Outlining an Export Management and Compliance Program (EMCP) at NDSU
Research Integrity and Compliance
Office of Research and Creative Activity

Implemented, revised, and updated: 04/26/2017 by Dr. Tschetter and Lynn Titus Jr. NDSU Export Control Administrator.
# Table of Contents

**SECTION I: NDSU Policy on Export Controls** ................................................................. 6

**SECTION II: Overview of U.S. Export Control Regulations** ........................................ 6
- Introduction .................................................................................................................. 6
- Export Controls and University Research .................................................................... 8

**SECTION III: EAR versus the ITAR** ............................................................................. 8

**SECTION IV: International Traffic in Arms Regulations (ITAR)** ................................. 9
- Export of Defense Articles and Services ....................................................................... 9
- Items Controlled Under the ITAR ............................................................................... 9
- Definition of Export under the ITAR ........................................................................... 10
- ITAR Classification ...................................................................................................... 10
- ITAR: The United States Munition List (USML) Categories ....................................... 11
- Licenses and Export Authorizations under the ITAR ............................................... 12
  - ITAR Prohibitions: Embargoed Countries under DDTC Regulations ..................... 13

**SECTION V: Export Administration Regulations (EAR): Export of Commercial Dual-Use Goods and Technology** ................................................................. 13
- Items Controlled under the EAR .............................................................................. 13
- Definition of Export and Re-export under the EAR ................................................... 14
- EAR: The Commerce Control List (CCL) Categories ................................................ 14
- Licenses and Export Authorizations under the EAR ............................................... 15

**SECTION VI: OFAC Sanctions** .................................................................................. 16
- OFAC Sanctions Program and Barred Entities/Restricted Parties’ Lists ................. 16
- Sanctioned Countries ................................................................................................. 16
- Terrorist and Other Barred Entity Lists ..................................................................... 17
- Anti-Boycott Restrictions ......................................................................................... 17

**SECTION VII: Penalties for Export Violations** ............................................................. 18

**SECTION VIII: Key Issues for University Research** .................................................. 19
- Deemed Exports ........................................................................................................ 19
- U.S. and Foreign Persons ........................................................................................................... 20
- Information Not Subject To/Excluded From Export Controls ........................................... 20
- Publicly Available ....................................................................................................................... 21
  ITAR provision ............................................................................................................................. 21
  EAR provision ............................................................................................................................... 21
- Educational Information Exclusion ............................................................................................. 21
  More on the Educational Information Exclusion: ......................................................................... 22
- Fundamental Research Exemption (FRE) .................................................................................. 23

SECTION IX: NDSU Procedures on Export Controls ................................................................. 24
- Core Processes: ............................................................................................................................ 24
- Technology Control Plans (TCPs) .............................................................................................. 25
- Physical Security ........................................................................................................................ 26
- EAR Classification ...................................................................................................................... 26
- Biosafety .................................................................................................................................. 27
- Sponsored Research ................................................................................................................... 28
- Bona Fide Employee Exemption ................................................................................................. 28
- International Collaboration Agreements .................................................................................... 29
- International Visitors and Activities .......................................................................................... 30
  Authorizations to Visit NDSU ...................................................................................................... 30
  Responsibility for International Activities .................................................................................. 30
- Travel Abroad ............................................................................................................................. 31
- Shipping Services ........................................................................................................................ 32
  General Shipping and Receiving .................................................................................................. 32
- Record Keeping ........................................................................................................................... 33
- OFAC Restrictions ..................................................................................................................... 33
- Issue Reporting and Notification ............................................................................................... 33
- Export Control Training and Assessment .................................................................................. 34
  Training ..................................................................................................................................... 34
  Export Assessment ...................................................................................................................... 35

SECTION X: Export Control At NDSU ....................................................................................... 35
- Export Control Administrator ..................................................................................................... 35
  Export Control Analysis .............................................................................................................. 36
- Sponsored Programs Administration (SPA)/Office of Research and Creative Activity (RCA) ............................................................................................................ 37
- Information Technology ............................................................................................................. 38
• Key University Managers and Research Administrators ..................................38
• Business Administrators ..................................................................................39
• Principal Investigators (PIs) ..............................................................................39
• Faculty, Staff, and Other Applicable NDSU Personnel ..................................39
• Procurement .....................................................................................................40
• New Employees at NDSU ................................................................................40
• Provost/International Offices ..........................................................................40
  I-129 Certification ................................................................................................40
• Restricted Parties’ Screenings .........................................................................41
• Distance and Continuing Education ...............................................................42
• High Performance and Advanced Computer (HPC) Facilities/CCAST ..........42
• Web-Based Services and Licensed Software Agreements, Etc. .......................42
• Technology Commercialization and Transfer ...............................................42
• University Foundations ...................................................................................43
• Incubator and Spin-off Activity .......................................................................43
• Disciplinary Actions and Non-Retaliation .......................................................43

SECTION XI: Appendixes ..................................................................................44

• Appendix 1 — Glossary ....................................................................................44
  Glossary of Export Controls Terms & Abbreviations ......................................44
• Appendix 2 — Web Resources .........................................................................51
  Website References ...........................................................................................51
  U.S. Agencies Regulating Export Controls ....................................................51
  Export Control Regulations .............................................................................51
  Other Agencies Involved in Export Controls .................................................52
  Department of Homeland Security – U.S.
    Immigration and Customs Enforcement (ICE) ...........................................53
  Federal Bureau of Investigation .......................................................................53
  Other Resources ................................................................................................53
• International Export Controls/Regimes..........................................................54
• Appendix 3: Forms .....................................................................................55
  NDSU Technology Control Plan ................................................................57
  NDSU Briefing Certification for Additional Project Personnel ......................64
  NDSU Technology Control Plan Departure Statement ................................66
  NDSU Technology Control Plan Closeout Form ........................................67
  NDSU International Travel Briefing .............................................................71
  NDSU Certification on the Handling of Export controlled Items/Information .79
  NDSU Full-time Bona Fide Employee Certification and Written Notification 81
  NDSU Export License Exception (TMP) ......................................................83
  NDSU Export License Exception (BAG) .....................................................85
  NDSU Sample Agreement (Article Language) ..........................................87
  NDSU Export Control International Shipment Review Form/ Material Transfer Checklist ..........................................................90
  Brochure ...................................................................................................92
  NDSU Export Control Training PowerPoints ..........................................94
  NDSU Export Controls Controlled/Not Controlled Project Chart ..................96
• Appendix 4: Legal Disclaimer .................................................................97
• Appendix 5: Revision Record .....................................................................97
  ITAR Label Example ..................................................................................98
  ITAR Marking Cabinets/Lockers/Rooms Example ....................................99
  ITAR Marking Shipping Label Example ..................................................100
  Fundamental Research Example ..............................................................101
  ITAR/EAR Research Computing Encryption Example Procedures ............102
SECTION I: NDSU Policy on Export Controls

North Dakota State University is committed to acting in accordance with all applicable U.S. Government export regulations. NDSU requires ALL faculty, staff, students, and other University personnel to be aware of, and comply with, U.S. export control laws and regulations, and NDSU’s policy and procedures thereto (See NDSU Policy 722).

SECTION II: Overview of U.S. Export Control Regulations

Introduction

Export controls are Federal statutes and regulations that govern the transfer of certain goods, technologies, services, data, and money to non-U.S. persons and locations. The U.S. export control system has been shaped by U.S. national security, economic interests, and foreign policy, and is aimed at achieving various related objectives. These controls generally restrict the export of products and services based on the type of product and the destination of the export.

Export controls affect all scientific (and many other) disciplines involving sponsored or non-sponsored research; contracts; agreements; business and service transactions with restricted countries and restricted end-users; shipping items to foreign destinations; international travel; and the hiring of foreign nationals (persons without green cards).

The U.S. Government defines exports to include not only tangible, or “physical,” items – such as software, biological materials, chemicals, and equipment – but also intangible information, which may include research data, technology, engineering designs, and ideas. Further, an export is defined not only as an actual physical shipment or a hand-carried item taken out of the United States, but also includes electronic and voice transmissions out of the U.S. (e.g., an e-mail or a phone call to a colleague at a foreign institution, or remotely accessing controlled documents while travelling internationally).

Exports also include the release of technology to foreign nationals within the U.S. (e.g., laboratory access to foreign nationals for whom the item is controlled); the provision of training or services involving controlled equipment to foreign nationals in the U.S. or abroad; and providing services to, or engaging in transactions with, entities and individuals who are on embargo or specially designated nationals lists.

North Dakota State University (NDSU, or the “University”) primarily is concerned with three sets of export control regulations:

- The Export Administration Regulations (EAR), administered by the Department of Commerce.
- The International Traffic in Arms Regulations (ITAR), administered by the Department of State.
- The Office of Foreign Assets Control (OFAC), administered by the Department of Treasury.

These export control regulations are part of a complex export control system that has been in existence since the 1940s. Each agency has its own procedures for enforcement, but violations of any of these regulations can result in significant institutional and personal penalties, including fines of up to $1,000,000 per violation; incarceration for up to 20 years; and the loss of future exporting privileges. This NDSU “Export Controls Compliance Manual” (‘’Manual’’) provides an overview of export controls and how they apply to the activities of University personnel. It also outlines the Export Management and Compliance Program (EMCP) at NDSU.

Export control issues can arise in a variety of surprising circumstances, and are not always intuitive. For example, NDSU may need a U.S. Government export license before disclosing controlled technical data to a non-U.S. researcher, even when the disclosure takes place entirely on University grounds within the U.S. Given this complexity, the NDSU community should seek guidance from NDSU’s Export Control Administrator (ECA) when dealing with export control issues, especially in the following circumstances:

- Conducting research that involves defense, military, weapons, or space technologies.
- Whenever documents from sponsors or other parties refer to the EAR, the ITAR, or export controls generally.
- Whenever sponsors attempt to impose publication or personnel access restrictions on research activities.
- Before receiving export-controlled technical information from an outside party, such as an industry or U.S. Government research sponsor.
- Before partnering/collaborating with a foreign person or company.
- Whenever foreign persons/foreign nationals/foreign visiting scholars are proposing to participate in research.
- Before hosting foreign visiting scholars or students for the purpose of touring research labs and facilities that contain export-controlled items.
- Before accepting hardware, software, technology, or technical data from an outside party (such as an industry sponsor) to be used in a project as part of an instructional course.
- Before exporting from the U.S. any technology, equipment, materials, or chemical or biological agents (including toxins and genetic elements) on the EAR’s Commerce Control List (e.g., laptops, GPS equipment, other hand-held mobile devices, or other devices containing encrypted software).
- Before handling or exporting from the U.S. any hardware, software, technical data, or services subject to the ITAR.
- Before attending a conference where registration is limited to U.S. citizens, or attending a conference outside of the U.S., or planning or participating in a conference where foreign colleagues and/or foreign students may be present.
Before supplying certain technologies or data at a closed conference (e.g., a meeting that is not open to all technically qualified members of the public, and attendees are not permitted to take notes).

Before providing anything of value to someone from a sanctioned country, or on the entity list, denied persons list, debarred or excluded parties’ lists, or any other restricted parties’ lists.

Before any international travel, and especially before travel to an embargoed country: Cuba, Iran, North Korea, Sudan, or Syria.

Contact NDSU’s Export Control Administrator (ECA) at 701.231.6455 or ndsu.exportcontrols@ndsu.edu with any questions or concerns regarding export control laws, or NDSU policy and procedures.

Export Controls and University Research

Technological innovations and advantages are the machines that power U.S. national security and economic interests. Many of the nation’s cutting-edge technologies are being discovered by both U.S. and foreign national students, scholars, faculty, and researchers at universities across the nation. U.S. policymakers recognize that foreign students and foreign researchers have made substantial contributions to research efforts in this country. However, the prospective transmission of controlled information and defense-related technologies to foreign home countries could have a detrimental impact upon U.S. national interests.

Thus, export controls present an interesting challenge to universities because they require a balance between U.S. national security and economic concerns with the traditional concept of free and unrestricted academia. Universities are subject to the same export controls as other U.S. organizations, companies, and individuals, so it is critical that NDSU personnel know what an export is and when a license may be required. The good news is that most NDSU activities fall within one of the export exemption or exclusion categories. The bad news is that despite these generally useful exemptions/exclusions, some NDSU activities may remain subject to export control requirements and require restrictions on access, or even export licensure.

SECTION III: EAR versus the ITAR

There are a number of key differences between two of the primary sets of export control regulations, the Export Administration Regulations (EAR, administered by the Department of Commerce) and the International Traffic in Arms Regulations (ITAR, administered by the Department of State).

In general, the EAR is clearer and more specific in its coverage than the ITAR. Primarily, the EAR is concerned with “dual-use” items, or those tangible items, software, and/or technology that have both commercial and military or proliferation applications. Under the EAR’s “dual-use” rules,
controls are based on the type of item, the end use/user, and the destination country. Not all items are controlled for all countries.

Conversely, the ITAR regulates tangible and intangible items that are inherently military in nature. The ITAR also contains the concept of “defense services,” which includes furnishing either training or technical data related to ITAR-controlled items to foreign persons either in the U.S. or abroad. Under ITAR’s defense regulations, all exports of defense articles and defense services are controlled.

Additionally, both sets of regulations treat “fundamental research” (explained in “Key Issues for University Research,” below) differently: in the EAR, it is a separate and distinct category, whereas in the ITAR, it is subsumed under “public domain.”

