abroad as well as the physical export of hardware and software. Sponsoring faculty must be aware of their obligations as well as the U.S. export laws, regulations and sanctions. UCF faculty, staff, students and visiting foreign persons must comply with such regulations.

The administrative process to review and approve foreign scholar, scientists or guests includes a technical examination pursuant to federal regulations of:

1. Proposed activities of the visiting foreign person (including academic, sponsored and unsponsored research)
2. The research activities of the U.S. sponsor
3. Research instrumentation and equipment involved in the sponsors research activities that may be accessed by the visiting scholar
4. Applicable regulatory requirements imposed by the U.S. Government on any of the above.

BACKGROUND

Export control laws and regulations seek to ensure that foreign nationals are not inappropriately granted access to controlled or sensitive information, including information that under U.S. law may not be transferred to foreign entities or persons without a license. This type of material is generally referred to as "export controlled information." The process of ensuring that export control

restrictions are followed requires cooperation and collaboration between researchers and export control professionals.

GUIDELINE STATEMENT

No foreign national may be given access to a UCF facility, IT system or labs until completion of an export control assessment and a favorable access determination by UCF export control personnel. Foreign persons cannot participate in sponsored program activities while on UCF property pending completion of the assessment and favorable determination by UCF export control officials. UCF policy requires the implementation of security protocols for technology transfer to outline the foreign national's approved access to UCF facilities and information.

The technology control protocols for international visitors set the general parameters of a foreign national's access to UCF facilities and IT systems. As part of the plan, a UCF employee is designated as the host or sponsor of the foreign national and charged with taking all reasonable measures to prevent the disclosure of inappropriate information to foreign persons. Specifically, unless the foreign national has received an export license, a sponsor is permitted only to share information that is unclassified, non-sensitive, non-proprietary or non-export controlled or that has been approved for release to the general public.

Hosts/sponsors are required to (1) be trained to host international visitors and (2) brief foreign nationals on the contents of the technology control plan for international visitors and ensure that co-workers in the area in which the foreign national will work are aware of his or her status and the restrictions on the foreign national's access to certain information.

PROCEDURES

Process Narrative

The process begins with submission of a visa request to the International Services Center and completion of all DS-2019 materials. Part of this package includes the requestor completing the "Questionnaire for Sponsoring a Foreign Scholar, Scientist, Visitor or Guest." The requestor enters basic personal information about the foreign national, the anticipated activities, research equipment to be used, and any other UCF personnel who will be involved in the activities. The completed questionnaire must accompany a recent resume. The completed DS-2019 package is routed and reviewed by the Office of Export Controls.

Export control personnel review requests from "designated technical areas" to ensure:

(1) That all information furnished is valid and complete,
(2) That no foreign national or entities are affiliated with a denied party or entity, on the terrorist watch list, or from a country under U.S. sanctions or embargo, and
(3) That proposed activities are consistent with applicable U.S. foreign policy, agreements, and laws related to the country of citizenship of the visitor.

Once these checks are complete, export control personnel will make a licensing determination regarding the activities of the foreign person which considers the type of work, and the information and technology to which the foreign national will have access or generate. If needed, the Office of Export Controls can apply for a license on behalf of foreign persons. If no license is required, a

final assessment memo listing all regulatory requirements will be issued stating the necessary technology control protocols, conditions or "provisos" that will apply to the foreign national's visit to ensure compliance with federal law. For example, the foreign national may be required to be escorted at all times when he or she is within certain labs. These provisos are selected from a pre-set list developed by the Office of Export Controls.

A final copy of the assessment with all final security determinations will be sent to the sponsor/host for subsequent acknowledgement and signature. The message will also contain information about the provisos export control personnel have placed on the foreign national's visit. A copy of the assessment must be provided to all UCF parties who may have contact with the foreign person in order that they are briefed on the assessments proviso requirements. The sponsor/host is required to furnish a copy of the assessment and review the contents with the foreign person.

General:

- Note, there are different attestation requirements depending on visa type. H-1B must have a formal written attestation for all beneficiaries before the I-129 can be submitted by ISC. J-1 are only required for technical colleges and are not required as part of the visa application.

- Certain colleges and research centers have different special deemed export requirements, such as the College of Medicine and AMPAC due to the use/presence of hazardous materials. Others have specific review requirements for HPC, encryption or certain equipment.

- Each attestation requires a back-up of all documentation made to determine the license requirement, including notes.

- It is important to recognize that a questionnaire is part of a packet of required visa forms. When routed to ORC, the package has already been in process by other UCF departments for up to two weeks. Therefore attestations should be completed as soon as possible because the Immigration Advisor will delay submitting the visa until the ORC attestation is complete.

- UCF Export Compliance I-129 website: http://www.research.ucf.edu/ExportControl/I-129.html

Procedure

1. Upon initial receipt of a questionnaire, it must immediately be logged onto the Export Compliance Log and tracked until completion.

2. Conduct a cursory review of the completed questionnaire for completeness. Return any incomplete questionnaire or wrong version of the form to the submitter and ISC Immigration Advisor as necessary.

3. Conduct analytical review for responses marked "yes" or "unknown." Responses marked "no" should not conflict with any other information gathered during the review process.

4. Acquire specific contractual documents and statements of work from all referenced Projects/Account numbers using ARGIS.

5. Print and review current faculty/staff "Proposal & Awards Listing" in ARGIS. Look for any DoD, NASA, or defense industry -funded or possible ITAR projects. These must be specifically listed in the attestation.

6. Ensure all research projects qualify as fundamental research.
    a. No access, participation, publication or participation restrictions
    b. If a license is required, coordinate meeting with sponsor to review licensing protocols.
    c. If no license required, document findings on template.

7. Telephone Sponsor or coordinator if more information is required.

8. Screen Beneficiary name and institution/entity using RPS software. Print results.

9. If on entity list, refer to protocol "Sponsoring or Collaborating with a Foreign Person Affiliates with a Listed Entity"
    a. Authorize the denied entity or deny the entity depending upon legal criteria

10. Compile information as obtained into Deemed Export Attestation letter (Form ECO-8.4).
    a. Print, sign and scan completed letter

11. Distribute the attestation letter as follows (Form ECO-8.3):
    a. For H-1B visas – email the attestation letter to the following:
        i. ISC Representative
        ii. Faculty/Sponsor
        iii. Immigration Legal Counsel
        iv. Department Coordinator or Beneficiary (or direct Coordinator to forward on to beneficiary)
    b. For J-1 or all other visa types:
        i. ISC Representative
        ii. Faculty/Sponsor
        iii. Department Coordinator or beneficiary (if known)
        iv. ORC Staff

Primary Contacts:

H-1B

Georgiana DeBoer
Employment and Taxation Coordinator
International Services Center
Ph: 407.823.1851 | Fax: 407.823.2526

Em: Georgiana.Deboer@ucf.edu

Jason Kennedy
Assistant Director
Employment & Taxation
International Services Center
P: 407-823-5491 | F: 407-823-2526
Em: Jason.Kennedy@ucf.edu

J-1

Daren Caine
Coordinator, Academic Support Services
International Services Center
Ph: 407-823-1852 or 407-823-2337
Em: daren.caine@ucf.edu

Fragomen, LLP:
MLeviste@Fragomen.com
ABlumberg@Fragomen.com
YLeon@Fragomen.com

QUESTIONNAIRE FOR SPONSORING A FOREIGN SCHOLAR, SCIENTIST, VISITOR or GUEST

Follow instructions completely or your form will be unable to be processed. If you have any questions, contact the Office of Research & Commercialization, Export Control Officer at 407-882-0660

All questions on this form must be answered completely and truthfully in other that UCF may make legal and regulatory determinations. Civil and criminal penalties may be associated with inaccurate or false statements that lead to violations of federal law.

Purpose of this Questionnaire
Although academic research and scholar activities are normally conducted openly and are not subject to federal limitations on performance, there are certain conditions under which the sharing, transmission or the "export" of critical technologies with a foreign person whether in the U.S. or abroad may be either prohibited by law or require a federally-issued export license or other U.S. government approval. Such "export control" laws regulate certain transfers of technology, technical and scientific data, know-how, software or tangible items to foreign nationals, either in the U.S. or abroad as well as the physical export of hardware and software. Sponsoring faculty must be aware of their obligations as well as the U.S. export laws, regulations and sanctions. UCF faculty, staff, students and visiting foreign persons must comply with such regulations.

The administrative process to review and approve foreign scholar, scientists or guests includes a technical examination pursuant to federal regulations of :

5. Proposed activities of the visiting foreign person (including academic, sponsored and unsponsored research)
6. The research activities of the U.S. sponsor
7. Research instrumentation and equipment involved in the sponsors research activities that may be accessed by the visiting scholar
8. Applicable regulatory requirements imposed by the U.S. Government on any of the above.

Regulations:

- Export Administration Regulations (EAR), 15 CFR 700 - 799
- International Traffic in Arms Regulations (ITAR), 22 CFR 120 - 130.
- U.S. Sanctions and Embargoes.

Procedures:

a. Download and complete the "Request to Sponsor a Foreign Scholar, Scientist or Guest" form to the best of your ability. All finalized forms must be signed by the sponsor. Your completed form will be used to make legal decisions with potential civil and criminal liabilities.
b. Submit the completed form along with the CV/Resume of the foreign person along with the completed DS-2019 package to the UCF International Services Center (ISC). ISC does not perform the export compliance assessments.
c. Packages are reviewed by ISC for completeness. Incomplete packages or those that do not use the current version of all forms cannot be processed by ISC and will be rejected.
d. Packages meeting required review criteria are forwarded to the Office of Research & Commercialization, Export Control Officer (ECO) for comprehensive assessment. ISC will not process DS-2019 without verification that ORC has completed the export control assessment.
e. In certain circumstances based upon the information provided, a summary and assessment of export control compliance findings will be issued to the UCF sponsor. The sponsor is required to comply with all provisios of the assessment.
f. Final assessments are NOT BOILERPLATE.

SECTION 1. BIOGRAPHICAL

1. UCF Host (faculty)
2. UCF Visa Sponsor (if other than Host)
3. Department
4. Department Administration Point of Contact (other than Host or Sponsor)
5. Full Name of Foreign Person
6. Date of Birth
7. Country of Birth
8. Last Country of Residence
9. Country of Citizenship
10. Home Address
11. Current Institution(s) / Employer(s) (list all)
12. Status/position/title at Home Institution or Employer
13. Intended immigration status (e.g. J-1 visiting scholar, H-1B, F-1, etc.)
14. Were any of the foreign person(s) previously affiliated with UCF? If yes, explain.
15. Are the proposed activities of the foreign person(s) part of an official UCF international program, such as a scientific mobility program or research experience for undergraduates program? If yes, please specify the program.
16. Is this research or activities part of an official academic catalog course? If yes, please list the exact course.
17. Is the foreign person(s) currently employed by, serving in, or on leave from, any foreign military? If yes, specify country and branch of military:
18. Is the foreign person(s) currently employed by or on leave from any foreign Government agency If yes, please specify the country and agency.
19. Is the foreign person(s) receiving funding from a foreign source for the U.S. visit or for the activity they will participate? (e.g. is the visitor being paid by a foreign source to work for you for free?) If yes, specify the source of funding (ex. institution, organization, scholarship, government scholarship fund, etc.).