Section 121.1 of the ITAR contains the United States Munitions List (“USML”), and includes the commodities and related technical data and defense services controlled for export purposes. The USML should always be checked first to ascertain whether or not an item or technology is export-controlled. The EAR controls items on the Commerce Control List (CCL), which should be checked after the USML. The CCL only places export controls on items/technology when they are not contained on the USML (and, therefore, controlled by the ITAR).

**SECTION IV: INTERNATIONAL TRAFFIC IN ARMS REGULATIONS (ITAR)**

**Export of Defense Articles and Services**

Under the International Traffic in Arms Regulations (ITAR, 22 C.F.R. §§ 120-130 [www.pmddtc.state.gov/regulations_laws/itar.html]), the Department of State Directorate of Defense Trade Controls (DDTC) administers the export and re-export of defense articles, defense services, and related technical data from the United States to any foreign destination – or to any foreign person, whether located in the United States or abroad.

The ITAR controls not only end items – such as radar and communications systems, military encryption, and associated equipment – but also the parts and components that are incorporated into the end item. (For example, a commercial radio that normally would not be controlled under the ITAR becomes a controlled defense article if it contains an ITAR-controlled microchip.) Certain non-military items, such as commercial satellites – and certain chemical precursors, toxins, and biological agents – also are controlled.

**Items Controlled Under the ITAR**

The ITAR uses three different terms to designate export-controlled items: defense articles, technical data, and defense services.

Defense Article: any item or technical data specifically designed, developed, configured, adapted, or modified for a military, missile, satellite, or other controlled use listed on the USML. Defense article also includes models, mock-ups, or other items that reveal technical data relating to items designated in the USML.
Technical Data: any information for the design, development, assembly, production, operation, repair, testing, maintenance, or modification of a defense article. Technical data may include drawings or assembly instructions, operations and maintenance manuals, and email or telephone exchanges where such information is discussed.

Defense Service: providing assistance, including training, to a foreign person in the United States or abroad in the design, manufacture, repair, or operation of a defense article, as well as providing technical data to foreign persons. Defense services also include informal collaboration, conversations, or interchanges concerning technical data.

**Definition of Export under the ITAR**

The ITAR defines the term “export” broadly. Again, 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 also defines as an “export” the passing of information or technology to foreign nationals even in the United States (“deemed export”). The following are examples of exports:

- **Exports of articles from 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, inside or outside the United States.

- **Extra-territorial transfers:**
  - The re-export or re-transfer of defense articles from one foreign person to another, and 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.

- **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.

**ITAR Classification**

While DDTC has jurisdiction over deciding (“jurisdictional determination”) whether an item is ITAR- or EAR-controlled, it encourages exporters to self-classify the item. If doubt exists as to whether an article or service is covered by the USML, upon written request in the form of a Commodity Jurisdiction (“CJ”) request, DDTC will provide advice as to whether a particular article is a defense article subject to the ITAR, or a dual-use item subject to Commerce Department licensing. Determinations are based on the origin of the technology (i.e., as a civil or military article), and whether it is predominantly used in civil or military applications.
The process of ensuring that all defense articles, technical data, and defense services are properly identified and treated as such is fundamental to NDSU’s export controls compliance program. ITAR determinations govern licensing and authorization requirements for access by foreign nationals/foreign persons in NDSU laboratories, as well as transfers and exports out of the country. In the event a clear jurisdictional determination cannot be made from the available relevant information (i.e., there is ambiguity as to whether the item may be alternatively controlled by the Department of Commerce as “dual-use,” or not controlled at all), NDSU’s ECA, in conjunction with others, will apply for a CJ from DDTC. (Note: CJs are potentially complex documents that require significant time and preparation, the results of which can have significant implications for NDSU’s current and future endeavors.)

Contact NDSU’s ECA at 701.231.6455 or ndsu.exportcontrols@ndsu.edu when classifying items under the ITAR or the EAR.

One important exception to the ITAR laboratory access restrictions involves the ITAR items that NDSU self-invents, whether or not patented, as the product of fundamental research (discussed in greater detail in “Key Issues for University Research,” below). When both the process and the results are intended for publication and dissemination, a restriction may not apply. However, outbound ITAR exports will ALWAYS trigger a license requirement analysis. Further, use of an ITAR item that NDSU procures or licenses from a vendor or third party, to develop or inform its fundamental research, likewise may trigger access restrictions (because the procured/licensed item is not, per se, self-invented). In other words, the Fundamental Research Exemption may exempt the results of your research – but certain components (controlled software or another controlled item/technology) used in the process by which you have achieved fundamental research results likely will remain export-controlled.

The requirement to determine whether an item meets the definition of a defense article may be triggered at numerous phases of the research process, beginning with the earliest stages of concept/design. Many NDSU activities and functions – such as Purchasing, Human Resources, and Information Technology Services – are directly affected by this requirement. Therefore, all affected NDSU personnel must be aware of the jurisdiction determination process, as assisted by the ECA, and remain aware of all locations where such items are being used or stored. Once the jurisdiction determination has been made, this information shall be provided by the ECA to all affected parties.

**ITAR: The United States Munition List (USML) Categories**

Once an item has been determined to fall under ITAR jurisdiction, its USML category must be identified. The USML designates particular categories and types of equipment as defense articles and associated technical data and defense services. The USML is available at: [www.pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_121.pdf](http://www.pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_121.pdf).

The USML divides defense items into 21 categories:

I. Firearms, Close Assault Weapons, and Combat Shotguns
II. Guns and Armament
III. Ammunition/Ordnance
IV. Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs, and Mines
V. Explosives, Propellants, Incendiary Agents, and their Constituents
VI. Vessels of War and Special Naval Equipment
VII. Tanks and Military Vehicles
VIII. Aircraft and Associated Equipment
IX. Military Training Equipment
X. Protective Personnel Equipment and Shelters
XI. Military Electronics
XII. Fire Control, Range Finder, Optical, and Guidance and Control Equipment
XIII. Auxiliary Military Equipment
XIV. Toxicological Agents, Including Chemical Agents, Biological Agents, and Associated Equipment
XV. Spacecraft Systems and Associated Equipment
XVI. Nuclear Weapons, Design, and Testing Related Items
XVII. Classified Articles, Technical Data, and Defense Services Not Otherwise Enumerated
XVIII. Directed Energy Weapons
XIX. [Reserved]
XX. Submersible Vessels, Oceanographic, and Associated Equipment
XXI. Miscellaneous Articles

**Licenses and Export Authorizations under the ITAR**

Items and activities controlled under the ITAR may require licensing or other authorization from the DDTC. Unless otherwise authorized, ITAR items of any kind must not be exported, or accessed by a non-U.S. person, without proper licensing or authorization from the Department of State. The specific type of license or authorization required depends on the type of export transaction subject to control (for example, temporary versus permanent export licenses). ITAR authorizations also include Technical Assistance Agreements (TAAs) and Manufacturing License Agreements (MLAs). For more information on ITAR authorizations, please refer to the DDTC web site.

Each type of license requires its own specific set of data points that DDTC collects through its DTrade application process and associated documentation, such as Transmittal Letters. A Transmittal Letter describes the transaction in detail, including end use, end user profile, and ultimate disposition of the item, amongst other things. Therefore, data requirements are specific to the type of license/authorization being used.
Before NDSU applies for an ITAR license, it must comply with all DDTC requirements pertaining to registration as an ITAR exporter, Empowered Official (EO) designation, and DTRADE User status.

All ITAR license applications or other Government approvals must be submitted by NDSU’s Export Control Administrator.

Contact NDSU’s ECA at 701.231.6455 or ndsu.exportcontrols@ndsu.edu with EAR or ITAR licensing.

Typically, any U.S. person or entity that manufactures, brokers, or exports defense articles or services must be registered with DDTC. Registration is required prior to applying for a license, or taking advantage of some license exemption. NDSU generally is not required to register with DDTC because its researchers tend to be engaged only in the creation of unclassified technical data, or only in the fabrication of articles for experimental or scientific purposes (including research and development). However, if NDSU desires to involve foreign nationals in ITAR-controlled research, it must register with the DDTC to apply for a license or take advantage of certain license exemptions.

**ITAR Prohibitions: Embargoed Countries under DDTC Regulations**

In general, no ITAR exports may be made either under license or license exemption 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 at [www.pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_126.pdf](http://www.pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_126.pdf).

**SECTION V: Export Administration Regulations (EAR): Export of Commercial Dual-Use Goods and Technology**

The Department of Commerce, Bureau of Industry and Security (“BIS”), regulates the export of “dual-use” items, or items designed for potentially commercial purposes that can have military applications, under the Export Administration Regulations (EAR). 15 C.F.R. §§ 730-774 (available at [www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear](http://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear)). The EAR covers both exports of these commodities to and from the U.S., as well as the transfer of technical data about them to a foreign national both inside and outside the U.S. It also covers the re-export of foreign commodities incorporating controlled U.S. commodities.

**Items Controlled under the EAR**

The following summarizes the types of items controlled under the EAR:
Commodities: includes finished or unfinished goods ranging from high-end microprocessors to airplanes to ball bearings.

Manufacturing Equipment: 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: includes certain alloys and chemical compounds.

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

Technology: As defined in the EAR, technology includes both technical data and services. Unlike the ITAR, generally there is no distinction between the two. However, the EAR may apply different standards to technology for “use” of a product versus for the “design” or “manufacture” of the product. Examples of technical data/technology include: blueprints, plans, diagrams, models, formulae, tables, engineering designs, and specifications; and manuals and instructions written or recorded on other media or devices, such as discs.

Definition of Export and Re-export under the EAR

Export. An export is defined as the actual shipment or transmission of items subject to the EAR out of the United States. The EAR is similar to the ITAR in that it covers intangible exports of “technology,” including source code – as well as physical exports of items.

Deemed Export. Under the EAR, the release of technology to a foreign national (including foreign national graduate or post-doc students and researchers) in the U.S. is “deemed” to be an export, even though the release took place entirely within the U.S. Deemed exports may occur through such means as a demonstration, oral briefing, or a visit to a laboratory (e.g., visual inspection), as well as through an electronic transmission of non-public data that is received abroad.

Re-export. Similarly to the ITAR, the EAR attempts to impose restrictions on the re-export of U.S. goods – i.e., the shipment or transfer to a third country of goods or technology originally exported from the United States.

Deemed Re-export. Finally, the EAR defines “deemed re-exports” as the release of technology by a foreign national, who has been licensed to receive it, to the national of another foreign country, who has not been licensed to receive the technology. (For example, ECCN 5E001 technology may be exported to a university in Ireland under the license exception for technology and software, but might require a deemed re-export license authorization before being released to a Russian foreign national student or employee of that university in Ireland.)

EAR: The Commerce Control List (CCL) Categories

The CCL (www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl) provides a list of very specific items that are EAR-controlled, divided into ten categories:

CATEGORIES:
0. Nuclear-related Items and Miscellaneous Items
1. Materials, Chemicals, Microorganisms and Toxins
2. Materials Processing
3. Electronics
4. Computers
5. Telecommunications and Information Security (Encryption)
6. Sensors and Lasers
7. Navigation and Avionics
8. Marine (Vessels, Propulsion, and Equipment)
9. Propulsion Systems and Aerospace (Includes Aircraft and Aircraft Engines)

In addition to these ten categories, each category is subdivided into five groups, designated by the letters A through E: (A) Equipment, Assemblies, and Components; (B) Test, Inspection and Production Equipment; (C) Materials; (D) Software; and (E) Technology.

For example, e coli 0157:H7 – a shiga toxin-producing agent – is classified as ECCN 1C351.c.17. Under the export control regulations, 1C351.c.17:

1 = found in Category 1 of the CCL (“Materials, Chemicals, Microorganisms and Toxins”)

Subcategory C= Materials

351 = 1 of 5 technology ECCNs (relating to disposal technology)

Small c = Bacteria identified on the Australia Group (AG) “List of Biological Agents for Export Control”

Reasons for export controls: CB (Chemical & Biological Weapons); CW (Chemical Weapons); and AT (Anti-terrorism)

NOTE: “Deemed exports” (the release to a foreign national in the United States of “technology” or “source code” “required” for the “development,” “production,” or “use” of the controlled pathogen or controlled equipment) only apply to the release to a foreign national of technology and source code in Products Groups D and E on the Commerce Control List. While deemed exports do not apply to Products Groups A, B, and C, material commodities – including systems, equipment, and components (Product Group A); test inspection and production equipment (Product Group B); and raw materials (Product Group C – pathogens are controlled in ECCNs 1C351 and 1C352) – all would require authorization for physical export, and may require a license depending on the recipient’s country.

Licenses and Export Authorizations under the EAR

Under the EAR, exports of controlled items that do not meet certain license exceptions require prior authorization (licensing), before export, from the Bureau of Industry and Security (BIS). This
requirement applies to outbound shipments of items or data; re-exports of items or data; and export of a non-controlled item to a person or entity identified on one of the Government’s restricted entity lists. As with the ITAR, there are several different types of BIS licenses required (e.g., individual licenses, deemed export licenses, etc.), depending on the type of transaction. However, all license templates may be found in the BIS SNAP-R licensing system (an on-line system to request licenses and authorization), which will specify the required range of data necessary for each application type.

⚠️ All BIS/EAR license applications or other Government approvals must be submitted by NDSU’s Export Control Administrator.

Contact NDSU’s ECA at 701.231.6455 or ndsu.exportcontrols@ndsu.edu with EAR or ITAR licensing.

SECTION VI:
OFAC Sanctions

OFAC Sanctions Program and Barred Entities/Restricted Parties’ Lists
The Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury administers and enforces economic and trade sanctions, based on U.S. foreign policy and national security goals, against targeted foreign countries and regimes; terrorists; international narcotics traffickers; those engaged in activities related to the proliferation of weapons of mass destruction; and other threats to the national security, foreign policy, and/or economy of the United States. OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates; are multilateral in scope; and involve close cooperation with allied governments.