SECTION 2. ACTIVITIES

20. In detail, specify the assignment, purpose and proposed activity(ies) of the foreign person. This must be a comprehensive explanation.
21. Will the foreign person participate in or work on any Sponsored Research activity? If yes, provide the UCF project account(s) or Research ID of all projects they may participate in, or be afforded access to (this is not a Grant Number).
    a. Will the results of the sponsored activity be published in totality or taught in an official UCF course or otherwise shared with the interested public? If yes, provide a reference or example as to where the research or instruction can be found in the public domain.
22. Will the sponsored activity consist entirely of basic or applied research, the results of which are commonly found entirely in the public domain?
23. Will the foreign person assist any other UCF co-worker, faculty or staff in addition to the host/sponsor? If so, identify each individual the foreign person will assist.
24. Will the foreign person (You must affirm and answer these questions regardless of whether they apply):
    a. Be provided access to any unpublished, proprietary or confidential information, items, materials, software, prototypes or articles furnished by a sponsor? Yes, No and Describe your response.
    b. Contribute to any research program sponsored by the Department of Defense, NASA, Energy or other defense industry sponsors, including SBIR or STTR, or U.S. defense industrial base flow-thru awards? Yes, No and Describe your response.
    c. Does the sponsored activity or research have any potential military, space or intelligence application? Yes, No and Describe your response.
    d. Is the sponsored activity subject to any access or dissemination, or national security restriction? Yes, No and Describe your response.
    e. Will any of the activities be related to the development of a new or emerging technology? Yes, No and Describe your response.
    f. If yes, will any portion be withheld to protect proprietary or confidential information ? Yes, No and Describe your response.

SECTION 3: RESEARCH INSTRUMENTATION ACCESS & USE

25. Will the foreign person(s) have access to or be operating any research instruments?
    a. If yes, specify all of the research instrument(s):
26. Will the foreign person(s) be provided instruction in how to develop, produce or use (operate, installation, maintenance, repair, overhaul and refurbishing) the research instruments.
27. If a sponsored activity, does the sponsor have any proprietary technology or technical data related to the development, production or use (operate, installation, maintenance, repair, overhaul and refurbishing) of any proprietary item, article, device or software? Such technology and technical data is commonly subject to an non-disclosure, confidentiality or material transfer agreement.
    a. If yes, will the foreign person(s) be allowed access to the sponsor proprietary or technical data, or materials? If yes, specify the technology or technical data.
28. Will the foreign person be exposed or allowed to access any UCF proprietary technology or technical data? If yes, specify the technology or technical data.
29. Will the foreign person be conducting any research or experiments in university labs? If yes, specify the lab.
30. Are any lab areas shared with other UCF researchers? If yes, specify which researchers.

SECTION 4. OTHER ASSURANCES

31. Does the UCF host/sponsor currently have any programs subject to export controls, Technology Control Plans or US government security classification?
    a. Will the visiting foreign person be contributing in any way to any programs subject to a TCP or other US government restriction?
32. NASA Restrictions on Funding activities with China or any Chinese-owned Company. Grant Information Circular (GIC 12-01) restricts researchers accepting NASA funding from allowing any collaborator or visiting scholar to participate in NASA funded research activities when the scholar is affiliated in any way with the Government of China or a Chinese-owned company. This restriction applies to students, student interns, visiting scholars or professors (even on a volunteer basis) who retain an affiliation with a Chinese institution of higher learning or the Government of China, or receive any international funding from the Chinese State while they are in the U.S. or abroad. Is the foreign person:
    a. Affiliated with the Government of China as a student, intern, visiting scholar, employee (faculty, staff, lecturer, researcher, etc.) even on a volunteer basis or in the US on sabbatical? This includes professors with joint appointment, Chinese company representatives, or Chinese government entity, and all others that receive scholarships or other types of funding from the Chinese Government.
    b. A Non-Chinese researchers performing research for China, such as other U.S. researchers acting on behalf of a Chinese University or corporation?
    c. Will the proposed visiting foreign person participate in any NASA-funded activity?
33. Dissertation Assurance:
34. Encryption Assurance
35. High Performance Computer Assurance

SECTION 5. CERTIFICATION

Sponsoring UCF Faculty:

Name of person completing form:

Department:

Department Contact for Administrative Matters:

Certification:
To the best of my knowledge, I certify that the information provided herein is accurate and truthful.

Additional Comments: _____
_____

Please contact the Office of Research & Commercialization, Export Control Officer at (407) 882-0660 should you require assistance. Additional information for hiring foreign nationals is available on the Export Compliance website at: http://www.research.ucf.edu/ExportControl/I-129.html

Background

Export control laws and regulations seek to ensure that foreign nationals are not inappropriately granted access to controlled or sensitive information, including information that under U.S. law may not be transferred to foreign entities or persons without a license. This type of material is generally referred to as "export controlled information." The process of ensuring that export control restrictions are followed requires cooperation and collaboration between researchers and export control professionals.

No foreign national may be given access to a UCF facility, IT system or labs until completion of an export control assessment and a favorable access determination by UCF export control personnel. Foreign persons cannot participate in sponsored program activities while on UCF property pending completion of the assessment and favorable determination by UCF export control officials. UCF policy requires the implementation of a security protocols for technology transfer to outline the foreign nationals approves access to UCF facilities and information.

The technology control protocols for international visitors sets the general parameters of a foreign national's access to UCF facilities and IT systems. As part of the plan, a UCF employee is designated as the host or sponsor of the foreign national and charged with taking all reasonable measures to prevent the disclosure of inappropriate information to foreign persons. Specifically, unless the foreign nationals has received an export license, a sponsor is permitted only to share information that is unclassified, non-sensitive, non-proprietary or non-export controlled or that has been approved for release to the general public.

Hosts/sponsors are required to (1) be trained to host international visitors and (2) brief foreign nationals on the contents of the technology control plan for international visitors and ensure that co-workers in the area in which the foreign national will work are aware of his or her status and the restrictions on the foreign national's access to certain information.

Export Control Review Process for International Visitors

The "Questionnaire for Sponsoring a Foreign Scholar, Scientist, Visitor or Guest" is designed to contain all information needed to review and approve a foreign national's access request including the technology control plan for international visitors.

The process begins with submission of a visa request to the International Services Center and completion of all DS-2019 materials. Part of this package includes the requestor completing the "Questionnaire for Sponsoring a Foreign Scholar, Scientist, Visitor or Guest." The requestor enters basic personal information about the foreign national, the anticipated activities, research equipment to be used, and any other UCF personnel who will be involved in the activities. The completed questionnaire must accompany a recent resume. The completed DS-2019 package is routed and reviewed by the Office of Export Controls.

Export control personnel review requests from "designated technical areas" to ensure: (1) that all information furnished is valid and complete, (2) that no foreign national or entities are affiliated with a denied party or entity, on the terrorist watch list, or from a country under U.S. sanctions or embargo, and (3) that proposed activities are consistent with applicable U.S. foreign policy, agreements, and laws related to the country of citizenship of the visitor.

Once these checks are complete, export control personnel will make a licensing determination regarding the activities of the foreign person which considers the type of work, and the information and technology to which the foreign national's will have access or generate. If needed, the Office of Export Controls can apply for a license on behalf of foreign persons. If no license is required, a final assessment memo listing all regulatory requirements will be issued stating the necessary technology control protocols, conditions or "provisos" that will apply to the foreign national's visit to ensure compliance with federal law. For example, the foreign national may be required to be escorted at all times when he or she is within certain labs. These provisos are selected from a pre-set list developed by the Office of Export Controls.

A final copy of the assessment with all final security determinations will be send to the sponsor/host for subsequent acknowledgement and signature. The message will also contain information about the provisos export control personnel have placed on the foreign national's visit. A copy of the assessment must be provided to all UCF parties who may have contact with the foreign person in order that they are briefed on the assessments proviso requirements. The sponsor/host is required to furnish a copy of the assessment and review its' contents with the foreign person.

Possible Provisos

- No international hand-carry of any laptops, pda, memory-stick, external portable hard drive or other devices. Only IT equipment approved by the Export Control Officer for use outside the United States may be taken on international travel.
- No access to any proprietary computer files
- No copying of any UCF proprietary or sponsored program materials
- Sponsors are required to consult with UCF export control staff prior to allowing access or exports of such devices, materials, information and technical data
- The visitor shall be escorted at all times.
- With escort, no computer access to any UCF domain. Laptop access to a guest Wi-Fi internet connection authorized for purposes, such as checking email.
- Approved access is limited to information in the public domain; no access to classified, sensitive but unclassified, or export-controlled information or hardware is authorized.
- The visit is authorized only so long as there is a valid visa in effect.
- Copies of the visit approval provisos/conditions are to be provided by the UCF host to all UCF employees, on-site contractor employees and students working with this foreign person.
- The visit is approved based on no cost to UCF; payment of stipends/expenses against a grant, contract or agreement is not authorized.
- Host is to confer with the Office of Export Controls to determine export classification of data and hardware to be accessed prior to visit.
- A non-disclosure agreement is required for this assignment.
- A Security/Technology Control Plan must be in place and approved prior to this visit due to restricted programs of the host/sponsor
- Release of software source code is not authorized. Only access and dissemination of computer code that is in the public domain is authorized.
- The PI shall coordinate the decision to make this project fundamental research with the Export Control Officer and will document the decision; a copy should be kept by the [Export Control Officer and PI
- The U.S. employer of the foreign person, [name of employer], is responsible for compliance with U.S. export control laws and regulations and for seeking an appropriate license if required; UCF host should be apprised of these provisos and is responsible for informing the employer of this proviso.

5.9 ECO-9 RESTRICTED DISSERTATIONS

OFFICE OF RESEARCH & COMMERCIALIZATION

SUBJECT:	**Effective Date:** November 2014	**Guideline Number:** ECO-9
Restricted Dissertations	**Supersedes:** June 2014	
	Responsible Authority: Export Control Officer	

APPLICABILITY
These protocols are applicable to all UCF faculty, staff, students, visiting scholars, volunteers and other individuals.

PURPOSE
Students voluntarily choosing to undertake thesis/dissertation topics subject to publication restrictions or export controls must include provisions that are compliant with Graduate Studies academic requirements, those of the sponsor and federal law.[8] Concomitantly, these provisions must also enable a student to fulfill all academic requirements while still publishing the work. This may be accomplished by:

(1) Predefining research that is outside the scope of the subject agreement (e.g. treatments or measurements that are not of a sensitive nature), or
(2) Sanitizing (e.g. "writing around") the restricted scope, or
(3) Controlling the research while it is taking place in accordance with federal laws and obtaining approval to publish the results from either the sponsor, or cognizant federal approval agency, or both, as required.

Compliance measures must allow the student to fulfill the academic requirements for his/her degree, in the event the sponsor imposes restrictions as defined in the subject agreement. If the work is sanitized, it must have sufficient scholarly merit to demonstrate the student's ability to do independent research of high quality and meet the expectations for a significant contribution to knowledge in the field.

UCF POLICY
UCF requires that graduate students be able to publically disseminate and publish the results of thesis and dissertations within a specified and approved timeframe (usually six months, with a possible six month extension for patent or proprietary concerns) pursuant to College of Graduate

[8] The International Traffic in Arms Regulations (ITAR) codified at 22 Code of Federal Regulations (CFR) §§ 120-130, and the Export Administration regulations codified at 15 Code of Federal Regulations (CFR) §§ 300 – 799.

Studies Policy: http://www.students.graduate.ucf.edu/policy/ETD_Dissemination/. However, there are certain circumstances when UCF may consider approving a student engaging in restricted research, the results of which may be part of a thesis or dissertation. The policy includes a requirement that all patent and proprietary issues be resolved before publications are disseminated. Any delay must be approved and agreed by the advisor.