Contact NDSU’s ECA at 701.231.6455 or ndsu.exportcontrols@ndsu.edu for assistance with OFAC issues.

Sanctioned Countries
U.S. economic sanctions broadly prohibit most transactions between a U.S. person and persons or entities in an embargoed country, including Cuba, Iran, North Korea, Syria, and Sudan. This prohibition includes importation and exportation of goods and services, whether direct or indirect, as well as “facilitation” by a U.S. person of transactions between foreign parties and a sanctioned country. (For example, sending a check to an individual in Iran could require an OFAC license, or be prohibited.)

More limited sanctions may block particular transactions, or require licenses under certain circumstances, for exports to a number of countries, including, but not limited to, Burma, Liberia,
and Zimbabwe. Because this list is not complete and is subject to change, please visit http://www.treasury.gov/resource-center/sanctions/Pages/default.aspx.

**Terrorist and Other Barred Entity Lists**

Various U.S. Government agencies also maintain a number of lists of individuals or entities barred or otherwise restricted from entering into certain types of transactions with U.S. persons. Particularly since 9/11, U.S. companies are becoming more assertive in drafting contractual terms with foreign companies related to these lists. Such lists must be screened to ensure that NDSU does not engage in a transaction with a barred entity.

- NDSU uses Visual Compliance™ to expedite screening of these and other lists. Contact NDSU’s ECA/RCA for assistance screening individuals and entities.

Examples of terrorist and other barred entity lists include:

- Specially Designated Nationals and Blocked Persons List (“SDN List”). Maintained by OFAC, this is a list of barred terrorists, narcotics traffickers, and persons and entities associated with embargoed regimes. Generally, all transactions with such persons are barred.
- List of Debarred Parties. The Department of State bars certain persons and entities from engaging in the export or re-export of items subject to the USML. Note: The number of countries subject to a U.S. arms embargo is much broader than those subject to OFAC embargoes.
- Denied Persons List. These are individuals and entities that have had their export privileges revoked or suspended by BIS.
- Entity List. These are entities identified as being involved in proliferation of missile technology, weapons of mass destruction, and related technologies.
- Unverified List. These are foreign persons and entities for which BIS has been unable to verify the nature of their operations. While transactions with these entities are not barred, special due diligence is required.
- Nonproliferation Sanctions. These lists are maintained by the Department of State.

**Anti-Boycott Restrictions**

A subset of the EAR, known as the Anti-Boycott Regulations, prohibits U.S. persons from participating in – or even agreeing to participate in – a boycott that is not consistent with U.S. Government policy. These regulations were created specifically in response to the Arab League’s boycott of Israel, which the U.S. Government does not support.

The Anti-Boycott provisions prohibit the following activities (amongst others):

- Agreeing to refuse, or actually refusing, to do business with a boycotted country (e.g., Israel) or a blacklisted person/company.
- Agreeing to discriminate, or actually discriminating, against persons based on race, religion, sex, national origin, or nationality (such as agreeing not to hire Israeli nationals).
Agreeing to furnish, or actually furnishing, information about the race, religion, sex, or national origin of personnel.

Agreeing to furnish, or actually furnishing, information about relationships with a boycotted country or blacklisted person/company.

Agreeing to pay, or actually paying/otherwise implementing, letters of credit that include requirements to take boycott-related actions prohibited by these regulations.

The countries most implicated in anti-boycott scenarios include Bahrain, Bangladesh, Kuwait, Lebanon, Libya, Oman, Qatar, Saudi Arabia, Syria, the United Arab Emirates, and Yemen. Note: There are strict reporting requirements even where the U.S. person or entity refuses to participate in a requested boycott action.

More information on BIS’ Office of Anti-Boycott Compliance (OAC) can be found at www.bis.doc.gov/index.php/enforcement/oac.

NDSU personnel who encounter boycott-related language in any transaction must contact the ECA (701.231.6455 or ndsu.exportcontrols@ndsu.edu) immediately before taking any further action.

SECTION VII:
Penalties for Export Violations

Generally, any person or entity that brokers, exports, or attempts to export a controlled item without prior authorization, or in violation of the terms of a license, is subject to penalties. Violators may incur both criminal and civil penalties. A series of violations added up by the penalizing agency, or violations occurring over a period of time, may result in millions of dollars of penalties. In addition to monetary penalties, jail time and revocation of exporting privileges may be imposed.

IMMEDIATELY contact NDSU’s Export Control Administrator or the Director of Research and Creative Activity, if you anticipate, suspect, or have knowledge of any NDSU non-compliance (past, present, or future) with U.S. export controls laws and regulations.

In assessing penalties, DDTC, BIS, and OFAC will consider a number of factors, both aggravating and mitigating. Mitigating factors may include whether:

- The disclosure was made voluntarily.
- This was a first offense.
- The entity had compliance procedures.
- Steps were taken to improve compliance after discovery of violations.
- The incident was due to inadvertence, mistake of fact, or good faith misapplication of the laws.
Aggravating factors may include: (1) willful or intentional violations; (2) failure to take remedial action after discovery; (3) lack of a compliance program; and (4) deliberate efforts to hide or conceal a violation. For more information, see “Detecting and Reporting Violations” below.

SECTION VIII:
**Key Issues for University Research**

**Deemed Exports**

While exports commonly are associated with the shipment of a tangible item across the U.S. border, export controls have a much broader application. One of the most difficult issues with respect to export controls is the fact that an export is defined to include the transfer of controlled information or services to foreign nationals even when the transfer takes place within the territory of the United States. Though taking place inside the U.S., the transfer is “deemed” to be an export (as if exporting to the home country of the foreign national). The term “deemed export” is unique to the EAR.

Both the ITAR and the EAR provide for deemed exports, even though in the case of defense exports, the regulations generally speak of exports. While the ITAR distinguishes between the transfer of technical data and defense services, the EAR generally provides for the release of technology. Such transfer or release may be made through oral, visual, or other means.

A deemed export may occur in many ways, including:

- A demonstration,
- Visual inspection of facilities or lab/work spaces,
- An oral briefing,
- A telephone call or message,
- A laboratory or plant visit,
- Presenting at conferences and meetings,
- Faxes or letters,
- Hand-carried documents, hardware, or drawings,
- Design reviews,
- The exchange of electronic communication,
- Carrying a laptop with controlled technical information/software to an overseas destination,
- Posting non-public data on the Internet or the Intranet, or
- Collaboration with other universities/research centers through research efforts.

The issue of deemed exports is particularly relevant to university research because of the activities that normally take place at a university. While a university may be involved in the shipment abroad of equipment or machinery to participate in a conference, a joint project, or equipment loan programs, most often faculty and students are engaged in teaching and research. Whenever
teaching or research are related to controlled equipment or technology, foreign students’ or foreign researchers’ involvement may trigger export control compliance issues.

NOTE: Again, under the EAR, “deemed exports” only apply to the release to a foreign national of technology and source code in Products Groups D and E on the Commerce Control List – NOT to products groups A, B, or C. See “EAR: The Commerce Control List (CCL) Categories,” explained above.

U.S. and Foreign Persons

For purposes of defense and dual-use exports, a U.S. person is defined as a:

- U.S. entity or a U.S. citizen,
- Person lawfully admitted for permanent residence in the United States (green card holder),
- Person who is a protected individual under the Immigration and Naturalization Act.

A U.S. person may be engaged in activities that are export-controlled, unless there are some additional restrictions that limit participation to U.S. citizens.

The regulations define foreign person/foreign national as anyone who is not a U.S. person. BIS looks at the person’s most recent citizenship or permanent residence. DDTC looks at the person’s country of origin (i.e., country of birth) and all current citizenships. Note that the definitions for a U.S. and a foreign person differ for purposes of the OFAC sanctions.

Information Not Subject To/Excluded From Export Controls

The vast majority of teaching and research activities at NDSU falls within one or more of several exemptions and exclusions from U.S. export licensing requirements. However, it is important to understand how the laws apply to NDSU activities, as well as NDSU’s corresponding compliance obligations. The onus is on NDSU to understand and comply with these regulations.

Fortunately, most – but not all – research activities on campus fall under the “fundamental research exemption” (FRE), discussed further along in this Section. This exemption provides that basic and applied research activities that are free from restrictions on publication or access will be excluded from export controls. Other exemptions apply to information shared in the conduct of teaching activities on campus within the U.S., as well as to information that already exists in the public domain. U.S. export regulations are complex and continually changing, so each activity must be considered on an individual basis.

Contact NDSU’s ECA at 701.231.6455 or ndsu.exportcontrols@ndsu.edu with export exemptions/exclusions.
Publicly Available

The ITAR and the EAR do not control information that is published and/or generally accessible or available to the public (and hence, information that does not require export licensing). Note that even though the two regimes have similar scope, the ITAR and the EAR vary in the specific information that qualifies as “publicly available.”

**ITAR provision**
The ITAR describes such information as “information in the public domain.” The information in the public domain may be obtained through:

- Sales at newsstands and bookstores.
- Subscription or purchase without restriction to any individual.
- Second-class mailing privileges granted by the U.S. Government.
- At libraries open to the public.
- Patents available at any patent office.
- Public release in any form after approval of the cognizant U.S. Government agency.
- Fundamental research in the United States.
- Unlimited distribution at a conference, meeting, seminar, trade show, or exhibition, generally accessible to the public, in the United States.

**Note:** Unlike the EAR, the ITAR limits participation in conferences/similar events to those that are taking place in the United States.

**EAR provision:**
The EAR does not control 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.
- Release at an open conference, meeting, seminar, trade show, or other gathering open to the public.

**Note:** The EAR does not specify where an open conference, meeting, seminar, or trade show must take place – and thus allows, for example, participation at a foreign conference – so long as the conference is open to all technically qualified members of the public, and attendees are permitted to take notes.

**Educational Information Exclusion.**
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 practical effect is
that most university courses clearly are excluded from export controls, and that the information
released in the courses is considered to be publicly available (and, therefore, excluded from
controls).

To ensure that a course dealing with advanced or sensitive technology qualifies for the Educational
Information Exclusion, first determine which export control regime has jurisdiction over the
course’s technology, and then apply the criteria for that regime.

ITAR provision: The ITAR specifically provides that the definition of “technical data” does not
include information concerning general scientific, mathematical, or engineering principles
commonly taught in schools, colleges, and universities. This ITAR provision is less broad
(specified areas, “principles” rather than “information”) and more ambiguous (“general”,
“commonly taught”) than the EAR exclusion.

EAR provision: The EAR provides that publicly available “educational information” is not subject
to the EAR, if it is released by instruction in catalog courses and associated teaching laboratories of
academic institutions. This EAR provision is more broad and unambiguous (except encryption
technology, which is complex) than the ITAR exclusion. Additionally, the EAR Educational
Information Exclusion does not extend to the release of information in research labs not associated
with catalog courses.

Therefore, a university graduate course on the design and manufacture of very high-speed
integrated circuitry will not be subject to export controls, even though the technology is on the
CCL – the key factor being that the information is provided by instruction in a catalog course.
International students from any country may attend this course because the information is not
controlled.

Further, the information will not be controlled even if the course contains recent and unpublished
results from laboratory research, so long as the university did not accept separate obligations with
respect to publication or dissemination (e.g., a publication restriction under Federal funding).

More on the Educational Information Exclusion:

- Material released in catalog courses is considered “publicly available”, and therefore
  excluded from U.S. export controls, by delivery in instruction at universities in the U.S. or
  abroad, except for: (1) encryption (EAR); (2) principles not commonly taught (ITAR); and
  (3) sensitive nuclear technology (DoE).

- Courses with no export controls content/connection: many courses in business; media
  studies; economics; foreign languages; history; literature; management; music and theater
  arts; political science; writing and humanistic studies; and some courses in other
  departments and programs have subject matter that is not within the scope of the export
  controls (which focus on controlled items and the resources needed to make them).

- Courses with content within the scope of the EAR (possibly in engineering, chemistry,
  etc.): educational information is not subject to the EAR if it is released by instruction in
catalog courses and associated teaching laboratories of “academic institutions” (both inside
and outside the U.S.; again, note that encryption technology is treated differently.)
Courses with content within the scope of the ITAR (possibly in aero-/astro-physics, nuclear science, etc.): “information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities” is excluded from the definition of ITAR-controlled “technical data” and is not subject to ITAR controls. Courses with unusual content should be evaluated for consistency with this criterion. Note: Even though the course material is excluded from export controls, follow-on discussion or active selection, collection, and transfer of the uncontrolled course material can meet the definition of “defense service” (which IS subject to control).

Courses with content within the scope of the Department of Energy (including some courses in nuclear science and engineering and physics): furnishing public information, including information “in university courses”, generally is authorized, provided that no “sensitive nuclear technology” is transferred. Note: Follow-on-questions and discussion in this area can go beyond the public information and into practical implementation, which may require specific authorization.

**Fundamental Research Exemption (FRE)**

During the Reagan Administration, several universities worked with the Federal Government to establish national policy for controlling the flow of information produced in Federally funded fundamental research at colleges, universities, and laboratories, resulting in the issuance of the National Security Decision Directive 189 (“NSDD”), the National Policy on the Transfer of Scientific, Technical and Engineering Information (September 21, 1985). President George W. Bush’s Administration reaffirmed this directive in 2001.

NSDD 189 provided the following definition of fundamental research that has guided universities in making licensing decisions relative to fundamental research exclusions provided under both the EAR and the ITAR:

- Basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.

Therefore, both the ITAR and the EAR provide that research conducted by scientists, engineers, or students at a university normally will be considered fundamental research and NOT subject to export controls. In order to take advantage of this Fundamental Research Exemption, such information 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).

University-based research is NOT considered fundamental research if the university or its researchers (or the Primary Investigator) – for example, at the request of an industrial sponsor – accept other restrictions on publication of scientific and technical information resulting from the project or activity.
**ITAR provision:** the fundamental research exception does NOT apply to research the results of which are restricted for proprietary reasons, or specific U.S. Government access and dissemination controls.

**EAR provision:** 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.

**Note:** The EAR instructs that prepublication review by a sponsor of university research, solely to ensure that the publication would not inadvertently divulge proprietary information that the sponsor initially has furnished – or compromise patent rights – does NOT constitute restriction on publication for proprietary reasons. Therefore, scientific and technical information resulting from this research will nonetheless qualify as fundamental research once all such restrictions have expired/been removed.

Remember: The Fundamental Research Exemption may exempt the results of your research – but certain components (controlled software or another controlled item/technology) used in the process by which you have achieved fundamental research results likely will remain export-controlled.

**Note:** The EAR does not include a similar license exemption/exception (in other words, this exemption does NOT apply to EAR-controlled items or technology). Accordingly, it is important to consult with NDSU’s ECA before relying on this ITAR license exemption.

**Note:** In the EAR, fundamental research is a separate and distinct category, whereas in the ITAR, it is subsumed under “public domain.”

### SECTION IX:
**NDSU Procedures on Export Controls**

**Core Processes:**
The following procedures outline how the North Dakota State University (hereinafter referenced as “NDSU”) implements core processes of its export compliance program. These procedures are intended to inform NDSU’s faculty, staff, and all affected personnel on how to manage export controlled transactions. Contact information on who to seek for assistance is provided herein. For additional background on how the export regulations affect NDSU’s research activities in general, please see Overview and Frequently Asked Questions and Answers. (See https://www.ndsu.edu/research/integrity_compliance/export_controls/regulations/ and https://www.ndsu.edu/research/integrity_compliance/export_controls/faqs/

**End User Screening Against U.S. Government Watch Lists**
This Section addresses required screening of export recipients and certain collaborative research partners against the U.S. Government’s published denied party/restricted entity watch lists.

The Departments of State, Treasury, and Commerce separately maintain published lists of known export violators. These lists are referred to collectively as the “denied parties lists.” NDSU must not enter into:
Contracts;

Conduct business;

Information exchanges, or

Participate directly or indirectly, in any activities with any entity or person found on these lists.

In order to comply with this requirement, NDSU employs the Visual Compliance software service for denied party screening.

If a match using the software is discovered pertaining to a person or entity appearing on any of the U.S. Government denied parties lists and a name or entity on NDSU transaction, the transaction must be stopped and evaluated in order to avoid export violations.

Note: Rescreening is automatically done daily through Visual Compliance. Entities subject to these screening and rescreening requirements include collaborators on international MOUs; however, we don’t screen international collaborators on proposals unless they come to campus as a VSVR; signatories to MOUs/MOAs, as well as foreign research institutions/organizations, etc.

Technology Control Plans (TCPs)

This Section addresses the implementation of Technology Control Plans (TCP’s) as required to restrict laboratory access of certain items and data from foreign nationals for whom the item is controlled, and would otherwise require an export license to access.

Under certain circumstances such as the safeguarding of ITAR instruments or data that NDSU has not self-invented, or the receipt of proprietary information from a sponsor or collaborator that NDSU uses to pursue its fundamental research, it may be necessary to develop and implement a TCP to specifically safeguard and restrict access to these items.

Before any individual may have access to export-controlled items or technology, he or she must be informed of the conditions of the TCP and agree to comply with the security measures outlined in the TCP. A copy of the TCP must remain with the ECA, and any Government inquiries relating to TCPs (whether as part of a licensing procedure, or an audit) will occur through the office of the ECA.

The TCP is a documented set of procedures that generally includes but is not limited to the following areas:

- NDSU commitment to export control compliance;
- Project overview:description;
- Responsible parties for implementing the TCP;
- Physical controls (laboratory security);
- IT controls (data file/computer access security);
- Deemed export license requirements (as potentially applicable to foreign nationals who NDSU believes should have authorized access but for whom the items are otherwise restricted).
- Protocols for sharing and transferring the items with other authorized parties outside the scope of NDSU’s laboratories, and/or
- Any other requirements concerning:
  - Screening.
  - Personnel authorization.
  - Labeling of items as controlled.
  - Time frame for which the TCP is applicable.

Note: in cases where a U.S. Government agency wishes to review a TCP as part of a licensing procedure or as part of an audit process, the PI and/or administrator in charge of implementing the TCP shall notify the ECA of such a request so that appropriate oversight is in place.

Note: All ITAR-controlled items at NDSU are required to have a TCP.

**Physical Security**

This Section addresses the process for physically securing ITAR and other controlled items where applicable in NDSU’s research laboratories.

Within laboratories containing ITAR and EAR-controlled items (equipment, materials, software, and technical data), NDSU is required to maintain safeguards that prevent unauthorized physical and/or visual access to such items, depending on the applicable deemed export situation.

Depending on the particular control requirement, access restrictions may apply to NDSU personnel as well as to visitors (vendors, research collaborators, etc.). Where foreign national personnel are authorized by license to access controlled items, such personnel and their PIs/managers must be fully aware of the limits of such access as provided for in the license and/or its provisos.

Contact NDSU’s ECA at 701.231.6455 or ndsu.exportcontrols@ndsu.edu for assistance with export control site/physical security procedures.

**EAR Classification**

NDSU EAR classification is the responsibility of the ECAS, therefore, all EAR Classification will be conducted by the ECA.

EAR classification is the exercise of understanding where an item or technology falls on the Commerce Control List (CCL). A classification will determine whether an export license is required based on the destination of the item or technology. Items for purchase “off-the-shelf,” directly from a manufacturer, or by any other commercial means may be controlled under the EAR.
Likewise, imported items – notwithstanding foreign origin – may also be subject to EAR restrictions upon export out of the U.S.

Determination as to whether or not authorization to export is required is determined by the following criteria in the transaction:

- What is the Export Control Classification Number (ECCN) of the item/data?
- Where is it going?
- Who is the end-user?
- What is the end-use?

While the majority of U.S. commercial exports do not require a license, the first step in this process is determining the correct classification of the item. If the item is subject to the EAR, a determination of the Export Control Classification Number (ECCN) found on the Commerce Control List (CCL) must be made.

**Note:** Items subject to the EAR that are not listed on the CCL are designated “EAR99”.

There are three ways to determine the ECCN of the item:

- Go to the source (contact the manufacturer, producer, vendor, or developer of the item).
- Ask the NDSU ECA to classify the technology.
- Request an official classification from the Bureau of Industry and Security (this could take weeks to months).

**Note:** Again, for classification purposes, the EAR – unlike the ITAR – generally looks at the classification of the complete product being exported, rather than at the classification of each subcomponent of the item.

After careful review of the item against the CCL, if it does not fit within the parameters of any ECCN, it may be designated as “EAR99” (assuming it is not controlled by another Government agency). If EAR99, the item may be exported using the license exception “NLR” (No License Required), as long as the following criteria is met:

- The item is NOT being shipped to a sanctioned destination.
- The item is NOT being shipped to a denied person, sanctioned entity, or to any restricted party, or being shipped for a prohibited end-use.
- The item will NOT be used for a specific end-use that is subject to higher controls.

NLR can be used for items with an ECCN if not being shipped to restricted countries (e.g. laptop computer (5A992c) being shipped to France)

**NDSU requires proper export classification of EAR items to determine licensing requirements BEFORE any shipment or release is made, including “deemed exports.”**
Contact NDSU’s ECA at 701.231.6455 or ndsu.exportcontrols@ndsu.edu when classifying an item under the EAR.

Biosafety

Risk management protocols also require that the transfer of biological materials by NDSU to another institution strictly adhere to NDSU’s protocols. In certain cases, such materials may also be export controlled under the EAR and in rare cases under the ITAR. Exporters should work with the the ECA to ensure compliance with export controls. See also export control requirements contained within the IBC Protocol.

Sponsored Research

This Section addresses the export control process:

- When reviewing proposals.
- Contracts.
- Grants and awards.
- To ensure conformity with the Fundamental Research (EAR) and Public Domain (ITAR) Exclusions.

Sponsored Programs Administration (SPA) is responsible for the first assessment based on the bullet points below in determining whether an agreement, award or contract contains or may trigger export control restrictions. ECA will make the final determination if something actually triggers export controls. Some examples are listed below:

- In general, NDSU does not accept restrictions in its awards or contracts that would restrict NDSU faculty members, students and administrators who are not U.S. persons from access to research and research results which would otherwise remain unrestricted under the Fundamental Research Exclusion (FRE). However, exception to this policy may occur, requiring export control analysis. For example, ITAR content or tools associated with fundamental research trigger certain access as restrictions. International collaborative research may also trigger limitations to the FRE.

- In certain cases, a sponsor’s intention with regard to export controls or the control implication of a particular clause or set of clauses may be ambiguous as to NDSU’s export control responsibilities.
  - This may occur with respect to “flow down” restrictions in a subcontract, or vague or open ended publication and/or citizenship limitations.
  - The ECA will be contacted for an assessment of export control implications.

Bona Fide Employee Exemption

Under certain circumstances where NDSU receives or procures an ITAR defense article and/or data, the ITAR makes a limited exception available to bona fide, full time university foreign
national employees to access the item or data without an export license, subject to certain documentary requirements. Assuming these requirements are satisfied, the foreign national employee is subject to the same ITAR restrictions that a U.S. person is with regard to restricting access to the item from all other foreign national individuals (i.e. foreign national students, visitors, post docs who are not employees) as governed by a TCP.

Under a specific exemption, the ITAR allows a university to disclose unclassified technical data in the U.S. to a foreign person who is the university’s bona fide and full-time regular employee. The exemption is available only if the:

- Employee’s permanent abode throughout the period of employment is in the United States.
- Employee is not a national of a country to which exports are ITAR-prohibited, or which is embargoed.
- University informs the individual in writing that the technical data may not be transferred to other foreign persons without the prior written approval of DDTC.
- University complies with certain additional legal requirements set forth in the ITAR.

Note: 22 C.F.R § 125.4(b) (10). The “full-time bona fide employee” requirement typically precludes the following individuals from qualifying for access to technical data under this exemption: temporary and adjunct.

International Collaboration Agreements

This section addresses the process for managing the export control requirements associated with international collaborations with potential international research partners.

Several export control requirements are applicable.

- Faculty must follow NDSU procedures for international MOUs as illustrated on the Provost’s website; https://www.ndsu.edu/provost/faculty_affairsr_administration/forms/international_agreements/. Current procedures dictate that every international MOU request be reviewed by the ECA and a member of the RCA. When drafting or planning to sign a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) with a potential non-US research partner that does not directly fall under the auspices of SPA, it is NDSU’s policy that we follow NDSU procedure and U.S. law.
- Prior to signing such an Agreement, NDSU shall screen such entity and signatories against the U.S. Government’s watch lists to ensure that potential partners are not listed.
- MOUs or MOAs may contemplate the exchange of export controlled items or data that drive the collaborative research. Because the export of such items or their receipt into NDSU’s laboratories potentially has export control implications, these implications must be identified at the earliest opportunity so that the parties can plan accordingly.

In certain cases, where the research is predicated on the receipt of (or access to) an export controlled item that requires prior government approval through a license or authorization, it is important that the parties take this contingency into account either in the MOU/MOA
process or in a subsequent writing.

It is NDSU’s policy not to bind itself to a contractual obligation, without acknowledging the need to fulfill a regulatory condition without which the program cannot proceed as intended.

- Subsequent amendments to the MOU/MOA must proceed according to the same evaluation process, to the extent they subsequently alter the terms of the initial MOU/MOA or where the parties/signatories change over time.

**International Visitors and Activities**

**Authorizations to Visit NDSU**

- It is the responsibility of all colleges, schools, units, departments, centers, faculty, researchers, and administrators at NDSU, intending to invite or host international visitors (including international academic partners/collaborators, visiting scholars/researchers, tour groups, etc.), to notify and request from the ECA the approval of such visit BEFORE the arrival of the international visitor(s).

- For visiting scholars/researchers, NDSU sponsors must complete the “North Dakota State University Visiting Scholar or Visiting Researcher Request Form”, administered by NDSU’s Provost Office, before such collaboration occurs. This request contains several export control compliance questions that must be answered. The Sponsor’s Chair, Dean, and ECA, must approve all Visiting Scholar or Visiting Researcher (VSVR) requests before the visitor arrives to NDSU.

Such visitors include all foreign nationals/foreign persons teaching or conducting research at NDSU who are not employed by NDSU, and are not currently employed by a college or university based in the U.S.

<NDSU uses Visual Compliance™ to expedite screening for these and other issues. Contact NDSU’s ECA at 701.231.6455 or ndsu.exportcontrols@ndsu.edu for assistance with restricted parties’ and other screenings.>

**Responsibility for International Activities**

The ECA is responsible for developing and implementing procedures to screen international programs, centers, and activities for compliance with export control laws and regulations.

In the case of NDSU activities conducted outside the U.S., it is the responsibility of the NDSU activity organizer and/or responsible official to contact the ECA for activities including, but not limited to, the following:

- Execution of agreements to be performed outside the United States.
- Non-credit-bearing study abroad courses.
- Making payments to foreign persons and foreign vendors.