BACKGROUND

The above referenced research includes terms and conditions that permit the sponsor to reject, edit, or otherwise restrict proposed publications or limit participation or access to certain data. The acceptance of these restrictions is outside of normal University policy for the performance of thesis/dissertation research, which is intended to be "publically available." The graduate advisor and members of the advisory committee must recognize that in the case of graduate degree programs for which a thesis or dissertation is the required culminating experience, academic policies require review and approval by the student's committee, a public presentation of the work (in the case of doctoral students) and submission of the final approval document to the University Library, available for public access. However restricted research programs, such as those subject to publication restriction, may affect or limit one if not all of the above requirements. Therefore due diligence should be exercised when identifying topics for graduate student research that include sensitive/classified or otherwise restricted information (e.g. projects subject to export controls) since compliance with federal law may have a chilling effect on publication, committee participation, and public defense of the body of the work.

GUIDELINE STATEMENT

A thesis or dissertation submitted for an advanced degree at the university must not contain information that is subject to restriction. Examples of restricted information include classified, proprietary and export controlled materials, including data, results, methods or other content.

It is important to note that these restrictions do not apply to non-thesis or non-dissertation research that is approved by the student's advisor and allowed by UCF policies. Questions regarding the applicability of this policy or thesis or dissertation content should be referred to the College of Graduate Studies and the Export Compliance Officer, Office of Research & Commercialization.

Should a student choose to participate in an export controlled activity, any resulting information may be used in a thesis or dissertation only after approval for unlimited public release or dissemination by the appropriate regulatory agency. Students desiring to include export controlled technology in their thesis/dissertation will be required to work with their graduate advisor and Export Compliance Officer to develop a Technology Control Plan (TCP) and modify an existing TCP regarding how all degree requirements will be met while preventing unauthorized exports of controlled technology. The TCP must be submitted to the graduate advisor, Dissertation Advisory Committee and College of Graduate Studies for approval. Following approval, the secure research may take place in accordance with TCP requirements. The work cannot be published or released to anyone outside the Dissertation Advisory Committee until such time as written approval is obtained by the sponsor and cognizant federal approval agency (if applicable).

PROCEDURES

Graduate students assigned to research projects with publications restrictions or subject to export controls (whether related to the student's thesis/dissertation work project or not) must be made aware of the nature and extent of all restrictions applicable to the project, and confirm their awareness and willingness to comply by signing the enclosed "Memorandum of Understanding" (MOU).

Due to the restrictive nature of these types of controlled research , the following conditions must be met:

- All participants, advisor(s) and members of the review committee must be either U.S. Citizens or Permanent Residents.
- All work (i.e. methods, lab notebooks, posters, etc.), including related publications and presentations, must **NOT** be disseminated to anyone outside of the pre-approved advisory team.
- All draft-publications **CANNOT** be distributed to anyone not a member of the review committee. Publications cannot be further disseminated by members of the review committee, even for peer-review.
- The portion of a thesis/dissertation defense containing restrictive research must be closed to the general public until such time as the content has been approved for public release in writing by the sponsor or cognizant federal regulatory agency.
- These procedures and other federal regulatory requirements are summarized in a "Technology Control Plan" coordinated by the Office of Research & Commercialization, Export Compliance Officer.

In similar manner, due to the fundamental academic principle that degrees are conferred by the university faculty, all defenses of doctoral dissertations and masters theses must be made in a public forum at which all faculty can attend and test the hypotheses and ability of the student to defend the research. , , Therefore the following minimum conditions must also be met;

- The student can conduct restricted research but must publically defend his/her dissertation or thesis using either non-restricted data or by sanitizing the restricted elements in the research. In recognition of the unique nature of this research, the defense may include both a public and a closed portion. The public portion must be comprehensive enough so that the public can understand and challenge the research, ascertain the quality of the work, and ascertain the ability of the candidate to defend the work. The closed portion may only include advisory committee members and representative(s) of the Academic College and/or the Graduate College who will ascertain the ability of the candidate to defend the restrictive elements of the work. It is suggested that the student and the advisor in concert with the funding agency preview the public presentation to sanitize the restrictive elements prior to the defense.
- The entire dissertation may be embargoed in the UCF library with no public access for up to five years but all parties must recognize that after this time the dissertation or thesis will be released to the Florida Virtual Library at which point it will be made available to the public.
- In cases where either of the above conditions cannot be made, the restricted research cannot be included in the dissertation or thesis.

Memorandum of Understanding
for the
Performance of Restricted Thesis / Dissertation Research

College:

Department:

Graduate Student Researcher:

Principal Investigator:

Graduate Advisor (if different than PI):

Advisory Committee Members:

Topic/Title:

Sponsored Program (if applicable):

Memorandum of Understanding: I understand that acceptance of access, dissemination, publication or participation restrictions on thesis/dissertation research is outside of normal UCF Policy. In accepting the subject restricted activity, all parties agree to comply with the necessary restriction measures as detailed in the Technology Control Plan (TCP) until such time as approval for public release is granted. It remains the responsibility of the Academic Advisor and the Dissertation Advisory Committee to ensure that all graduate students will be able to publish a final version of the thesis/dissertation under consideration. In fulfillment of that responsibility, I hereby confirm that:

1. I am aware that restricted research is subject to federal law, the violation of which may include criminal and civil penalties, up to and including a prison sentences of up to 10 years and fines of up to $1M per violation.
2. The sponsor reserves the right to restrict proposed publications. I understand these provisions and accept them without change. .
3. I agree to comply with access and dissemination restrictions associated with this restricted coursework and will not redistribute copies of data or publications nor allow a foreign person's access. I will keep all such information in a secure area.
4. I will return or destroy all copies of all restrictive data and publications related to this thesis/dissertation unless approved for public release with 24 months from date of completion.
5. The Graduate Student, Graduate Advisor and members of the Dissertation Advisory Committee have had ample time to discuss the above restrictions and make necessary contingency plans that would allow the student to meet his/her academic requirements in

the event publication restrictions are imposed that would otherwise impact the thesis/dissertation.

6. I understand that a public defense of the student's dissertation or thesis is required using either non-restricted data or by sanitizing the restricted elements in the research. I also understand that the defense may consist of a public and a closed portion. The public portion must be comprehensive enough so that the public can understand and challenge the research, ascertain the quality of the work, and ascertain the ability of the candidate to defend the work. The closed portion may only include advisory committee members and representative(s) of the Academic College and/or the Graduate College who will ascertain the ability of the candidate to defend the restrictive elements of the work. It is suggested that the student and the advisor in concert with the funding agency preview the public presentation to sanitize the restrictive elements prior to the defense.
7. I understand that the entire dissertation may be embargoed in the UCF College of Graduate Studies with no public access for up to five years but all parties must recognize that after this time the dissertation or thesis will be released to the extent permitted by law to the Florida Virtual Library and the UCF Library at which point it will be made available to the public.
8. In cases where either of the above conditions cannot be made, the restricted research cannot be included in the dissertation or thesis.

GRADUATE STUDENT APPROVAL:

_____ _____

Name (Type or Print) Signature Date
Graduate Student

PI APPROVAL:

_____ _____

Name (Type or Print) Signature Date
Principal Investigator

ADVISOR(S) APPROVAL:

_____ _____

Name(s) (Type or Print) Signature Date
Advisor

COLLEGE APPROVAL

_____ _____

Name (Type or Print) Signature Date
Dean, College of Graduate Studies

5.10 ECO-10 INTERNATIONAL TRAVEL

OFFICE OF RESEARCH & COMMERCIALIZATION

SUBJECT:	**Effective Date:** May 2012	**Guideline Number:** ECO-10
International Travel	**Supersedes:** Original	
	Responsible Authority: Export Control Officer	

APPLICABILITY
These protocols are applicable to all UCF faculty, staff, students, visiting scholars, volunteers and other individuals.

PURPOSE
UCF faculty, staff or students traveling internationally as part of their UCF roles must be aware that there are Federal, State of Florida, and UCF Policies that may apply to their travel. The level or restriction, as well as the process of review, will vary depending on the destination, purpose or type of activity (e.g., attending a conference, field research, study abroad) and funding entity. Travel outside the United States can trigger the need for a federally-issued license(s), depending on the proposed destination, what you plan on taking with you, the nature of the project associated with the travel, and with whom you will be working.

BACKGROUND
Travel requests are reviewed by UCF Finance and Accounting ("F&A"). Travel to a location under a U.S. State Department Travel Warning requires adherence to UCF Policy 2-903 "Travel to Restricted Destinations." Such requests are identified and flagged by F&A. F&A will send instructions, copy of the Preliminary Approval for Restricted Travel Form and other information to the traveler. Upon completion, the forms are submitted to the Office of Internationalization. The Office of Internationalization will forward the forms to the appropriate compliance offices for additional review. The Office of Export Controls receives all travel requests.

GUIDELINE STATEMENT
UCF travelers need to comply with United States export statutes and regulations anytime equipment, devices, computer software or technical data are exported, including by being hand carried, on a trip outside of the country. Certain sponsored programs may be subject to federal law that requires government approval or licensing before exporting equipment, research data or performing research abroad. This can include the hand carrying of items that have both commercial and military or proliferation applications, proprietary information, or items that are considered defense articles, even if used in an academic or research environment. Such items may include data, software or technology, blueprints, design plans, field data, equipment and retail software packages and technical information.

PROCEDURES
Export control review of travel is required under the following circumstances:

- UCF Policy 2-903 "Travel to Restricted Destinations" requires export compliance review of travel to any location of which the U.S. Department of State has issued a Travel Warning.
- Travel associated with sponsored programs subject to restriction
- Travel with university-owned equipment
- Travel to any country subject to a Department of Treasury Sanctions program.

International Travel Review Procedure
The following points of concern are those most often implicated by international travel or collaborations abroad and the various federal export control regulations and embargoes/ economic sanctions. The Export Control Officer will review all submitted travel requests and provide a written synopsis of compliance requirements.

Destination
Travel to countries under a U.S. sanction or embargo may require government approval. Information concerning U.S. Sanctions programs and country specific requirements is available at: http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx

International travel must not involve the export of defense articles, data or performance of defense services, including instruction unless authorized by the U.S. Government. Certain countries are subject to a U.S. Arms embargo wherein they are ineligible for U.S. Government approval: http://www.pmddtc.state.gov/embargoed_countries/index.html

This includes research collaborations involving research conducted in the U.S. subject to restrictions that does not otherwise qualify as "fundamental research."

Export of Equipment or Data
In most situations, licensing is not required to take items abroad under a "tool of trade" exception with only a requirement of maintaining effective control of the equipment. Export regulations will generally not restrain you from taking commercially available laptop computers and standard software to most countries. However, other research equipment, select agents and toxins may not qualify under this exception. All data must qualify as public domain.

To qualify for the "tool of trade" exception, the export must:

- Be less than one year.
- Consist only of reasonable equipment, i.e. laptop computers, other portable computing devices, data storage devices and other equipment that researchers in a particular discipline would generally recognize as a "tool of trade."
- Travelers must maintain effective control by retaining physical possession of the equipment at all times or securing the item in a secure environment such as a hotel safe, a bonded warehouse, or a locked or guarded meeting or conference facility.

- The travel cannot be to an embargoed country (Cuba, Iran, North Korea, Syria or Sudan).

The following equipment requires a license or other government approval for export, including hand-carry:

- University-owned scientific equipment (other than a sanitized laptop computer, PDA or electronic storage device)
- Data or information received under an obligation of confidentiality.
- Data or analyses that result from a project for which there are contractual constraints on the dissemination of the research results
- Computer software received with restrictions on export to or on access by foreign nationals.
- *Devices* or equipment received with restrictions on export to or on access by foreign nationals.
- Private information about research subjects
- Devices, systems or software that was specifically designed or modified for military or space applications.
- Classified information

Purpose of the Trip

Presentations & Seminars: In general, travel outside of the U.S. to attend a conference not to present - does not require a license. However, information presented at seminars must be limited to topics that arc not related to export-controlled items or technologies unless that information is already in the public domain. Open seminars are usually not problematic unless they take place in a sanctioned country or involve restricted parties. Technical discussions could require a license.