More detailed information on international activities can be found throughout this Manual.
Travel Abroad

This Section addresses the process for ensuring export control compliance when shipping or carrying tangible items associated with conferences, assignment, or conducting research abroad; transfer of technical data by laptop or other electronic means.

NDSU personnel who intend to travel abroad for fieldwork, conferences, etc., must be familiar with whether these activities are subject to export controls under ITAR, EAR, and Office of Foreign Assets Controls (OFAC) regulations, to the extent that the scope of activity involves the transfer of technical data and/or any commodity. This includes possible transfer of proprietary data by laptop, jump drive, or other portable device and to countries sanctioned/embargoed under OFAC.

Note: merely presenting fundamental research results at international conferences or teaching curriculum-based courses abroad do not trigger export control requirements. However, the shipping or hand-carrying of materials in support of these activities may have control requirements.

As to the so-called T4 countries subject to OFAC the analysis must not only take into account the transfer of commodities and technical data, but in the case of Cuba, take into account the travel itself. In some cases, the research activity may trigger a restricted “service” to those countries. For purposes of conducting fundamental research abroad, shipping instruments used in field research or during the course of an inter-institutional collaboration may require obtaining an export license and sufficient lead time should be taken into account in order to receive an export license/authorization as necessary.

As a general rule, an export license is not required to take luggage and a laptop during international travel, provided the traveler is not transporting any EAR- or ITAR-controlled technical data, and provided the traveler is not going to Cuba, Iran, North Korea, Sudan, or Syria. However, if travelers need to take controlled technical data along – or wish to travel with a laptop and/or a smartphone to one of these aforementioned embargoed countries – NDSU’s ECA must be consulted (travel to certain countries subject to OFAC must take into account not only the transfer of commodities and technical data, but also take into account the travel destination itself and, in many cases, the full extent to which the activity provides a restricted “service” to those countries).

Note: Laptops and smartphones can often be lost or stolen, and both U.S. and foreign customs officials may inspect and seize belongings. Accordingly, NDSU personnel should not travel with anything they do not need, including information stored in laptops and other devices (e.g., sensitive technical data and software, including unpublished research technical data).

If equipment, materials, or samples are to be taken or shipped to non-U.S. destinations in advance of international travel, NDSU’s ECA must be consulted prior to travel in order to determine whether a U.S. Government export license is required. Furthermore, depending upon the type of materials and/or samples, other types of import/export permits may be required.

All NDSU faculty, staff, and other personnel traveling outside the country must register their international travel via NDSU’s business form (“Authorization for Out-of-State Travel”), and answer several export control compliance questions, regardless of whether they plan to engage in controlled exports. See also www.ndsu.edu/accounting/travel/.
For more information on NDSU’s cyber security and international travel recommendations, see also [www.ndsu.edu/its/security/traveling_abroad_with_electronic_devices/](http://www.ndsu.edu/its/security/traveling_abroad_with_electronic_devices/).

[https://www.ndsu.edu/research/integrity_compliance/export Controls/international travel/](https://www.ndsu.edu/research/integrity_compliance/export_controls/international_travel/)

Contact NDSU’s ECA at 701.231.6455 or ndsu.exportcontrols@ndsu.edu for travel-related questions.

### Shipping Services

This Section addresses the process for shipping and receiving tangible items:

- Under export license/authorization.
- Transmission of export data to freight forwarders.
- Record keeping.
- U.S. Customs compliance.

### General Shipping and Receiving

As NDSU has no centralized shipping/receiving facilities, each department is responsible to insure that outgoing shipments follow all export control regulations. It is best practice for all departments to be aware of the following:

Prior to shipping:

- Appropriate references to classification;
- Export control classification of item being shipped;
- Value;
- Licensing requirements;
- License conditions;
- Quantity;
- Consignee;
- Schedule B#, and:
- Numerous other data points must be incorporated into all shipping documentation, including Automated Export Statement (AES) filing.

Likewise, when NDSU receives items into inventory, certain regulatory requirements (Customs and export control control) must be anticipated. For example, when an ITAR item is imported, the item will need to be handled consistent with ITAR physical security access restrictions.

Contact NDSU’s ECA at 701.231.6455 or ndsu.exportcontrols@ndsu.edu for export compliance information related to the shipping/receiving.
Record Keeping
NDSU must comply with regulatory requirements regarding export control-related recordkeeping. These records must be organized so as to be available when requested by U.S. governmental authorities. Records include printed and hard copy documents, as well as electronic records (including e-mail, e-mail attachments and other electronic files). All records will be retained for a minimum period of five (5) years from the date of export or from the date of license expiration, as per the requirements of ITAR Section 123.22 and EAR Section 762.6. In some cases, records will require restricted access where, for example, they contain controlled technical data as part of the transaction.

OFAC Restrictions
The Department of Treasury administers the Office of Foreign Assets Control (OFAC) regulations. These regulations outline the parameters of economic embargoes against various countries. When contemplating any activity involving an OFAC country, NDSU must ensure compliance with the applicable OFAC regulations for that country.

OFAC regulations vary on a country-by-country basis, depending on the type of activity involved. For the import/export of certain items and services provided to beneficiaries in Iran, Cuba, Syria and Sudan, particular license rules apply.

BIS controls a number of items for “AT” (Anti-Terrorism) purposes, controls which apply in parallel with the OFAC regulations but are distinct controls. AT-controlled items on the CCL are specifically referenced for certain countries in relation to the Country Chart. Likewise, ITAR independently controls any export to Section 126.1 prohibited countries, which includes but does not directly correspond to the list of OFAC designated countries.

Denied parties screening should always include the Specially Designated Nationals List (SDNL), comprised of individuals/entities which OFAC specifically restricts and associates with a licensing requirement. Hence, Finance should be vigilant about screening direct foreign payees for this purpose.

Note: Collaborative research arrangements, that contemplate the transfer or receipt of tangible materials; the establishment of research facilities at institutions in these countries; field work being conducted in these countries; and the payment of any kind for service performed (even in support of fundamental research activity) can trigger these restrictions and require prior authorization.

Contact NDSU’s ECA at 701.231.6455 or ndsu.exportcontrols@ndsu.edu for OFAC-related concerns and questions.

Issue Reporting and Notification
NDSU must make every effort to identify suspected or actual violations that occur in conjunction with its export activities. All known or suspected export compliance problems must be documented and NDSU’s ECA notified.
Every instance of a suspected violation must be reviewed by the ECA. All export shipments and releases of technical data related to the suspected incident must be placed on hold until otherwise authorized. Timeliness of reporting is a key issue, since export violations are evaluated not only in terms of their content, but also frequency of occurrence, and system-wide implication.

The ECA shall consult with the ND Attorney General’s Office as appropriate and consider Voluntary Disclosure to the relevant agency (agencies) as applicable. Timeliness of reporting is a key issue, since export violations are evaluated not only in terms of their content, but also frequency of occurrence, and system-wide implication.

IMMEDIATELY contact NDSU’s ECA or the Director of Research Integrity and Compliance if you anticipate, suspect, or have knowledge of any NDSU non-compliance (past, present, or future) with U.S. export controls laws and regulations.

Export Control Training and Assessment

Training
In addition to regularly export control training sessions open to faculty, students, and administrators, NDSU makes available ongoing export briefing sessions as needed or upon request. These sessions are designed to answer specific questions pertaining to research and international collaborative endeavors.

Moreover, NDSU personnel can access and download Export Control training PowerPoints located at https://www.ndsu.edu/research/integrity_compliance/export_controls/regulations/ and https://www.ndsu.edu/research/integrity_compliance/export_controls/faqs/ just click on the large green box.

Lastly, NDSU personnel have access to Export Control Training through Citi which can be accessed on the Web at https://www.citiprogram.org/

CITI offers the following export control courses (free) which discuss general and specific information to researchers. These are a great resources for faculty, post docs, and lab personnel, and they can print a certificate for each course that they complete. This is also a great resource for documentation purposes for your department. The following courses are offered:

- Introduction to Export compliance (ID: 16800)
- Export Compliance for Researchers: Part I (ID: 16801)
- Export Compliance for Researchers: Part II (ID: 16802)
- Export Compliance for Research Administrators (ID: 16803)
- Export Compliance and Biosafety (ID: 16805)
- Export Compliance for Operational Departments (ID: 16806)
- Export Compliance for International Shipping (ID: 16807)
- Export Compliance and Purchasing (ID: 16808)
- Export Compliance and Collaboration (ID: 16810)
- Export Compliance and United States Sanctions Programs (ID: 16812)

The U.S. Government’s export control authorities consider awareness training a key element of a compliance program, and it is NDSU’s intention to familiarize faculty and staff as
comprehensively as possible on these requirements. In this regard, training logs should be maintained, reflecting the date of trainings given and attendees.

Please contact the ECA to learn about the next scheduled Export Control training or to arrange customized briefing sessions.

Export Assessment
NDSU’s Export Assessment program is designed to identify and address export compliance gaps and weaknesses. Where a compliance exposure is discovered, corrective action procedures shall be implemented and, depending on the particular circumstances, a Voluntary Disclosure Notification to the appropriate government agency shall be initiated.

SECTION X: Export Controls at NDSU

Under the U.S. export control regulations, any individual or institution who is undertaking any export activity is responsible for properly complying with the regulations. Civil and criminal enforcement liability extends to both individual and institutional activity. Taking that into account, NDSU’s leadership is committed to supporting the institution’s export compliance program.

Export Control Administrator
NDSU’s ECA will serve as a key resource to perform the following functions, as supported by internal and external advisors:

- Determine whether an item being exported (hardware, software, materials, or technical data) requires an export license by virtue of its ITAR jurisdiction, EAR classification, end user status, or potential OFAC restriction.
- Assist campus departments in expanding the existing screening program of end users against the U.S. Government’s published Denied Parties/Restricted Entities Lists.
- Apply for any required export licenses and authorizations where required and advise supervising PIs and license recipients on how to comply with license conditions.
- Advise faculty members on travel-related export control requirements, conducting research abroad, and international collaborations.
- Advise and support export control compliance for those Departments potentially effected by export control requirements, including but not limited to the following functions:
  - Human Resources.
  - Procurement/Purchasing.
  - Information Technology (IT) Services.
  - Campus Security.
  - Safety Office.
  - Sponsored Programs Administration.
  - Technology Transfer Office.
  - Provosts Office.
- Oversee export control recordkeeping processes.
- Conduct campus-wide export control training for faculty, administrators, and others requiring such training.

- Conduct periodic audits of export control processes and activities to proactively manage compliance.

- Serve as the liaison between NDSU and any U.S. Government agency requesting documentation from NDSU, inquiring about an export control related item/activity.

**Export Control Analysis**

Export control analyses will be conducted by the ECA and others under a number of circumstances, primarily when an inquiry is submitted to the ECA. The ECA conducts campus-wide and specific trainings in order to educate NDSU units and departments to identify the following RED FLAGS, which indicate the possible presence of export control issues:

- The project/activity or research proposal/award/agreement/contract:
  - References U.S. export control regulations (ITAR, EAR, OFAC), beyond a mere/general statement to comply.
  - Restricts access or participation based on country of origin (e.g., participants limited to U.S. citizens only).
  - Involves export-controlled information, technology, or equipment (if stated, known, or suspected).
  - Involves military, security, or intelligence applications – or classified, secured, or top secret materials – or dual civilian or military applications.
  - Restricts access or participation based on country of origin (e.g., participants limited to U.S. citizens only).
  - Limits or restricts publication, including granting the sponsor pre-publication review and approval (for matters other than the inclusion of patent or sponsor proprietary/confidential information) or allowing the sponsor to claim the results or data generated in the agreement as proprietary or trade secret or confidential.
  - Involves, in any way, certain countries/foreign nationals, including (but not limited to) Afghanistan, China, Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria, etc.
  - Involves international travel, shipping, or work performed outside of the United States.
  - Includes or involves foreign sponsors or collaborators.
  - Is funded by the Department of Defense, the Department of Energy, the Army, the Air Force, the Naval Office, NASA, the National Reconnaissance Office, or other U.S. Government agencies.

- Or, when the client/customer:
  - Has an address/contact information similar to that found on a restricted parties’ list.
  - Requests or provides payment/invoice descriptions that are vague or nonsensical.
  - Has little/no business background.
  - Lists the freight forwarding firm as the product’s final destination.
  - Their packaging is inconsistent with the stated method of shipment or destination.
Requests an abnormal shipping route for the product and destination.

When questioned, buyer/client/customer is evasive and especially unclear about whether the purchased product is for domestic use, for export, or for re-export.

All implicated individuals and entities are screened against the specially designated and restricted parties’ lists. Export-controlled equipment, data, and/or technology is identified and referred to NDSU’s ECA. Upon completing any final review, the ECA will advise the PI:

- Concerning any export controls that apply to the project/activity.
- Any restrictions on access by foreign persons.
- Any other relevant requirements pursuant to export control laws and regulations.

Contact NDSU’s ECA at 701.231.6455 or ndsu.exportcontrols@ndsu.edu for assistance with ITAR and/or EAR licensing.

Sponsored Programs Administration (SPA)/Office of Research and Creative Activity (RCA)

NDSU’s Sponsored Programs Administration works closely with the Export Control Administrator (ECA) in identifying export control issues and providing support for their solution. SPA in conjunction with the ECA, will:

- Review terms of sponsored program agreements and other awards or contracts, to determine whether an agreement contains or triggers possible export control issues. For example:
  - Sub-Contracts from Foreign Institutions
  - Sub-Contracts to Foreign Institutions
  - Personnel Restrictions
  - Publication and dissemination Restrictions
  - Confidential and Proprietary Restrictions

- Communicate identified potential export control issues to the PIs and the ECA.