Foreign Collaborations: Publically available information or fundamental research can be shared wid1 foreign colleagues so long as the recipients are not employees or representatives of the government of a sanctioned country, or restricted parties. This includes normal academic peer review or publishing processes.

Research & Instruction Outside of the U.S.: Research and course instruction conducted outside of the U.S. may not qualify for the fundamental research exclusion. Export controls may apply until the work is published or is otherwise in the public domain. Before teaching a course or disclosing information outside of the U.S. it is important to ensure that the information is not subject to export control laws and regulations.

Furnishing Financial Assistance: OFAC regulations prohibit the university from providing material financial assistance or anything of value, including services, to any blocked or sanctioned country, individual, entity or organization, including a government agency of a sanctioned country. This can involve subcontracts, international vendors or payments to research participants. For example, a professional presentation, whether or not it contains materials controlled under **ITAR or EAR** is deemed under OFAC to be a "service" and "something of value" provided to the recipient audience.

5.11 ECO-11 Reserved

This page intentionally blank

5.12 ECO-12 EXPORT CONTROL RECORDS

OFFICE OF RESEARCH & COMMERCIALIZATION

SUBJECT:	**Effective Date:** February 2014	**Guideline Number:** ECO-12
Export Control Records Protocol	**Supersedes:** December 2009	
	Responsible Authority: Export Control Officer	

APPLICABILITY
These protocols are applicable to the Office of Export Controls.

PURPOSE
The University at-large will maintain all records related to export activities in accordance with UCF Policy

BACKGROUND
The University at-large maintains all records in compliance with Florida's public records law and Florida's retention schedule for public records pursuant to Policy 2-100.4 "Florida Public Records Act: Scope and Compliance." This policy makes most documents, including email messages and text messages, created or received by UCF employees in connection with official business public records. Such records must be maintained for a period of seven years.

Certain types of research records, such as those related to export activities are not public records. These records are retained for a period of seven years pursuant to State of Florida requirements.

Export Administration Regulations ("EAR") require the following records related to exports be retained for a five year period in accordance with and 15 CFR Part 762 (EAR):

- All license documentation, applications, and supplemental materials submitted in support of a license
- International Import documents
- Shipping documentation, to include Automated Export System ("AES") filings and Shippers Export Declaration ("SED") documentation, dock receipts, bills of lading, all documents prepared by agents or carriers,
- U.S. Customs documentation, Manifests of Goods, Permits, other Agency permits (APHIS, etc.).

International Traffic in Arms Regulations ("ITAR") require the following records be retained for a period no less than five years pursuant to 22 CFR 122.5 that relate to the manufacture, acquisition and disposition of defense articles, technical data or the provision of defense services.

As necessary, the Office of Export Controls may require access to multiple records systems, including:

- Peoplesoft (Financial and Payroll Information)
- ARGIS (Research Database)
- Tera (Research Documentation Archive)
- Fragomen, LLP (Visa Information)
- Viewstar HR (Employee Records, excluding medical information)
- Viewstar International (Records pertaining to all international students and employees registered with UCF in any capacity)
- Viewstar Registrar (Student Records)
- Joint Personnel Adjudication System (JPAS) Cleared Personnel Records
- DTRADE (Department of State Licensing System)
- SNAP-R (Department of Commerce Licensing System)
- TLO (Background Investigation System)
- Infraguard (FBI Strategic Partnership Information System)
- Visual Compliance (International Trade Compliance Software)

GUIDELINE STATEMENT

Each of the relevant export control regulations contain specific recordkeeping requirements that must be satisfied. In addition, the university maintains its own recordkeeping requirements in order to document its commitment to, and compliance with, export control regulations generally. Departments or programs must keep soft or hard copies of all export documentation, including financial records, shipping documentation (Commercial Invoices, Shipper's Export Declarations), and appropriate UCF paperwork in their research project files for a period of seven years from the date of the export, re-export or controlled deemed export.

Procedure

All university records must be retained for a period of seven years. UCF utilizes multiple record systems, all of which are not interoperable. Due to this inconsistent approach, the Office of Export Controls employs a customized records system comprising of electronic and hardcopy records.

A Master Index of export controlled programs, information, and records of assessments are maintained by the Office of Export Controls for the following types of documents, organized according to "Field Elements"

- Contracted Research / Sponsored Research
    - Restricted Research
    - Unrestricted Research
- Visa Screens
    - J1 and H1B
- Commodity Jurisdiction, Commodity Classification and Advisory Opinion Records
- Export Licenses and other approvals

- Import Reviews
- Internal Compliance Investigations and Voluntary Self Disclosures
- Agreements & Memoranda of Understanding
- Sole Source Equipment Purchase Requests
- International Travel Reviews
- International Shipping Reviews
- NASA Specific Compliance Reviews (NASA China Assurance)
- Miscellaneous Review Requests, such as specialized regulatory assessments and impact studies

The Master Index is divided according to the Field Element Code as follows:

AGR	Agreement
CFR	Contracted Research
CJ	Commodity Jurisdiction
H1B	I-129 Assurance Reviews
J1	Visiting Scholar Reviews
LIC	License / Other Government Approvals
MOU	Memoranda of Understanding
IMP	Import
IN	Internal Investigations
MTA	Material Transfer Agreement
NASA	NASA China Assurance
NDA	Non Disclosure Agreement
OTH	Miscellaneous Regulatory Review Records
SHP	Shipping
SS	Sole Source Equipment Purchase
TRA	Travel

The Field Element Codes will be recorded in the order in which they were received and organized by year. For example, AGR-09-001 refers to "Agreement", Year 2009, File No. 001. This number is required to be typed or written on all electronic and hard copy documentation to ensure that all records are properly assigned to a particular task.

Preferred record types will be electronic and as many records as possible will be scanned and uploaded into electronic file folders corresponding to the assigned field element code. For certain activities, hardcopy files may be necessary. All hardcopy files will be noted on the Master Index and properly labeled for retention purposes.

Metrics will be gathered on each of the record types as information is collected and recorded on a master spreadsheet. Such metrics will include:

- Receipt date of initial request and final completion data
- Research ID (obtained from ARGIS)
- Principal investigator or other Point of Contact
- Department

- Review Type (e.g. contract review)
- Sponsor information
- Jurisdiction
- USML/CCL if known
- Security protocol implemented (if required)
- Description
- Contract manager
- Location of stored data (if on server after February 2014)

5.13 ECO-13 Foreign Person Payroll Charge

This page intentionally blank

6 TRAINING & EDUCATION

ORC provides periodic general awareness and special export and trade sanctions training to all Principal Investigators ("PI") for any international collaboration that meets the criteria of fundamental research, or does not involve technology transfer.

Academic departments will be responsible for appropriate orientation of all new employees, graduate, and undergraduate students, including foreign nationals employed by their departments for projects that fall within this TCP. When appropriate, foreign nationals will be briefed and/or informed concerning those areas of export control and export licensing actions that are pertinent to their activities. ORC will make available export awareness training to university personnel.

The Office of Export Controls will consult with appropriate university administrative and academic units to assure provision of instructional resources considered necessary to the understanding and implementation of policy. These resources will include written and web-based material, formal and informal course offerings, and individualized consultation.

The Office of Export Controls provides targeted training for all participants in restricted research, and periodic awareness training tailored to specific college, department, center, and administrative unit needs. When notified of international travel plans, the Office of Export Controls provides travel advisories to faculty, staff, and students on potential export and sanction issues related to that travel.

7 APPENDICES

7.1 APPENDIX 1: OFFICE OF RESEARCH GUIDELINES FOR COMPLIANCE WITH U.S. EXPORT CONTROL LAWS

SUBJECT:	Effective Date:	Policy Number:	
University Guidelines for Compliance with U.S. Export Control Laws	01/17/2006	EC-001	
	Supersedes:	Page	Of
		1	5
Office of Research & Commercialization	Responsible Authority: Vice President for Research		

PREAMBLE:

U.S. export control laws regulate certain transfers of technology to foreign nationals as well as the physical export of hardware and software. This policy establishes guidelines to ensure the University of Central Florida's compliance with these laws.

GENERAL POLICY:

It is the policy of the University of Central Florida that all employees, professors, students, researchers and collaborators 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.

APPLICABILITY:

These guidelines are applicable to all members of the university community engaged in university research.

POLICY STATEMENT:

U.S. export control laws, including the Export Administration Regulations (EAR), the International Traffic in Arms Regulations (ITAR), and U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC) sanction regulations, require that the University of Central Florida obtain an export license prior to providing controlled technologies to certain foreign national employees, professors, students, researchers or other foreign national collaborators. However, information generated during the course of "Fundamental Research", as defined under such laws, is exempt from export licensing requirements.

The University will 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. To this end, the University will ensure that, unless unavoidable, information generated during the performance of any university research, including sponsored contract activities, qualifies for the Fundamental Research provisions of applicable export control laws.

University Guidelines for Compliance with U.S. Export Control Laws

The civil and criminal penalties associated with violating export control regulations can be severe, ranging from administrative sanctions including loss of research funding to monetary penalties to imprisonment for individuals.

The University 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 http://research.ucf.edu/compliance/export control that contains university export control policies, forms, training modules and reference materials.

DEFINITIONS:

Foreign National. Any person who is not a:

a. U.S. Citizen or national;
b. U.S. Lawful Permanent Resident;
c. Person granted asylum;
d. Person granted refugee status; or
e. Temporary resident (does not include persons who hold status such as F-1, J-1, H-1, L-1 etc. as well as those in or outside the U.S. without status).

Fundamental Research. For the purposes of this policy, Fundamental Research means, as defined by the EAR and ITAR, basic or applied research in science and engineering performed or conducted 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 that results in information that is restricted for proprietary reasons or national security reasons or pursuant to specific U.S. government access and dissemination controls.

Hardware. Any article, material, or supply except technology and software.

Software. A collection on one or more programs or microprograms fixed in any tangible medium of expression.

Technology. Specific information necessary for the development, production, or use of a product.

PROCEDURES:

A. Responsibilities

(1) The Export Compliance Officer shall:

a) Ensure implementation of University export control policy and related guidelines and serve as the primary contact for the University on export

control matters. The Associate Director, Office of Research & Commercialization, shall serve as the ECO.

b) In coordination with Contract Managers, conduct export licensing determinations and prepare, file, and monitor compliance with export licenses, as necessary.
c) In conjunction with Contract Manager, brief Principal Investigators ("PIs"), as necessary, on applicable U.S. export control law requirements.
d) Consult the Office of General Counsel, as necessary, for export control regulatory guidance and interpretation.
e) Provide export control training to University staff, students, researchers and other collaborators, as necessary.
f) Report instances of possible export control law non-compliance to the Office of General Counsel.

(2) Contract Managers shall:

a) Assist the ECO in implementation of University export control policy and related guidelines.
b) Complete the Export Control Review Form (Attachment 1) as provided in Section III.
c) In conjunction with the ECO, brief PIs, as necessary, on applicable U.S. export control laws.

(3) Principal Investigator (PI) shall:

a) Assist the ECO and Contract Manager, as necessary, in determining applicable export control requirements for hardware, software and/or technology subject to U.S. export control laws.
b) Execute the Export Control Review Form as provided in Section III, as applicable.
c) Implement export control guidelines provided by the ECO and Contract Manager.
d) Identify hardware, software and technology to be exported to a foreign destination and, in advance of export, report the same to the ECO for an export licensing determination.
e) Report instances of possible export control law non-compliance to the ECO.

(4) Office of General Counsel shall:

a) Upon request, provide regulatory guidance to the ECO, Contract Manager, and PI on export control matters.
b) Assist the Contract Manager with contract negotiations, as provided in Section III.
c) Investigate potential export control non-compliance issues.

B. Export Control Review

(1) The Contract Manager will review University contracts to determine whether the Fundamental Research exemption will apply to contract activity. With the assistance of the Office of General Counsel, as necessary, the Contract Manager shall revise, modify or negotiate problematic contract provisions with the Sponsor with the goal of preserving the Fundamental Research exemption. The Contract Manager shall document the end-results of this review using the Export Control Review Form.

(2) Where the Contract Manager determines the Fundamental Research exemption is inapplicable to contract activity, the following actions shall occur:

a) The Contract Manager provides the Export Control Review Form to the ECO.
b) The ECO, in coordination with the Contract Manager and PI, determines applicable U.S. export control law requirements. The ECO documents applicable U.S. export controls on the Export Control Review Form.
c) The ECO briefs the PI on applicable U.S. export control restrictions, with the PI and ECO executing acknowledgement of such briefing on the Export Control Review Form.
d) The ECO coordinates with the Contract Manager and PI to perform export control screening for persons participating in contract activity. To do so, the ECO circulates the Export Control Compliance Questionnaire (Attachment 2) to all University employees, professors, students, researchers or other collaborators participating in contract activity.
e) The ECO reviews the completed Export Control Compliance Questionnaire and determines whether the University requires an export license to transfer contract related technology or technical data to any persons participating in contract activity.
f) The ECO prepares and submits export licenses, as appropriate. If granted, the ECO implements the export license and any conditions thereto.

(3) University employees, professors, students, researchers or other collaborators desiring to export hardware, software and/or technology shall notify the ECO of the intended export. The ECO will determine applicable export licensing requirements, if any, and prepare/submit export license applications as required.

RELATED DOCUMENTS:

(1) Export Administration Regulations, 15 C.F.R. Parts 730-774.
(2) International Traffic in Arms Regulations, 22 C.F.R. Parts 120-130.
(3) U.S. Department of Treasury, Office of Foreign Assets Control Sanctions Program and Country Summaries (http://www.treas.gov/offices/enforcement/ofac/sanctions/).

FORMS:

(1) Export Control Review Form
(2) Export Control Compliance Questionnaire

RELATED INFORMATION:

(1) Association of American Universities (AAU)/Council on Government Relations (COGR) Report, Restrictions on Research Awards: Troublesome Clauses (http://aau.edu/research/Rpt4.8.04.pdf).
(2) COGR Report, Export Controls and Universities: Information and Case Studies (http://206.151.87.67/docs/Export%20Controls.pdf).
(3) National Security Directive 189 (http://www.fas.org/irp/offdocs/nsdd/nsdd-189.htm).

INITIATING AUTHORITY: Office of Research & Commercialization

7.2 APPENDIX 2: UCF POLICY 4-209 "EXPORT CONTROLS"

SUBJECT Export Control Policy	Effective Date	Policy Number 4-209
	Supersedes	
	Responsible Authority Director of Research Compliance and Assistant Director of Export Controls	

APPLICABILITY/ACCOUNTABILITY

This policy applies to all members of the university community.

BACKGROUND

U.S. export control laws including, but not limited to the Arms Export Control Act (AECA), implemented by the International Traffic Arms Regulations (ITAR), the Export Administration Act (EAA) of 1979 implemented by the Export Administration Regulations (EAR) and U.S. Department of Treasury, Office of Foreign Assets Control (OFAC) sanction and embargo regulations, regulate the distribution by whatever means, of strategically important hardware, software, and technology to foreign nationals, whether in the U.S. or abroad. Violations of these regulations may result in civil and criminal penalties and fines, including imprisonment.

U.S. export control laws, sanctions and embargo regulations exist for reasons of national security, foreign policy, non-proliferation, short-supply and multilateral obligations and regulate both civil and military commodities, implements of war and related technologies and services specifically enumerated in the U.S. Munitions List (USML) of the ITAR or Commerce Control List (CCL) of the EAR.

Although most university activities and research are exempt from export control laws, the University of Central Florida (UCF) engages in activities, research, and the development of new technologies that are subject to export restrictions. The application of export control laws requires a detailed analysis of covered university activities and research to determine if the export is prohibited, or requires a license or other government approval. This policy establishes the program and procedures necessary to ensure the university and its employees remain in full compliance.

POLICY STATEMENT

The University of Central Florida is committed to compliance with federal export control laws, regulations, and sanctions. The Office of Research & Commercialization (ORC) is the designated authority charged with compliance oversight of U.S. export control requirements for sponsored program activities 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.

The Office of Research Compliance, a unit within the ORC, is the functional administrative unit charged with the responsibility for oversight of compliance and recordkeeping of all applicable exports and regulated transactions with sanctioned individuals, entities, and countries. UCF personnel are responsible to adhere to the protocols, policies, and procedures issued by the Office of Research Compliance when export or trade sanction regulations apply and must properly handle export controlled hardware, software, information, technology, or technical data by regulating access, use, storage, and disposal.

The civil and criminal penalties associated with violating export control regulations can be severe, ranging from administrative sanctions including loss of research funding to monetary penalties to imprisonment for individuals. Anyone found to have engaged in conduct contrary to this policy is subject to disciplinary action by the university up to and including dismissal or expulsion and civil or criminal prosecution.

EXPORT CONTROLS COMPLIANCE PROGRAM

Export compliance protocols, policies and procedures and key cooperating offices are available in the online UCF Export Control Management Plan (ECMP) http://www.research.ucf.edu/documents/PDF/UCF%20ECMP%203_25_2014_Rev%20_2.pdf. UCF personnel must comply with the requirements and procedures communicated in the ECMP. The Office of Research Compliance in concert with other departments and units as necessary will administer the compliance program for:

1. Identification and management of export controlled sponsored program activities
2. Sponsored program activities involving disclosures or transfers to foreign persons of export controlled technologies in the United States (deemed exports)
3. Non-immigrant worker visa applications (H-1B, H-1B1, L-1, O-1 and J-1) involving export controlled technologies (deemed export visa applicant screening)
4. Sponsored program activities involving international exports (shipping)
5. International travel
6. Compliance screening for denied party/entity list and other government debarred list transactions
7. Sponsored program activities involving the use of export controlled equipment

8. Restrictive trade practices, foreign corrupt practices, financial transactions, and anti-boycott compliance

The Office of Research Compliance will assist academic, research, and business units and direct support organizations to comply with export and trade sanction regulations on non-sponsored activities on a case-by-case basis.

The university 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: http://www.research.ucf.edu/ExportControl/ that contains the ECMP, forms, training modules, and reference materials.

FUNDAMENTAL RESEARCH EXCLUSION

Export control regulations may conflict with the university's tradition of academic freedom and openness in research and provide a broad exclusion from export controls for certain academic research that meets several legal criteria, commonly referred to as the "Fundamental Research Exclusion."

The qualifying criteria for research results to be exempt from U.S. export controls are established by the U.S. Government and include basic and applied research as follows:

1. conducted free of any participation restrictions,
2. conducted free of any publication restrictions, or
3. conducted free of any access or dissemination controls required for proprietary or national security reasons.

It is critical that all research activity is assessed to determine if any hardware, software, information, technology, or technical data involved or generated would void the fundamental research exclusion.

EXPORT LICENSE OR OTHER APPROVAL REQUIREMENT

While most research results qualify as "fundamental research" and are not subject to export controls, there are certain conditions under which the performance of the actual research or export of critical technologies, including certain technical and scientific data, software or tangible items, is either prohibited by law or requires an export license or other government approval before an export may take place.

Examples include, but are not limited to:

1. Shipment or transmission of tangible equipment, items, software, materials, and technical data listed on the Commerce Control List (CCL) or U.S. Munitions List (USML) outside of

the United States by any means (e.g., shipping, hand-carrying, emailing), whether temporarily or permanently.
2. Providing controlled technologies or technical data related to a USML defense article in any manner to foreign national employees, professors, students, researchers, or other foreign national collaborators whether in the U.S. or abroad without a license or other approval.
3. Importing or using a defense article.
4. Conducting international collaborations or exchanges (e.g., financial transactions and providing goods and services of value) with embargoed or sanctioned entities, governments, and countries.

MONITORING AND COMPLIANCE

UCF is registered with the federal government as a defense manufacturer and has designated ORC to monitor export compliance in sponsored program activities that are not otherwise exempt. The vice president of research and commercialization, director of research compliance, and assistant director of export controls are empowered officials. Possible violations of governmental laws and regulations will be investigated by a university empowered official or designee. Action will be taken according to the nature, severity, and scope of the offense. The university empowered official(s) have the authority to suspend or terminate a research, teaching, testing, or other export activity if the empowered official determines the activity is not in compliance, or will lead to noncompliance with existing export or sanction laws or policy.

DEFINITIONS

Empowered official. Authorized full-time permanent employees registered with the Department of State in accordance with federal regulation 22 CFR 120.25, who have independent authority to inquire into any aspect of a proposed export or temporary import, to verify legality and compliance with U.S. export control laws and sanctions, and to refuse to authorize or limit the transaction without prejudice or other adverse recourse.

Export control laws, regulations, and sanctions. Specifically, 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 U.S. Department of Treasury, Office of Foreign Assets Control (OFAC) sanction and embargo regulations, and other applicable federal agency export control regulations.

Foreign national. Any person who is not a U.S. citizen or U.S. lawful permanent resident.

Fundamental research. For purposes of this policy, fundamental research means, as defined by the EAR, ITAR, and NSDD 189, basic or applied research in science and engineering performed or conducted on campus at an accredited institution of higher learning in the U.S. where the resulting

information is ordinarily published and shared broadly in the scientific community. Fundamental research is distinguished from research that results in information restricted for proprietary reasons, national security reasons, or pursuant to specific U.S. government access and dissemination controls. Information or technology that results from fundamental research is not subject to export controls.

Hardware. Any article (ITAR term), item (EAR term), material, commodity, or supply except technology or software.

Permanent resident. Individuals who have permission to reside in the U.S. on a permanent basis (i.e., holders of "green cards").

Proprietary. Any form and type of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:
•The owner thereof has taken reasonable measures to keep such information secret, and;
•The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public. Proprietary information may take such forms as trade secrets, privileged or confidential commercial or financial information, or any other information not otherwise required to be disclosed.

Software. A collection of one or more programs or microprograms fixed in any tangible medium of expression such as source code (programming statements) or object code (machine-readable instructions).

Sponsored research. All organized research and development activities sponsored by federal and non-federal agencies and organizations, including university sponsored research that are accounted for and separately budgeted.

Technology. Specific information necessary for the development, production, or use of hardware or software, such as models, engineering designs, blueprints, drawings, technical assistance, or other types of information whether tangible or intangible.

Unsponsored research. The performance of work that is not funded by a sponsor and that is not separately budgeted or accounted for.

PROCEDURES

All sponsored research activities and unsponsored research activities that interface with sponsored programs must be evaluated prior to commencement to determine if export controls are applicable, as detailed within the following protocols. Sufficient time must be allowed for the empowered official to review such activities and issue guidance. Key faculty, staff, and administrative personnel will assist the empowered official in determining applicable export control measures to regulate the export of hardware, software, technology by any means, including deemed-exports. Such measures

include implementing necessary security measures (e.g., restricting access, acquiring licenses or other government approval, implementing a technology control plan).

Identification and Management of Export Controlled Sponsored Program Activities. Principal Investigators (PI) engaged in research of any scope and duration shall, prior to commencement, be responsible to review whether the intended research is subject to controls or requirements contained within export regulations and, if applicable, to comply with such requirements. This includes continually reviewing the research project while being performed for changes that would subject the project to export controls.