- Communicate with the ECA about any changes in awards that necessitate another review of the project for export controls.

In certain situations, a sponsor’s intention with regard to export controls – or the control implication of a particular clause or set of clauses – may be ambiguous as to NDSU’s export control responsibilities (e.g., “flow down” restrictions in a subcontract, or vague or open-ended publication and/or citizenship limitations).

While the ITAR does not contain such descriptive provisions, the EAR is instructive as to interpreting the limitations on fundamental research.
Information Technology
NDSU’s Information Technology (IT) Services supports EAR and ITAR-driven access restrictions. Typically, IT requirements will have to address, among other things, the following areas:

- Laptop security.
- Network security.
- Back-up and storage applications.
- File access approval (including download and print permissions).
- Email protocols.

ITAR and EAR controlled technical data must be secured and access limited to approved personnel only. The Information Security Office has set up ITAR/EAR Research Computing Encryption Procedures for this process. Review the section titled ITAR/EAR Research Computing Encryption for those procedures.

Note: NDSU does not provide encryption software on their computers or laptops. Within Windows 10 and Windows 7 there is a “bit locker” for full disc encryption; however, if you choose to utilize this option for encryption and you lose your password, NDSU staff will not be able to gain access to the encrypted material.

Contact NDSU’s ECA at 701.231.6455 or ndsu.exportcontrols@ndsu.edu for assistance with export control IT procedures.

Key University Managers and Research Administrators
Academic deans, directors, and department heads/chairs (‘‘University Managers’’) all share the responsibility of overseeing export control compliance in their respective schools, departments, centers, or institutes, as well as supporting the ECA in implementing procedures (as deemed necessary by the ECA) for export control compliance.

In addition, University and department research administrators work closely with RCA and the PIs. Together with RCA, they will:

- Provide assistance to PIs in reviewing terms of sponsored program agreements, material transfer agreements, and other non-monetary agreements to identify restrictions on publication and dissemination of research results, and flag such restrictions in agency requests for proposals.
- Provide assistance to PIs in identifying international components of sponsored program agreements, and identifying potential export control issues in the proposed international components.
- Communicate identified potential export control issues to the PIs and the ECA.
- Communicate with the ECA and RCA about any changes in awards that necessitate another review of the project for export controls.
Business Administrators

The University and department business administrators assist in ensuring compliance with export control regulations by identifying potential export issues within various unit activities. Such issues may include reviewing invoices for statements that items may not be exported and ensuring that international shipping is compliant with export control laws.

Principal Investigators (PIs)

PIs have expert knowledge about the types of information and technology involved in their research projects or other NDSU activities, such as presenting at conferences or discussing research findings with fellow researchers or collaborators. PIs must ensure that they do not disclose export controlled information or transfer controlled articles or services to a foreign national without prior authorization (as required). PI’s must:

- Understand export control obligations.
- Assist the ECA in correctly classifying technology and items that are subject to export control laws.
- Assist in identifying foreign nationals who may be involved in export controlled projects/activities. If export controls are implicated, notify the ECA to initiate the process of clearing foreign national participation well in advance of the project/activity in order to ensure that a license is obtained in a timely manner (or implement proper measures to isolate foreign nationals from participation).
- Develop and maintain the conditions of a TCP (with the assistance of the ECA for any activity, data, or equipment, where the need for such a plan is identified).
- Ensure that research staff and students have been trained on the TCP and on the export control regulations, should any apply.

Faculty, Staff, and Other Applicable NDSU Personnel

It is NDSU policy that all personnel – including employees, visiting researchers/scholars, post-doctoral fellows, students, and other persons retained by, or working at or for, NDSU – conduct their affairs in accordance with U.S. laws and regulations. This includes compliance with U.S. export control laws and regulations applicable to NDSU’s operations.

The laws and regulations governing exports are lengthy, detailed, and complex. Employees with responsibility for NDSU’s export control compliance program, or whose duties include a significant amount of work with foreign nationals, will be offered formal training sessions on the U.S. export-control laws and regulations and their applicability to their jobs (see “Training,” below). All NDSU employees with managerial or supervisory authority over foreign nationals, or projects involving materials or technology subject to export controls, must view export control compliance as an important part of their day-to-day responsibilities.
**Procurement**

It is important that in those instances where NDSU purchases an export controlled item or material for research purposes, the item be identified as such, and the controlled status communicated to the user on campus, for example the lab director or program administrator. This is particularly true where ITAR items are concerned, as foreign national access shall be restricted in addition to normal outbound export controls.

Once the vendor or supplier has identified a control status, this information shall be transmitted to the laboratory user or administrator, and noted for further disposition. Procurement shall likewise maintain a database of all such items so that access restrictions (ITAR) and outbound export of these items (ITAR or EAR) are appropriately flagged for potential licensing.

Where ITAR items are concerned, NDSU shall also screen those vendors from whom it is procuring the item against the U.S. Government watch-lists to ensure compliance with screening guidelines.

**New Employees at NDSU**

All new employees at NDSU agree to comply with the NDSU Policy Manual, which includes compliance with all U.S. export control laws and regulations.

Additionally, as requested, the ECA will meet with certain newly hired international employees in the scientific and related research fields for personalized export controls training and tailored Q&A sessions – and, specifically, to brief these personnel on the concepts of deemed exports and deemed re-exports. New international employees who have undergone training with the ECA will attest to attendance at same.

**Provost/International Offices**

**I-129 Certification**

As part of its I-129 H1 Visa Application process, the U.S. Immigration and Citizenship Service (USCIS) requires a certification as to whether the Beneficiary will require an export license to access export controlled technology or technical data during the course of his/her professional position.

If a license is required, the Certification also requires the Petitioner to state that it will prevent access or disclosure through a control plan until a license is approved by the Department of Commerce or State. Note that in certain cases, the U.S. Government might not issue a license for particular sensitive control reasons.

**Note:** For example, under ITAR Part 126.1, China is a proscribed country for which DDTC will not issue an ITAR license; this prohibition and presumption of license denial extends to Chinese foreign nationals for whom ITAR items remain absolutely restricted.

As a result, in advance of the H1 Visa petition being submitted to USCIS, it is critical to evaluate:

- Whether access will require an export license.
The likelihood of obtaining a license.

The need for an interim or permanent Technology Control Plan.

NDSU must assess precisely what controlled technology or technical data it has or plans to have which could be accessed by an H1 employee. Toward this objective, the pertinent faculty members and administrators shall complete NDSU’s Form I-129 Export Control Certification Questionnaire and return the form to the Provost/International Office during the recruitment process.

The ECA does conduct restricted parties’ screenings for departments which have completed VSVR or Export Control Certification Questionnaire Forms for visitors in order to evaluate any export control concerns (including external funding sources) prior to their participation in academic or research programs at NDSU.

No international visitor may have access (whether verbal, written, electronic, and/or visual) to export-controlled information or physical items on NDSU’s campus until the access has been reviewed by the ECA for export control concerns and, if required, an export control license or other appropriate authorization has been obtained.

☑️ It is the responsibility of the faculty, researcher, or administrator hosting the visitor(s) to ensure compliance with export control restrictions and to promptly disclose and report to the ECA.

**Restricted Parties’ Screenings**

☑️ Faculty, researchers, and administrators inviting and hosting international visitors should provide the relevant information to the ECA prior to their visit. The information should be sufficient enough for the ECA to conduct restricted parties’ screenings on the visitors. The ECA then will report the results to the requestor.

**Note:** Screenings of international visitors include the screening of the foreign entity or institution where the international visitors are employed – and, where applicable, the names and details of any financial institutions (or other external funding sources) involved.

If the restricted parties’ screenings results are of concern and/or impose restrictions, the ECA will notify the hosting department and attempt to resolve the concerns and/or restrictions, where possible. If resolution is not possible, the ECA will deny the visit and notify the hosting department/individual. If restricted parties’ screenings results do not raise concerns, the ECA will approve the visit, unless further inquiries are warranted based on the disclosures made by the hosting department/individual. If further inquiries are warranted, the ECA will contact the hosting department/individual and handle the situation accordingly.

☑️ It is the responsibility of all employees at NDSU to comply with the initial terms and intent of the visit as communicated to the international visitor(s), and to immediately notify the ECA of any changes in the intent of the visit prior to engaging the international visitor(s) in any activities that may require restricted parties’ screenings.
Distance and Continuing Education

NDSU faculty, staff, and others responsible for offering distance and continuing education instruction, including online education, will screen courses – as appropriate, and in conjunction with the ECA – in order to comply with export control laws and regulations and this Manual.

Similarly, international students who are enrolling and/or participating in distance and continuing education courses from outside the U.S. – or through one of NDSU’s colleges, schools, units, departments, or centers – will be subject to restricted parties’ screenings.

High Performance and Advanced Computer (HPC) Facilities/CCAST

The operation of NDSU’s high performance and advanced computing facilities, housed within the Center for Computationally Assisted Science and Technology (CCAST), at times may involve the use of export-controlled items, data, and/or technology. Overall, export control issues related to HPC operations will be identified, assessed, and managed by NDSU’s Director of CCAST, in coordination with the ECA.

As a condition of use, all CCAST account users (both new and renewing users) must attest that they have read, understand, and agree to comply with CCAST policies regarding the use of the HPC facilities as related to export-controlled items and information. Adherence to, compliance with, and liability related to, CCAST policies and export control laws is the responsibility of each account user. See www.ccast.ndsu.edu/users/policies.

In general, CCAST policies prohibit users from placing any export-controlled items, data, technology, or software (etc.) on the HPC facilities. However, in the rare event that users must utilize the HPCs for any export-controlled items or information inherent to their research or projects, they must request, in writing, an exception to CCAST’s controlled technology prohibition from CCAST’s Director. All requests will be handled on a case-by-case review basis by the Director, in coordination with the account user and the ECA, and will not be granted pro forma.

If the CCAST Director approves any request, and export-controlled items or information will be placed on the HPCs, the Director will work with the account user and the ECA to develop and implement a TCP in order to prevent unauthorized access of controlled information or items to foreign persons/foreign nationals.

Web-Based Services and Licensed Software Agreements, Etc.

This section is currently being revised by Information Technology Services and will be updated when the information becomes available.

Technology Commercialization and Transfer

Because the transfer of technology and/or materials pursuant to a Material Transfer Agreement (MTA) may trigger export control requirements, NDSU’s Technology Transfer Office shall work directly with the research compliance staff to proactively identify and resolve export control requirements associated with an MTA.
Such requirements may be triggered when the activity contemplates an international transfer or is domestic within the U.S., but NDSU has knowledge that the item will be re-exported by the receiving party. As applicable to the transaction at hand, the Material Transfer Agreement shall take into account necessary export control provisions that include but are not limited to notification of export control status (ITAR or EAR) as well as general end use/user restrictions and applicable destination control statements.

**Note:** incoming NDAs (where NDSU is requested to sign another party’s confidentiality agreement covering the receipt of proprietary items or data) must likewise be reviewed for export control purposes. NDAs should be handled separately from both MTAs and MOUs.

As the potential modification of another party’s Confidentiality Agreement can take additional time, the Technology Transfer Office shall be alerted as soon as possible to a pending Agreement so as to allow sufficient opportunity for timely evaluation.

**University Foundations**

Although created to benefit and support NDSU as a whole, University Foundations are separate legal entities and generally are not subject to NDSU policies and procedures, including this Manual.

As separate legal entities, generally the Foundations are responsible for performing their own restricted parties’ screenings; making their own export licensing decisions; and obtaining any necessary export authorizations prior to exporting NDSU-developed items, technical data, or technology to foreign persons/foreign nationals.

**Incubator and Spin-off Activity**

The use of NDSU’s laboratories and resources for any activity other than fundamental research could trigger export control requirements that NDSU would not otherwise be aware of or accept as part of its compliance risk. It is important that the directors and administrators of incubators or spin-off businesses and entities (who may in parallel hold teaching and research positions at NDSU) be aware that, per NDSU’s policy, all such proprietary activities must be performed separately from NDSU’s own and dedicated research laboratory space. This also includes proprietary consulting arrangements that faculty members may have.

**Disciplinary Actions and Non-Retaliation**

NDSU takes the issue of non-compliance with export controls very seriously. In this manner, in addition to the substantial criminal and civil penalties that may be imposed by a Government agency for violation of the export regulations, employees are subject to NDSU policies concerning non-compliance with federal and state laws.