The Sponsored Programs Office will ensure that contracts, grants, and agreements are executed in compliance with applicable export control regulations, laws, sanctions, and embargoes by assisting the principal investigator in identifying any export control, foreign national, or publication restrictions in solicitations and awards. When possible, the Sponsored Programs Office will negotiate any access, publication, dissemination, or participation restrictions to allow the sponsored project to qualify as fundamental research, in accordance with the protocols outlined in the ECMP http://www.research.ucf.edu/documents/PDF/UCF%20ECMP%203_25_2014_Rev%20_2.pdf

1. Determine whether the intended or current research qualifies as fundamental research as that term is applied in the export control regulations ITAR (22 CFR § 120.11) and EAR (15 CFR § 734.8). If the intended or current research qualifies as fundamental research, then no export license or restriction is required.
2. If, after review, it is determined that the scope of the intended or current research falls within the export control regulations contained in either the EAR, the ITAR, or potentially involve any sanction or embargo activities, or controlled technologies, the sponsored program will be forwarded to the ORC Office of Research Compliance for comprehensive compliance assessment review by an authorized staff member.

    a. The authorization for foreign nationals to engage in, access, use or possess export controlled hardware, software, or technology on sponsored program activities is dependent on the conditions identified in applicable U.S. laws, regulations, sanctions or government licenses, or approvals. It is the responsibility of the Office of Research Compliance to determine export compliance requirements.
    b. If the intended or current research does not qualify as fundamental research, the ORC Office of Research Compliance will determine whether the intended or current research is within the control of the Department of State under authority of ITAR (military applications only) or is within the control of the Department of Commerce under the authority of the EAR (dual usage – both military and commercial applications, or proliferation applications). In considering this issue, the ORC Office of Research Compliance will:

        i. Consult the USML (22 CFR § 121.1) and/or the CCL (15 CFR § 774, Supp. 1) to determine whether the intended or current research involves any items or technologies that are regulated.
        ii. Examine the procedures contained in the ITAR and/or the EAR (15 CFR § 732) to determine whether a license will be required to export, release,

transmit, or allow access to the results from the intended research, or is required to export, release transmit, or allow access to the current research.

iii. Examine U.S. sanction and embargo programs administered by the U.S. Department of the Treasury.

iv. Issue a request for commodity jurisdiction or commodity classification with the appropriate federal agency, if necessary.

v. Obtain export licenses, if necessary, and implement a project-specific Technology Control Plan and other documents required by applicable export control regulations including, restricting access and participation to foreign nationals.

c. The principal investigator and unit are responsible for implementing and complying with a project-specific Technology Control Plan issued by the Office of Research Compliance and other security measures necessary for compliance.

3. If, after review, it is determined that the scope of the intended research does not fall within the export control regulations the principal investigator and researchers may commence with the research initiative unless otherwise restricted by other policies or procedures of the university.

Sponsored Program Activities involving Disclosures or Transfers to Foreign Persons of Export Controlled Technologies in the U.S. (Deemed Exports).

The release or transmission of technology or technical data, including training, subject to export controls to a foreign national (including graduate students, postdocs, visiting scholars, collaborators, faculty, etc.) within the U.S. is a "deemed export" and is considered an export to that person's home country. A license may be required before the information can be released or transferred.

Examples of "releases" to foreign nationals include:

1. allowing a foreign person to participate in a research project,
2. instructing the foreign person in research techniques and methods,
3. providing access to equipment during a facility tour,
4. providing access to technical equipment, research samples, or experiments by visual inspection or use, and
5. verbal exchanges of controlled information.

It is the responsibility of the empowered official to determine the licensing requirements involving deemed exports. If a license is required, the empowered official will coordinate the license application process and submit the application to the appropriate federal agency. Obtaining a license can take two to six months (or more) and the U.S. government can deny a request thereby terminating the deemed export. No export can take place until the requisite license is obtained. Deemed export reviews conducted by an empowered official involving a sponsored program activity will, at a minimum, require the principal investigator to submit the following information:

1. Description of the information to be released – this includes a detailed description of the information, item, software, or technology, technical specifications, origin of the item and any contractual non-disclosure or use restrictions that may exist.

2. A list of the home country and citizenship of all persons that will be given access to the information, item, software, or technology, including all information required in a license application.
3. Supplemental explanation describing the source of the information or item, software, or technology and if it is a result of fundamental research.
4. Response to whether the information item is published, patented, or in some other manner in the public domain.

Non-immigrant Worker Visa Applications (H-1B, H-1B1, L-1, O-1, J-1) Involving Export Controlled Technologies (Deemed Export Visa Applicant Screening)
Faculty and staff sponsoring non-immigrant workers are responsible for complying with U.S. export and sanctions regulations in all university activities involving international collaborations or foreign exchanges, including hiring foreign persons on a permanent or temporary basis (international visitors, scholars) or allowing a volunteer to participate on a sponsored program activity. Training, educational activities, and technical assistance incidental to a controlled technology used in a sponsored program requires review by the ORC Office of Research Compliance to conduct a deemed export assessment for H-1B, H-1B1, L-1, O-1 and J-1visas.

Faculty and staff sponsoring a non-immigrant worker are required to furnish the ORC Office of Research Compliance with all necessary information to perform an attestation on the ***Questionnaire for Sponsoring a Foreign Scholar, Scientist, Visitor or Guest.*** Faculty, staff, units, and departments are responsible for complying with all regulatory guidelines issued by ORC regarding deemed exports in addition to all provisions issued by the U.S. government in licenses or other approvals.

Sponsored Program Activities Involving International Exports (Shipping)
It is the responsibility of the exporter, prior to shipping any item, article, technology, or technical data out of the U.S. related to a sponsored program activity, to determine if the export has any license requirements. To make this determination, the exporter needs to contact the ORC Office of Research Compliance who will investigate regulatory requirements and provide proper guidance. Determining license requirements of an item can be a complex and complicated process requiring proper commodity jurisdiction and classification of an item. The final determination of whether an item requires a license, qualifies for a license exemption or exception, or can be exported as "No License Required" (NLR) will be made by the empowered official.

All tangible items, software code, and information not on a U.S. export control list may be shipped or transmitted to any country, individual or entity that is not sanctioned, embargoed, or otherwise restricted for export. If a license is required for export, the empowered official will coordinate the license application process and submit the application to the appropriate federal agency. Obtaining a license can take two to six months (or more) and the U.S. government can deny a request, thereby terminating the export. No export (or deemed export) can take place until the requisite license is obtained. Exports involving a sponsored program activity will, at a minimum, require the exporter to submit the following information to the empowered official:

1. A list of the items, article, or technical data intended for export (including deemed export). This includes a detailed description of the item, software, technology, or technical

specifications, origin of the item or data, and any contractual non-disclosure or use restrictions implicated in the transaction.
2. The intended destination of the item, software, technology, or data.
3. The recipient and end-user.
4. The intended end-use.
5. Response to whether the time or data is published, intended to be published, patented, or in some other manner in the public domain.

International Travel
Travel outside the United States can require a federally-issued license, depending on the proposed destination, equipment, item(s) or data being exported (if any), the purpose of the travel, and persons, entities, or countries involved in the travel.

1. All international travel related to a sponsored program will be reviewed by the Sponsored Programs Office and **may** require the traveler complete an ***International Travel Compliance Review Form***. Certain sponsored programs may be subject to federal law that requires government approval or licensing before exporting equipment, research data, or performing research abroad. This can include the hand carrying of items that have both commercial and military, or proliferation applications, proprietary information, or items that are considered defense articles, even if used in an academic or research environment. Such items may include data, software or technology, blueprints, design plans, field data, equipment, and retail software packages and technical information.

   The questionnaire will be forwarded to the ORC Office of Research Compliance for review. The ORC Office of Research Compliance will determine if any of the equipment, items, samples, or technical data or services (including training) proposed for export in furtherance of a sponsored program activity require licensing or other approval and if any of the parties involved in the transaction are listed on various federal restriction lists or subject to a U.S. sanction or embargo.

U.S. Departments of State, Commerce and Treasury Compliance Screening for Denied Party/Entity List and other Government Debarred List Transactions
Faculty and staff are required, prior to engaging in a foreign collaboration, to review the various federal lists that restrict certain transactions, including:

1. certain practices,
2. instruction,
3. research performance or collaborations,
4. providing service activities, and
5. financial transactions.

The ORC Office of Research Compliance will coordinate and facilitate the screening of potential parties to such regulated transactions in accordance with federal regulation among various departments and units. The federal screening lists are available at the following federal website http://export.gov/ecr/eg_main_023148.asp , and include, but are not limited to:

1. Department of Commerce – Bureau of Industry and Security: Denied Persons, Unverified and Entity Lists.
2. Department of State – Bureau of International Security and Non-proliferation: Nonproliferation Sanctions
3. Department of State – Directorate of Defense Trade Controls: Arms Export Control Act Debarred List
4. Department of the Treasury – Office of Foreign Assets Control: Specially Designated Nationals List and countries and practices of which the U.S. government has imposed a sanction or embargo.

Upon positive identification of a party that appears to match a list, the screening party is obligated to contact the ORC Office of Research Compliance, which will issue regulatory guidance to comply with U.S. export control regulations, laws, and sanctions. There may be a strict export prohibition, requirement for seeking a license, evaluation of the end-use or user to ensure it does not result in an activity prohibited by any U.S. export regulation sanction or embargo. Faculty, staff, units, and departments are responsible for complying with all regulatory guidelines issued by ORC regarding Denied Party/Entity List and other government Debarred List transactions in addition to all provisions issued by the U.S. government in licenses or other approvals.

Sponsored Program Activities Involving the Use of Export Controlled Equipment
The ORC Office of Research Compliance will identify export controlled equipment in accordance with the following:

1. EAR Commerce Control List (CCL) equipment, technical data and "use":

    a. The release or transmission of technology or technical data subject to the EAR created or developed at UCF to a foreign national within the U.S., including training (including graduate students, postdocs, visiting scholars, collaborators, faculty, etc.) is allowable on sponsored program activities qualifying as fundamental research or in furtherance of an official published catalog course taught within the U.S. Technology or technical data subject to the EAR not qualifying as fundamental research or instructed outside of the U.S. is subject to export controls.
    b. The operation of equipment subject to the EAR by a foreign national on campus, including instruction of the manner of operation of the equipment, is allowable on sponsored program activities so long as the instruction does not involve each of the following six criteria pursuant to 15 CFR 772.1: Operation, installation (including on-site installation), maintenance (checking) repair, overhaul, and refurbishing. Instruction of all six criteria requires a license unless an exception or exclusion apply.

2. ITAR United States Munitions List (USML) defense articles, technical data and defense services:

    a. All defense articles including technical data and defense services (instruction, training, or know-how) related to defense articles, even if not for military use, and information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles

are subject to export controls and cannot be released to or operated by a foreign national without a license, or other government approval. Such articles and data require a Technology Control Plan or a Custody Access and Use Agreement.

3. Third party export controlled items or data:

    a. CCL items, USML defense articles, technology, technical data, and associated defense services provided by a third party to the university and any of its departments, divisions, colleges, units, and organizations or faculty, staff, and students may not be released to or openly shared with certain foreign nationals even though those individuals may be important contributors to the performance of a sponsored program activity utilizing the export controlled third-party item or data. Proprietary or restricted information that is required for the development, production, or use of an item subject to the EAR or the ITAR is itself export controlled. It is the responsibility of the recipient of the third-party export controlled items or data to notify the ORC Office of Research Compliance of the acceptance of such items and information by completing a ***Custody, Access and Use Agreement.*** If the researcher or principal investigator needs to transfer the items or information to foreign nationals, the exporting party is responsible to contact the empowered official for an export determination before such a transfer occurs. The empowered official will obtain a license or qualify the transaction under an exemption, exception, or exclusion, and document the transaction.