Further, no individual shall be punished or retaliated against by NDSU solely because he or she reported what was reasonably believed to be an act of export control noncompliance, wrongdoing, or violation. However, reporters will be subject to NDSU disciplinary action if they knowingly fabricated, distorted, or exaggerated any report submitted or notification given.
**SECTION XI: APPENDIXES**

Appendix 1 — Glossary

*Glossary of Export Controls Terms & Abbreviations*

<table>
<thead>
<tr>
<th>TERM/ABBREVIATION</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bureau of Industry and Security (BIS)</td>
<td>Bureau of Industry and Security (BIS) – An agency of the Department of Commerce (DOC) responsible for implementing and enforcing the Export Administration Regulations (EAR), which regulate the export and re-export of most commercial items.</td>
</tr>
<tr>
<td>Commerce Control List (CCL)</td>
<td>Commerce Control List (CCL) – The CCL is a list of items under the export control jurisdiction of the Bureau of Industry and Security, U.S. Department of Commerce. It is found in Supplement 1 to part 774 of the Export Administration Regulations (EAR).</td>
</tr>
<tr>
<td>CCL Category</td>
<td>The CCL is divided into 10 categories: (0) Nuclear Materials, Facilities and Equipment, and Miscellaneous; (1) Materials, Chemicals, “Microorganisms,” and Toxins; (2) Materials Processing; (3) Electronics; (4) Computers; (5) Telecommunications and Information Security; (6) Lasers and Sensors; (7) Navigation and Avionics; (8) Marine; and (9) Propulsion Systems, Space Vehicles, and Related Equipment.</td>
</tr>
<tr>
<td>CCL Group</td>
<td>The CCL is divided into 10 categories. Each category is subdivided into five groups, designated by the letters A through E: (A) Equipment, Assemblies, and Components; (B) Test, Inspection and Production Equipment; (C) Materials; (D) Software; and (E) Technology.</td>
</tr>
<tr>
<td>Consolidated Screening List</td>
<td>The Consolidated Screening List is a downloadable file that consolidates export screening lists of the Departments of Commerce, State, and the Treasury into one spreadsheet to assist in screening potential parties to regulated transactions. If the potential match is from the consolidated list, the detailed instructions on the Consolidated List homepage must be used to determine what list the potential match is from and under what government agency’s jurisdiction. See <a href="http://export.gov/ecr/eg_main_023148.asp">http://export.gov/ecr/eg_main_023148.asp</a>.</td>
</tr>
<tr>
<td>Controlled Country</td>
<td>A list of countries designated controlled for national security purposes found in Country Group D:1, including: Albania, Armenia, Azerbaijan, Belarus, Bulgaria, Cambodia, the People’s Republic of China, Estonia, Georgia, Kazakhstan, Kyrgyzstan, Laos, Latvia, Lithuania, Moldova, Mongolia, Romania, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, and Vietnam. Cuba and North Korea are controlled countries, but they are listed in Country Group E:2 (unilateral embargoes) rather than Country Group D:1.</td>
</tr>
<tr>
<td><strong>Countries supporting international terrorism</strong></td>
<td>In accordance with § 6(j) of the Export Administration Act of 1979, as amended (EAA), the Secretary of State has determined that the following countries' governments have repeatedly provided support for acts of international terrorism: Cuba, Iran, North Korea, Sudan, and Syria.</td>
</tr>
<tr>
<td><strong>Directorate of Defense Trade Controls (DDTC)</strong></td>
<td>Directorate of Defense Trade Controls (DDTC) – the office in the Department of State (DOS) that administers licenses for defense services and defense (munitions) articles. (Formerly known as the Office of Defense Trade Controls).</td>
</tr>
<tr>
<td><strong>Dual-use</strong></td>
<td>Items that have both commercial and military/proliferation applications. While this term is used informally to describe items that are subject to the EAR, purely commercial items are also subject to the EAR (see §734.2(a) of the EAR).</td>
</tr>
<tr>
<td><strong>Deemed Export</strong></td>
<td>The release of technology or source code subject to the EAR to a foreign national in the United States is “deemed” to be an export to the home country of the foreign national under the EAR. Technology is specific information necessary for the development, production, or use of a Commerce Department product controlled for export. “Use” is defined as operation, installation (including on-site installation), maintenance (checking), repair, overhaul, and refurbishing. Deemed exports can occur through a discussion, email, or phone call with a foreign national researcher or student within NDSU’s campus.</td>
</tr>
<tr>
<td><strong>Deemed re-export</strong></td>
<td>The EAR defines “deemed” re-exports as the release of technology by a foreign national, who has been licensed to receive it, to the national of another foreign country, who has not been licensed to receive the technology. (For example, ECCN 5E001 technology may be exported to a university in Ireland under the license exception for technology and software, but might require a deemed re-export license authorization before being released to a Russian foreign national student or employee of that university in Ireland.) See also definitions for “Deemed export” and “Re-export.”</td>
</tr>
<tr>
<td><strong>Defense article</strong></td>
<td>(ITAR § 120.6) means any item designated in the USML. Examples include specified chemical agents, cameras designated for military purposes, specified lasers, and GPS equipment as noted above. It also means any technical data recorded or stored in any physical form, models, mock-ups, or other items that reveal technical data directly relating to the particular item or “defense article” listed in the USML.</td>
</tr>
<tr>
<td><strong>Defense service</strong></td>
<td>(ITAR § 120. 9) means the furnishing of assistance (including training) anywhere (inside the United States or abroad) to foreign nationals in connection with the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing, or use of defense articles, and the furnishing of any controlled “technical data” (see definition below) to foreign nationals anywhere.</td>
</tr>
<tr>
<td><strong>Denied Persons List (DPL)</strong></td>
<td>A list, referenced in Supplement No. 2 to part 764 of the EAR, of specific persons that have been denied export privileges, in whole or in part. The full text of each order denying export privileges is published in the Federal Register.</td>
</tr>
<tr>
<td><strong>EAR</strong></td>
<td>The Export Administration Regulations (EAR), Title 15, Sections 730–774 of the Code of Federal Regulations (CFR), refers to the regulations promulgated and implemented by the Department of Commerce that regulate the export of goods and related technology identified on the Commerce Control List (CCL). Goods and technology on the CCL are not inherently military in nature; they are primarily and inherently commercial or potentially commercial in nature.</td>
</tr>
<tr>
<td><strong>ECCN</strong></td>
<td>Export Control Classification Number (ECCN) – An alpha-numeric code (e.g., 3A001) used by the Department of Commerce to classify most commercial items. An ECCN describes a particular item or type of item, and shows the controls placed on that item. All ECCNs are listed in the Commerce Control List (CCL) (Supplement No. 1 to Part 774 of the EAR).</td>
</tr>
</tbody>
</table>
| **Educational Information Exclusion** | EAR: Release of information by instruction in catalog courses and associated teaching laboratories of academic institutions is not subject to the EAR.  
ITAR: Information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities is not controlled by the ITAR. |
| **Effective control** | According to the EAR, maintaining effective control over an item occurs when you either retain physical possession of the item, or secure the item in such an environment as a hotel safe, a bonded warehouse, or a locked or guarded exhibition facility. Retention of effective control over an item is a condition of certain temporary exports and re-exports. |
| **End-use** | A detailed description of how the ultimate consignee intends to use the commodities being exported. |
| **End-user** | The person abroad that receives and ultimately uses the exported or re-exported items. The end-user is not a forwarding agent or intermediary, but may be the purchaser or ultimate consignee. |
| **Embargo** | An embargo is the prohibition of commerce and trade with a certain country, in order to isolate it and to put its Government into a difficult internal situation, given that the effects of the embargo are often able to make its economy suffer from the initiative. |
| **Export** | An actual shipment or transmission of items, services, or technical data subject to either the EAR or the ITAR out of the United States, or the “release” of technology, software (including source code), or technical data subject to either the EAR or the ITAR to a foreign national in (or outside of) the United States. (A release of technology or source code to a foreign national in the U.S. is considered a “deemed export.”) Technology, software, or technical data is “released” for export through:  
Visual inspection by a foreign national of U.S.-origin equipment and facilities  
Oral exchanges of information in the United States or abroad  
Transfer or shipment via any means (physical or electronic) to a foreign entity |
<table>
<thead>
<tr>
<th><strong>Provision of a service, or the application to situations abroad of personal knowledge or technical experience acquired in the United States</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Export controls</strong></td>
</tr>
<tr>
<td>Federal sets of laws, policies, and regulations that restrict the release of certain items, information, and software to foreign nationals in the United States and abroad. Primarily, those regulations are the Export Administration Regulations (EAR) and the International Traffic in Arms Regulations (ITAR), as well as regulations administered by the Office of Foreign Assets Control (OFAC).</td>
</tr>
<tr>
<td><strong>Export license</strong></td>
</tr>
<tr>
<td>The approval documentation issued by an export agency authority authorizing the recipient to proceed with the export, re-export, or other regulated activity as specified on the application.</td>
</tr>
<tr>
<td><strong>Foreign National/Foreign Person</strong></td>
</tr>
<tr>
<td>Anyone who is not a “U.S. person” (see definition below). A “U.S. person” is any one of the following:</td>
</tr>
<tr>
<td>U.S. citizen</td>
</tr>
<tr>
<td>lawful permanent resident alien (LPR, or green card holder)</td>
</tr>
<tr>
<td>refugee</td>
</tr>
<tr>
<td>protected political asylum or someone granted temporary residency under the amnesty provision</td>
</tr>
<tr>
<td>NOTE: Any foreign entity not incorporated or organized to do business in the United States falls within the definition of a foreign national. This includes any branch of a foreign government and also can include universities and research laboratories in other countries.</td>
</tr>
<tr>
<td><strong>Foreign Entity</strong></td>
</tr>
<tr>
<td>Business or other entity not incorporated in the U.S., and foreign Governments. See also “Foreign National/Foreign Person.”</td>
</tr>
<tr>
<td><strong>Fundamental Research</strong></td>
</tr>
<tr>
<td>(EAR and ITAR) means 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. The products of fundamental research are not subject to export license requirements or other Government approval. Fundamental research is distinguished from research that results in information that is restricted for proprietary reasons or national security reasons (EAR), or pursuant to specific U.S. Government access and dissemination controls (ITAR).</td>
</tr>
<tr>
<td><strong>Fundamental Research Exclusions (FRE)</strong></td>
</tr>
<tr>
<td>Under the EAR: The citation for the official definition of fundamental research under the EAR is 15 CFR § 734.8. The EAR provides that university research normally will be considered as fundamental research unless the university or its researchers accept sponsor restrictions on publication of scientific and technical information resulting from the project or activity. The EAR specifically permits limited prepublication reviews by research sponsors to prevent inadvertent divulging of proprietary information provided to the researcher by the sponsor or to insure that publication will not compromise patent rights of the sponsor.</td>
</tr>
<tr>
<td>Under the ITAR: The ITAR citation is 22 CFR § 120.11(8). The ITAR states that university research will not be deemed to qualify as fundamental research if: (1) the university or its researchers accept any</td>
</tr>
<tr>
<td><strong>International Traffic in Arms Regulations (ITAR)</strong></td>
</tr>
<tr>
<td><strong>License</strong></td>
</tr>
<tr>
<td><strong>License Exception</strong></td>
</tr>
<tr>
<td><strong>Office of Foreign Asset Control (OFAC)</strong></td>
</tr>
<tr>
<td><strong>Publicly Available</strong></td>
</tr>
<tr>
<td><strong>Public Domain</strong></td>
</tr>
<tr>
<td><strong>Re-export</strong></td>
</tr>
<tr>
<td><strong>Reasons for control</strong></td>
</tr>
<tr>
<td><strong>Restricted research</strong></td>
</tr>
<tr>
<td><strong>Sanctions</strong></td>
</tr>
<tr>
<td><strong>Sanctioned countries</strong></td>
</tr>
<tr>
<td><strong>Select agent</strong></td>
</tr>
<tr>
<td><strong>Specially Designated Nationals (SDN) and Blocked Persons List</strong></td>
</tr>
<tr>
<td><strong>Technical assistance</strong></td>
</tr>
</tbody>
</table>
| **Technical data** | (22 CFR § 120.10) Refers to information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of controlled articles. This includes information in the form of blueprints, drawings, plans, instructions, diagrams, photographs, etc. It may take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, and manuals and instructions written or recorded on other }
媒体或设备（如磁盘、磁带或只读内存）。ITAR定义不包括与普通科学、数学或工程原理相关的信息，这些知识通常在小学、学院和大学中教授，或在公共领域。**Technology**

任何具体信息和专有技术（无论是以有形形式，如模型、原型、图纸、草图、蓝图、手册或软件，还是以无形形式，如培训或技术性服务）所需的开发、生产或使用，但不包括该商品本身。

**Technology Control Plan (TCP)**

技术控制计划（TCP）是NDU项目人员将用于确保任何主题物品和信息不被未经授权的人士披露，或者不受必要的美国政府授权的情况下出口。NDU的ECA已经创建了一个模板TCP作为起点，首先和主要是为了遵守特定的监管要求，其次是为了适应相关的NDU项目或计划的需求和结构。

**Transfer**

向任何个人转移受EAR管辖的项目，无论是在美国境内还是在美国境外，如有意图或知识，它们将被运输、转移或传输给未经授权的接收者。

**United States Munitions List (USML)**

美国军火库名单（USML）—（22 CFR § 121.1）USML包括被指定为军火或军火服务的项目，这些项目根据《武器出口控制法》（AECA）指定。

**U.S. Person**

任何美国公民，或有合法永久居民身份（LPR）的外国公民。LPR也被称为永久居民（PRA）。

**Visual Compliance™**

Visual Compliance™是一款基于网络的出口合规工具，将多个监管要求整合到一个自动化的系统中，以避免手动筛选个人和实体，以避免被包含在受制裁的实体名单中。该系统被NDU用于快速筛查授权方、特别指定的国家，以及未来的筛选；搜索当前联邦出口控制法规和制裁；确定ECCN和USML类别；确定豁免、例外、排除或许可要求；筛选和追踪校园中出口管制的硬件；并确定其他OFAC合规领域。
## Web Resources

### Website References

<table>
<thead>
<tr>
<th>This Export Controls Compliance Manual</th>
<th><a href="http://www.ndsu.edu/research/integrity_compliance/export_controls/policy_procedures/ndsu_export_controls_compliance_manual/">www.ndsu.edu/research/integrity_compliance/export_controls/policy_procedures/ndsu_export_controls_compliance_manual/</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Vice President for Research and Creative Activity</td>
<td><a href="http://www.ndsu.edu/research">www.ndsu.edu/research</a></td>
</tr>
<tr>
<td>Export Controls at NDSU</td>
<td><a href="http://www.ndsu.edu/research/integrity_compliance/export_controls/">www.ndsu.edu/research/integrity_compliance/export_controls/</a></td>
</tr>
</tbody>
</table>