Restrictive Trade Practices, Financial Transactions and Anti-Boycott Compliance
The United States imposes restrictions under various legal authorities against engaging in certain restricted trade practices and transactions that impose a boycott of Israel. Those laws discourage, and in some circumstances, prohibit U.S. companies and universities from furthering or supporting the boycott of Israel sponsored by the Arab League, and certain Moslem countries, including complying with certain requests for information designed to verify compliance with the boycott. Anti-boycott provisions are issued in 15 CFR §760.

U.S. sanctions administered by the Office of Foreign Assets Controls (OFAC) regulations prohibit the university from providing material financial assistance or anything of value, including services, to any blocked or sanctioned country, individual, entity or organization, including a government agency of a sanctioned country. This can involve subcontracts, international vendors, or fellowship payments to a researcher in a foreign country. For example, a professional presentation, whether or not it contains materials controlled under ITAR or EAR, is deemed under OFAC to be a "service" and "something of value" provided to the recipient audience. Before agreeing to provide funding to a foreign national, personnel should contact the empowered official for assistance in identifying potential transaction restrictions.

RELATED INFORMATION

U.S. Department of State, Directorate of Defense Trade Controls
http://www.pmddtc.state.gov/

U.S. Department of Commerce, Bureau of Industry and Security
http://www.bis.doc.gov/

U.S. Department of Treasury, Office of Foreign Assets Control
http://www.treas.gov/offices/enforcement/ofac/

UCF, Office of Research & Commercialization, Export Compliance
http://www.research.ucf.edu/ExportControl/

UCF Export Compliance, Frequently Asked Questions
http://www.research.ucf.edu/ExportControl/faq.html

UCF, International Services Center
http://www.intl.ucf.edu/

UCF, Office of Internationalization
http://www.international.ucf.edu/

RELATED DOCUMENTS

UCF Export Compliance Guidelines
http://www.research.ucf.edu/ExportControl/policies.html

UCF Export Controls Management Program
http://www.research.ucf.edu/documents/PDF/UCF%20ECMP%203_25_2014_Rev%20_2.pdf

International Traffic in Arms Regulations (ITAR), 22 CFR §§120-130
http://www.ecfr.gov/cgi-bin/text-idx?SID=9e6812e666569c99554abd395da45965&tpl=/ecfrbrowse/Title22/22CIsubchapM.tpl

ITAR, U.S. Munitions List (USML), 22 CFR § 121.1
http://www.ecfr.gov/cgi-bin/text-idx?SID=86008bdffd1fb2e79cc5df41a180750a&node=22:1.0.1.13.58&rgn=div5

Export Administration Regulations (EAR), 15 CFR §§734-774
http://www.ecfr.gov/cgi-bin/text-idx?SID=9e6812e666569c99554abd395da45965&tpl=/ecfrbrowse/Title15/15CVIIsubchapC.tpl

EAR, Commerce Control List (CCL), 15 CFR § 774, Supplement No. 1
http://www.ecfr.gov/cgi-bin/text-idx?SID=9e6812e666569c99554abd395da45965&node=ap15.2.774_12.1&rgn=div9

Office of Foreign Assets Control (OFAC) Regulations, 31 CFR §§500-599
http://fedbbs.access.gpo.gov/library/fac_bro/facei.pdf

National Security Decision Directive 189
http://www.fas.org/irp/offdocs/nsdd/nsdd-189.htm

Office of Internationalization, International Academic Agreements (2-900)
http://policies.ucf.edu/documents/2-900InternationalAcademicAgreementsFinalonLetterhead11-16-11.pdf

Office of Internationalization, Travel to Restricted Destinations (2-903)
http://policies.ucf.edu/documents/2-903TraveltoRestrictedDestinationsFinalonLetterhead.pdf

International Services Center, UCF Policy for All Foreign Nationals (2-901)
http://policies.ucf.edu/documents/2-901UCFPolicyforAllForeignNationalsFinalonLetterhead11-16-11.pdf

FORMS

Questionnaire for Sponsoring a Foreign Scholar, Scientist, Visitor or Guest
http://www.research.ucf.edu/documents/PDF/DeemedExportQuestionnaire.pdf

International Travel Compliance Review Form
http://www.research.ucf.edu/documents/PDF/ORC_Travel_Compliance_Review.pdf

Tool of Trade Checklist
http://www.research.ucf.edu/ExportControl/checklist.html

Tool of Trade Certificate
http://www.research.ucf.edu/documents/Word/TMP%20-%20ENC%20Certification.docx

CONTACT

For questions regarding ORC, Office of Export Compliance policies and procedures please contact the assistant director of export controls with the Office of Research & Commercialization, Office of Research Compliance, 12201 Research Parkway, Suite 501, Orlando, Florida 32826-3246, (407) 823-3778.

INITIATING AUTHORITY

Vice President for Research & Commercialization

7.3 APPENDIX 3: Designated Departments & Units Principal Points of Contact

Central Administration

Audit

Kathy Mitchell, Associate Director
4364 Andromeda Loop, North
Room 431
Orlando, FL 32816-0080

Phone: 407-823-2889
Fax: 407-823-6330
Email: Kathryn.Mitchell@ucf.edu

Computer Support
Adiaak Gavarrete, Technology Manager
Phone: 407-823-0546
Email: adiaak@ucf.edu

Paul Turner, Systems Administrator
Phone: 407-823-4084
Email: pturner@ucf.edu

Compliance

Rhonda Bishop, Chief Compliance and Ethics Officer
4364 Andromeda Loop, North
Room 431
Orlando, FL 32816-0080

Phone: 407-823-6263
Fax: 407-823-6265
Email: Rhonda.Bishop@ucf.edu

Computer Support
Adiaak Gavarrete, Technology Manager
Phone: 407-823-0546
Email: adiaak@ucf.edu

Paul Turner, Systems Administrator
Phone: 407-823-4084
Email: pturner@ucf.edu

Environmental Health & Safety
Thomas Briggs, Director
3528 N. Perseus Loop
Orlando, FL 32816-3500

Phone: 407-823-1183
Email: Thomas.Briggs@ucf.edu

Renea Carver, Assistant Director
3528 N. Perseus Loop
Orlando, FL 32816-3500

Phone: 407-823-0071
Email: Renea.Carver@ucf.edu

Computer Support
Andrew O'Mara, IT Manager
Phone: 407-882-0183
Email: Andrew.O'Mara@ucf.edu

Finance & Accounting

Finance
Tracy Clark, Associate VP for Finance and Controller
Research Pavilion, Suite 300
12424 Research Parkway
Orlando, FL 32826-3249

Phone: 407-882-1006
Email: Tracy.Clark@ucf.edu

International Student Tuition
Glen Carlson, Senior Associate Controller
Research Pavilion, Suite 300
12424 Research Parkway
Orlando, FL 32826-3249

Phone: 407-882-1064
Email: Glen.Carlson@ucf.edu

Travel:
Justine Mercado
Research Pavilion, Suite 300
12424 Research Parkway
Orlando, Florida 32826-3249

Phone: 407-882-1081
Email: Lita.Mercado@ucf.edu

Property & Inventory Control
Tereasa Clarkson, Accountant
Research Pavilion, Suite 300
12424 Research Parkway
Orlando, Florida 32826-3249

Phone: 407-823-1953
Email: Tereasa.Clarkson@ucf.edu

Computer Support
Carlos Chardon, Department IT Manager
Phone: 407-882-1048
Email: Carlos.Chardon@ucf.edu

UCF Foundation

Albert J. "Bert" Francis II, Chief Financial Officer
12424 Research Parkway, Suite 250
Orlando, FL 32826

Phone: 407-882-2272
Email: Albert.Francis2@ucf.edu

Computer Support
Mohammed Dasser, Director
Phone: 407-882-1574
Email: Mohammed.Dasser@ucf.edu

General Counsel:

Scott Cole, Vice President & General Counsel
Associate General Counsel
4364 Andromeda Loop, North
Suite 360
Orlando, FL 32816-0015

Phone: 407-823-2482
Email: Scott.Cole@ucf.edu

Procurement Issues:
Natasha Hellerich, Associate General Counsel
4364 Andromeda Loop, North
Suite 360
Orlando, FL 32816-0015

Phone: 407-823-2482
Email: Natasha.Hellerich@ucf.edu

Research:
Sandra Sovinski, Associate General Counsel
12201 Research Parkway, Suite 501
Orlando, FL 32826

Phone: 407-882-2118
Email: Sandra.Sovinski@ucf.edu

Computer Support
Adiaak Gavarrete, Technology Manager
Phone: 407-823-0546
Email: adiaak@ucf.edu

Paul Turner, Systems Administrator
Phone: 407-823-4084
Email: pturner@ucf.edu

Human Resources

HR Liaisons Program
Roxane Walton, Director
3280 Progress Drive, Suite 100
Orlando, FL 32826

Phone: 823-6706
Email: Roxane.Walton@ucf.edu

Records
Abbee Camen, Records Manager
3280 Progress Drive, Suite 100
Orlando, FL 32826

Phone: 407-823-6382
Email: Abbee.Camen@ucf.edu

Computer Support
Marty Sibley, IT Manager
Phone: 407-823-4106
Email: Marty.Sibley@ucf.edu

International Services Center

Nataly Chandia, Executive Director
12701 Scholarship Drive, Building 81
Orlando, FL 32816

Phone: 407-823-1850
Email: nataly.chandia@ucf.edu

H1B Visas
Beejal Nayee, Coordinator
12701 Scholarship Drive, Building 81
Orlando, FL 32816

Phone: 407-823-1235
Email: Beejal.Nayee@ucf.edu

J1 Visas
Daren Caine, Assistant Director, Academic Support Services
International Services Center
12701 Scholarship Drive, Building 81
Orlando, FL 32816

Phone: 407-823-1852 or 407-823-2337
Email: daren.caine@ucf.edu

Employment & Taxation
Jason Kennedy, Assistant Director
12701 Scholarship Drive, Building 81
Orlando, FL 32816

Phone: 407-823-5491
Email: Jason.Kennedy@ucf.edu

Computer Support
Mikel Alustiza
Email: mikel.etxeberria@ucf.edu

Internationalization

Angel Cardec
Interim Assistant Vice President
Acting Director Center for Multilingual, Multicultural Studies ("CMMS")
12701 Scholarship Drive, Building 81, Room 102-F
Orlando, FL 32816

Phone: 407-823-5455
Email: Angel.Cardec@ucf.edu

Computer Support
Adiaak Gavarrete, Technology Manager
Phone: 407-823-0546
Email: adiaak@ucf.edu

Paul Turner, Systems Administrator
Phone: 407-823-4084
Email: pturner@ucf.edu

IT Security

Chris Vakhordjian, Information Security Officer
PO Box 162500
Building 54, Room 332
Orlando, FL 32816

Phone: 407-823-3863
Email: Chrisv@ucf.edu

Purchasing

Greg Robinson, Director
Orlando Tech Center
12479 Research Parkway
Orlando, FL 32826

Phone: 407-823-5348
Email: Greg.Robinson@ucf.edu

Vendor Input and RPS
Jenna Capp, Program Assistant
Orlando Tech Center
12479 Research Parkway
Orlando, FL 32826

Phone: 407-823-2661
Email: Jenna.Capp@ucf.edu

Computer Support
Carlos Chardon, Department IT Manager
Phone: 407-882-1048
Email: Carlos.Chardon@ucf.edu

Research Administration

Business Incubation

Dr. Tom O'Neal, Executive Director
12201 Research Parkway, Suite 200
Orlando, FL 32826

Phone: 407-882-1120
Email: oneal@ucf.edu

Facility Security

Dela Williams, Facility Security Officer
12201 Research Parkway, Suite 501
Orlando, FL 32826

Phone: 407-882-1123
Fax: 407-882-2233
Email: Dela.Williams@ucf.edu

Financial Compliance

Mary Stanley, Assistant Director
12201 Research Parkway, Suite 501
Orlando, FL 32826

Phone: 407-883-2836

Fax: Fax: 407-882-2233
Email: Mary.Stanley@ucf.edu

Research Foundation

Kim Smith, Director
12201 Research Parkway, Suite 501
Orlando, FL 32826

Phone: 407-823-3062
Fax: 407-882-2233
Email: Kim@ucf.com

Sponsored Programs

Jennifer Shambrook, Director
12201 Research Parkway, Suite 501
Orlando, FL 32826

Phone: 407-823-0387
Fax: 407-823-3299
Email: Jennifer.Shambrook@ucf.edu

Contracts Team Lead
Jane Gentilini, Assistant Director, Contracts & Grants
12201 Research Parkway, Suite 501
Orlando, FL 32826

Phone: 407-882-1452
Fax: 407-823-3299
Email: Jane.Gentilini@ucf.edu

Proposals Team Lead
Celeste Riveria-Nunez, Assistant Director, Proposals
12201 Research Parkway, Suite 501
Orlando, FL 32826

Phone: 407-882-1155
Fax: 407-823-3299
Email: Celeste.Rivera-Nunez@ucf.edu

Engineering Team Lead
Terri Vallery, Assistant Director, Contracts & Grants
12201 Research Parkway, Suite 501

Orlando, FL 32826

Phone: 407-882-1155
Fax: 407-823-3299
Email: Terri.Vallery@ucf.edu

Technology Transfer

Licensing
Svetlana Shtrom, Director, Technology Commercialization
12201 Research Parkway, Suite 200
Orlando, FL 32826

Phone: 407-823-5150
Email: Svetlana.Shtrom@ucf.edu

Computer Support
Ozlem Garibay, Executive Director, Research Information Systems
12201 Research Parkway, Suite 200
Orlando, FL 32826

Phone: 407-882-1122
Email: Ozlem.Garibay@ucf.edu

Research Centers & Institutes

Advanced Materials Processing Center (AMPAC)

Dr. Sudipta Seal
University Distinguished Professor and Director
4000 Central Florida Boulevard
Engineering Building 1, Room 381
Orlando, FL 32816

Phone: 407-823-5277
Email: Sudipta.Seal@ucf.edu

Kari Stiles, Assistant Director
4000 Central Florida Boulevard
Engineering Building 1, Room 381
Orlando, FL 32816

Phone: 407-882-1457
Email: Kari.Stiles@ucf.edu

Kirk Scammon, Research Engineer
Materials Characterization Facility (MCF)
12443 Research Parkway, Suite 304
Orlando, FL 32826

Phone: 407-882-1514
Email: Kirk.Scammon@ucf.edu

Computer Support
Don Harper, Associate Director
Phone: 407-823-2699
Email: Harper@ucf.edu

Pedro Cordero, Assistant Director
Phone: 407-823-4759
Email: Pedro.Cordero@ucf.edu

Center for Research and Education in Optics and Lasers (CREOL)
Dr. Bahaa Saleh, Dean and Director
4304 Scorpius Street, Building 53
Orlando, FL 32816-2700

Phone: 407-823-3326
Email: besaleh@creol.ucf.edu

Mark Wagenhauser, Associate Director of Research Programs
4304 Scorpius Street, Building 53
Orlando, FL 32816-2700

Phone: 407-823-6878
Email: mwagenha@creol.ucf.edu

Amy Perry, Coordinator of Administrative Services
4304 Scorpius Street, Building 53
Orlando, FL 32816-2700

Phone: 407-823-6879
Email: aperry@creol.ucf.edu

Matt Petrone, Purchasing
4304 Scorpius Street, Building 53
Orlando, FL 32816-2700

Phone: 407-823-5138

Email: mpetrone@creol.ucf.edu

Vicky Ortiz, Proposal Coordinator
4304 Scorpius Street, Building 53
Orlando, FL 32816-2700

Phone: 407-823-6825
Email: vsortiz@creol.ucf.edu

Computer Support
Deon Frank, IT Manager
Phone: 407-823-6807
Email: dfrank@creol.ucf.edu

Center for Research in Computer Vision (CRCV)
Dr. Mubarak Shah
UCF Trustee Chair Professor
Director, Center for Research in Computer Vision
4328 Scorpius Street, Suite 245
Orlando, FL 32816-2365

Phone: 407-823-1119
Email: shah@crcv.ucf.edu

Tonya Laprarie, Office Assistant
4328 Scorpius Street, Suite 245
Orlando, FL 32816-2365

Phone: 407-823-4952
Email: Tonya@crcv.ucf.edu

Cherry Place, Assistant
4328 Scorpius Street, Suite 245
Orlando, FL 32816-2365

Phone: 407-963-8999 (cell)
Email: cherry@crcv.ucf.edu

Computer Support
Don Harper, Associate Director
Phone: 407-823-2699
Email: Harper@ucf.edu

Florida Solar Energy Center (FSEC)

James Fenton, Director
1679 Clearlake Road
Cocoa, FL 32922-5703

Phone: 321-638-1002
Email: jfenton@fsec.ucf.edu

Mary Huggins, Director, Business Affairs
1679 Clearlake Road
Cocoa, FL 32922-5703

Phone 321-638-1480
Email: Mary@fsec.ucf.edu

Computer Support
Safvat Kalaghchy, Program Director
Phone: 321-638-1510
Email: Safvat@fsec.ucf.edu

Florida Space Institute
Ramon Lugo, Director
Partnership I Building, Room 214-B
12345 Research Parkway
Orlando, FL 32826-0650

Phone: 407-823-6172
Email: Ramon.Lugo@ucf.edu

Sreela Mallick, Assistant Director, Research Programs
Partnership I Building, Room 214-B
12345 Research Parkway
Orlando, FL 32826-0650

Phone: 407-823-6176
Email: Sreela.Mallick@ucf.edu

Computer Support
Robert Eppig
Phone: 407-823-6196
Email: Robert.Eppig@ucf.edu

Institute for Simulation and Training (IST)
Randall Schumaker,
Partnership II

3100 Technology Parkway
Orlando, FL 32826

Phone: 407-882-3100
Email: shumaker@ist.ucf.edu

Barry Wick, Associate Director
Partnership II
3100 Technology Parkway
Orlando, FL 32826

Phone: 407-882-1316
Email: bwick@ist.ucf.edu

Computer Support
Mark Darty, IT System Support
Phone: 407-882-1374
Email: Mdarty@ist.ucf.edu

STOKES, Advanced Research Computing Center
Dr. Brian Goldiez
Partnership II*
3100 Technology Parkway
Orlando, FL 32826

Phone: 407-882-1302
Email: bgoldiez@ist.ucf.edu

*Actual STOKES System is in Partnership III

Nano-Science Technology Center (NSTC)
Dr. Sudipta Seal
University Distinguished Professor and Director
4000 Central Florida Boulevard
Engineering Building 1, Room 381
Orlando, FL 32816

Phone: 407-823-5277
Email: Sudipta.Seal@ucf.edu

Kari Stiles, Assistant Director
4000 Central Florida Boulevard
Engineering Building 1, Room 381

Orlando, FL 32816

Phone: 407-882-1457
Email: Kari.Stiles@ucf.edu

Ernie Gemeinhart, Lab Manager & Safety Officer
12424 Research Parkway
Suite 407
Orlando, FL 32826

Phone: 407-882-0178
Email: Ernest.Gemeinhart@ucf.edu

Computer Support
Don Harper, Associate Director
Phone: 407-823-2699
Email: Harper@ucf.edu

Siemens Energy Center
Dr. Jayanta Kapat, Director
4000 Central Florida Blvd
Building 44
Orlando, FL 32816

Phone: 407-823-2179
Email: Jayanta.Kapat@ucf.edu

David Amos, Sr. Technical Advisor
4000 Central Florida Blvd
Building 44
Orlando, FL 32816

Phone: 407-823-6279
Email: David.Amos@ucf.edu

Computer Support
Don Harper, Associate Director
Phone: 407-823-2699
Email: Harper@ucf.edu

Pedro Cordero, Assistant Director
Phone: 407-823-4759

Email: Pedro.Cordero@ucf.edu

Colleges & Departments

College of Education & Human Performance

Assistant Dean
Dr. Andrew Daire
Phone: 407-823-2835
Email: Andrew.daire@ucf.edu

Computer Support
Larry Jaffe
Phone: 407-823-6047
Email: Jaffe@ucf.edu

College of Engineering & Computer Science

Dean
Dr. Michael Georgiopoulos
Phone: 407-823-2156
Email: michaelg@ucf.edu

Associate Dean
Dr. Ranganathan Kumar
Phone: 407-823-4389
Email: ranganathan.kumar@ucf.edu

Departments:

Civil, Environmental, and Construction Engineering
Dr. Mohamed Abdel-Aty, Chair
Phone: 407-823-5657
Email: m.aty@ucf.edu

Electrical Engineering and Computer Science
Dr. Gary Leavens, Chair CS
Phone: 407-882-0185
Email: leavens@ucf.edu

Dr. Zhihua Qu, Chair ECE
Phone: 407-823-5976
Email: qu@ucf.edu

Industrial Engineering and Management Systems
Dr. Waldemar Karwowski, Chair
Phone: 407-823-0042
Email: wkar@ucf.edu

Materials Science and Engineering
Dr. Sudipta Seal, Chair
Phone: 407-823-5277
Email: Sudipta.Seal@ucf.edu

Mechanical and Aerospace Engineering
Dr. Challapalli Suryanarayana, Chair
Phone: 407-823-6662
Email: surya@ucf.edu

Jade Laderwarg, Coordinator of Administrative Services
Phone: 407-823-5752
Email: Jade@ucf.edu

Computer Support
Don Harper, Associate Director
Phone: 407-823-2699
Email: Harper@ucf.edu

College of Graduate Studies

Senior Associate Dean
Dr. Max Poole
Phone: 407-823-6215
Email: rhinkle@ucf.edu

Computer Support
Brian Graham, Technology Manager

Phone: 407-823-2846
Email: Brian.Graham@ucf.edu

College of Optics & Photonics

Dean and Director
Dr. Bahaa Saleh
Phone: 407-823-3326
Email: besaleh@creol.ucf.edu

Associate Dean
Dr. David Hagan
(Academic Programs)
Phone: 407-882-6817
Email: hagan@creol.ucf.edu

Computer Support
Deon Frank, IT Manager
Phone: 407-823-6807
Email: dfrank@creol.ucf.edu

College of Sciences

Dean
Dr. Michael Johnson
Phone: 407-823-1911
Email: michael.johnson@ucf.edu

Associate Dean
Dr. Cynthia Young
Phone: 407-823-1912
Email: cynthia.young@ucf.edu

Departments:

Anthropology
Dr. Arlen Chase, Chair
Phone: 407-823-2227
Email: arlen.chase@ucf.edu

Chemistry
Dr. Kevin Belfield, Chair
Phone: 407-823-2246
Email: belfield@ucf.edu

Mathematics
Dr. Piotr Mikusinski, Chair
Phone: 407-823-6284
Email: piotr.mikusinski@ucf.edu

Physics
Dr. Talat Rahman, Chair
Phone: 407-823-2325
Email: talat.rahman@ucf.edu

Computer Support
JP Peters, IT & Communications Director
Phone: 407-823-1209
Email: JP@ucf.edu