### U.S. Agencies Regulating Export Controls

| --- | --- |

### Export Control Regulations

<table>
<thead>
<tr>
<th>The International Traffic in Arms Regulations (ITAR)</th>
<th><a href="https://www.pmddtc.state.gov/regulations_laws/itar.html">https://www.pmddtc.state.gov/regulations_laws/itar.html</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>The Export Administration Regulations (EAR)</td>
<td><a href="http://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear">http://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear</a></td>
</tr>
<tr>
<td>The Office of Foreign Assets Control (OFAC)</td>
<td><a href="http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx">http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx</a></td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>DDTC Debarred Parties List</strong></td>
<td><a href="http://pmddtc.state.gov/compliance/debar.html">http://pmddtc.state.gov/compliance/debar.html</a></td>
</tr>
<tr>
<td><strong>OFAC Specially Designated Nationals List (SDN)</strong></td>
<td><a href="http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx">http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx</a></td>
</tr>
<tr>
<td><strong>Consolidated Screening List</strong></td>
<td><a href="http://export.gov/ecr/eg_main_023148.asp">http://export.gov/ecr/eg_main_023148.asp</a></td>
</tr>
</tbody>
</table>

**Other Agencies Involved in Export Controls**

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bureau of Alcohol, Tobacco, and Firearms (ATF)</strong></td>
<td><a href="https://www.atf.gov/">https://www.atf.gov/</a></td>
</tr>
</tbody>
</table>
### Department of Homeland Security – U.S. Immigration and Customs Enforcement (ICE)

<table>
<thead>
<tr>
<th>Project Shield America</th>
<th><a href="http://www.ice.gov/project-shield">www.ice.gov/project-shield</a></th>
</tr>
</thead>
</table>

### Federal Bureau of Investigation

| “Counterintelligence Threat to Academic and Scientific Travelers” | http://www.rpi.edu/counsel/security_brief.pdf |

### Other Resources

| Export.gov – brings together resources from across the U.S. Government to assist American businesses in planning their international sales strategies and | http://export.gov/index.asp |
succeed in today’s global marketplace.

<table>
<thead>
<tr>
<th>International Export Controls/Regimes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Missile Technology Control Regime (MCTR)</td>
<td><a href="http://www.mtcr.info/">http://www.mtcr.info/</a></td>
</tr>
</tbody>
</table>
**Appendix 3: Forms**

See “Forms and Handouts from NDSU’s Export Control Office,” available at www.ndsu.edu/research/integritycompliance/exportcontrols/formshandouts/.

**Note:** The 2017 NDSU Audit Self-Assessment is not posted on the web-site.

<table>
<thead>
<tr>
<th>Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>NDSU Technology Control Form</td>
</tr>
<tr>
<td>NDSU Technology Control Plan Departure Form</td>
</tr>
<tr>
<td>NDSU Technology Control Plan Close Out Form</td>
</tr>
<tr>
<td>NDSU Briefing Certification for Additional Project Personnel (TCP’s)</td>
</tr>
<tr>
<td>NDSU International Travel Briefing</td>
</tr>
<tr>
<td>NDSU Certification on the Handling of Export-Controlled Items/Information (Non TCP)</td>
</tr>
<tr>
<td>NDSU Full-Time Bona Fide Employee Certification and Written Notification</td>
</tr>
<tr>
<td>NDSU Export License Exception (TMP)</td>
</tr>
<tr>
<td>NDSU Export License Exception (BAG)</td>
</tr>
<tr>
<td>NDSU Export Control Sample Language (Articles) Agreement</td>
</tr>
<tr>
<td>NDSU Export Control International Shipment Review Form/ Material Transfer Checklist</td>
</tr>
<tr>
<td>NDSU Export Control Brochure</td>
</tr>
<tr>
<td>NDSU Export Control Training PowerPoint (Listed on Export Control Web Site)</td>
</tr>
<tr>
<td>NDSU Export Control Training PowerPoint FAQ’s (Listed on Export Control Web Site)</td>
</tr>
<tr>
<td>NDSU Deemed Exports Presentation (Listed on Export Control Web Site)</td>
</tr>
<tr>
<td>NDSU Export Control Controlled/Not Controlled Project Charts</td>
</tr>
<tr>
<td>NDSU ITAR Label Example</td>
</tr>
<tr>
<td>NDSU ITAR Marking Cabinets/Lockers/Rooms Example</td>
</tr>
<tr>
<td>NDSU ITAR Marking Shipping Label Example</td>
</tr>
</tbody>
</table>
Technology Control Plan (TCP)

NDSU’S COMMITMENT TO EXPORT CONTROL COMPLIANCE

North Dakota State University is committed to acting in accordance with all applicable U.S. Government export regulations. NDSU requires ALL faculty, staff, students, and other University personnel to be aware of, and comply with U.S. export control laws and regulations, as articulated in NDSU’s Export Control Policy (722-Export Control) and procedures thereto. For more information, visit the Export Control web page http://www.ndsu.edu/research/integrity_compliance/export_controls/.

WHAT IS A TECHNOLOGY CONTROL PLAN?

A technology control plan (TCP) is used in order to secure Export Controlled information, equipment, materials, software, data, or technology from access by unlicensed and/or unauthorized foreign citizens. Before an individual has access to any Export Controlled equipment, they must know and agree to comply with security measures specified in the TCP. A signed TCP must be maintained by the Export Control Office for a period of five years.

In general, “export-controlled” means that activities, items, information, technology, and software related to the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, operation, modification, demilitarization, processing, or use of a controlled item requires an export license, or license exception, to physically export from the U.S. OR to discuss with or disclose to a person who is not a U.S. citizen or U.S. lawful permanent resident.

It is unlawful to send or take export-controlled information, technology, software, or items out of the U.S.; or disclose, orally or visually (including by email, fax, phone, etc.), or transfer to a foreign person inside or outside the U.S. without prior authorization from the cognizant U.S. Government agency. The U.S. Government can administratively and criminally punish individuals and NDSU for violating Export Control laws and regulations. Penalties could include imprisonment for up to 20 years, $1,000,000 fine per instance, and loss of import/export privileges.

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

Copies of the final TCP will be held by the Export Control Administrator and the PI of the project. Federal regulations require that the TCPs be kept for a minimum of 5 years after the end date of the plan.

Date: Click or tap here to enter text.

Individual Requesting TCP: Click or tap here to enter text.

Individual Responsible For TCP: Click or tap here to enter text.

Telephone Number: Click or tap here to enter text.

Email Address: Click or tap here to enter text.

PI Initials/Date: ____________________  Export Control Initials/Date: ____________________
## GENERAL PROJECT INFORMATION

<table>
<thead>
<tr>
<th></th>
<th>Click or tap here to enter text.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start Date of Plan:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>End Date of Plan:</strong></td>
<td></td>
</tr>
</tbody>
</table>

### Research Project Description (Brief Overview)

<table>
<thead>
<tr>
<th>Building and Office Where Export Controlled Information is Located (Building, Room)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click or tap here to enter text.</td>
</tr>
</tbody>
</table>

### Is Sponsored Research Involved?

| ☐ Yes | ☐ No |

- If Sponsored Research is Involved, Please Identify Sponsors (include FAR00XXXXX)

| Click or tap here to enter text. |

### EAR/ITAR Category if known - Please contact Export Control if you need assistance with classification.

| Click or tap here to enter text. |

### Will the project use Export Controlled Equipment?

- ☐ Yes
- ☐ No

- If yes, list Manufacturer and Model of Equipment

| Click or tap here to enter text. |

### Will the project use Export Controlled Technology (software)?

- ☐ Yes
- ☐ No

- If yes, list Name and Version of Computer Program(s)

| Click or tap here to enter text. |

### Will the project use or generate Export Controlled data?

- ☐ Yes
- ☐ No

- If yes, list the source of data and expected volume (MB, GB, TB)

| Click or tap here to enter text. |
PROJECT PERSONNEL

Clearly identify every person (including their country of citizenship) who may have authorized access to the controlled technology/item/data. Attach additional sheets if necessary.

<table>
<thead>
<tr>
<th>Name</th>
<th>Citizenship</th>
<th>US Permanent Resident?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>□ Yes □ No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>□ Yes □ No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>□ Yes □ No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>□ Yes □ No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>□ Yes □ No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>□ Yes □ No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>□ Yes □ No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>□ Yes □ No</td>
</tr>
</tbody>
</table>

Physical Security Measures

Please check which physical security measures you will have in place to prevent unauthorized access to secured areas, as well as protect materials and computers.

“One Lock” is the principal of securing items and information by using at least one mechanism to prevent access by unauthorized persons. This is the minimum requirement for safeguarding the Export Controlled equipment, technology or information listed above.

Project personnel are responsible for safeguarding Export Controlled equipment, technology or information at all times by meeting the “one lock” measures identified below in the PHYSICAL SECURITY MEASURES and INFORMATION SECURITY MEASURES below.

<table>
<thead>
<tr>
<th></th>
<th>YES</th>
<th>NO</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Will you have a Plan in Place to Protect Equipment?</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>2. Will the project ONLY be conducted in secure area?</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>3. Will Controlled Materials be Locked in Cabinet?</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>4. Will Controlled Materials will be in a Locked Office</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>5. Will ALL Controlled Equipment will be Clearly Marked?</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>6. Will a Procedure be in Place to Ensure ONLY Project Members will have access to Secured Area?</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>7. Will there be a Chain of Custody Log?</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>8. Will you prevent non-U.S. Person from viewing or having access to project areas?</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>9. Will you Ensure ALL Personnel are Trained in Export Controls?</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>10. Will you Ensure that Personnel are Monitoring Compliance on an On-Going Basis?</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
</tbody>
</table>

Notes

Click or tap here to enter text.
Please list any additional physical security measures you will have in place to prevent unauthorized access to Export Controlled secure areas, materials, and computers.

Please check which information security measures you will have in place to protect Export Controlled Data.

External portable hard drives or flash drives, rather than shared central servers, are recommended for data storage provided physical storage is employed when they are not in use (see “one-lock” information under PHYSICAL SECURITY MEASURES). Drives and devices used to store Export Controlled information must be password protected or encrypted. For data storage on drives with network access or backup servers, the Export Controlled information must be secured by encryption and password protection.

Email may not be used for the transfer of Covered Items or Information subject to the ITAR or EAR. A secure file transfer method (SSH/SCP/SFTP/SSL) or mailing a disk or flash drive are preferred methods to transfer Export Controlled information in electronic format. Note: Emailing Export Controlled information subject to regulations other than the EAR and ITAR will be considered on a case-by-case basis, but is NOT authorized unless specified below; when authorized to use email, the sender's is responsible for ensuring that the recipient is physically present in the US at the time of transfer.

<table>
<thead>
<tr>
<th></th>
<th>YES</th>
<th>NO</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Will data be encrypted?</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>2. Will data be password protected?</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>3. Will data be stored ONLY in a non-networked location?</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>4. Will you classify which data is Export Controlled and Non-Export Controlled?</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>5. Will you ensure that data is not sent over unsecured networks?</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>6. Will you ensure that ONLY Project Members (identified in this TCP) have access to Export Controlled equipment, technology, computers and networks?</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>7. Will you ENSURE project computers are NOT connected to a network?</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>8. Will you ENSURE computers have anti-Virus protection software that is updated frequently?</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>9. Will you PROHIBIT the use of external storage devices?</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>10. Will Export Controlled data be DESTROYED after the project is complete?</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>11. Will Export Controlled Computers be DESTROYED or ERASED after the project is complete?</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>12. Will Export Controlled external storage devices be DESTROYED or ERASED after the project is complete?</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>13. Will you ensure that data is not STORED in the CLOUD?</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>
Please list any additional information security measures you will have in place to prevent unauthorized access to Export Controlled data.

Click or tap here to enter text.
COMMON EXPORT CONTROL DEFINITIONS:

**Foreign Person:**
A person who is not a U.S. citizen or lawful permanent resident alien of the U.S. A person lawfully in the U.S. on a visa for work or study is a foreign person. The law makes no exceptions for foreign graduate students or visiting scientists.

**US Person:**
A person who is a U.S. Citizen or lawful Permanent Resident Alien.

**Export:**
Is the transfer of items, technology, software, or technical data found on the USML or CCL out of U.S. territorial borders by any means? Exports out of the U.S. also include the electronic, visual, or verbal transmission of technical data or technology through any means, such as email, verbal discussions, or hand-carrying information on International travel.

**Deemed Export:**
An Export of technology or source code (except encryption source code) is “deemed” to take place when it is released to a foreign national within the U.S. Technology is “released” for export when it is available to foreign nationals for visual inspection; when technology is exchanged orally; or when technology is made available by practice or application under the guidance of persons with knowledge of the technology.

**USE:**
Is defined as “operation, installation, maintenance, repair, overhaul and refurbishing.”

**USML:**
Identifies specially designed military technologies and systems.

**CCL:**
Identifies most other common items, materials, software, and technologies not on the USML which are in the U.S. or of U.S. origin that are also considered “dual use” in nature.
BRIEFING CERTIFICATION FOR SAFEGUARDING EXPORT-CONTROLLED EQUIPMENT, MATERIALS, SOFTWARE, TECHNICAL DATA OR TECHNOLOGY

Must be read and signed by all users (including PI) prior to access of any export-controlled materials or data

Project Title: Click or tap here to enter text.
PI Name: Click or tap here to enter text.
Participant Name: Click or tap here to enter text.
Sponsor: Click or tap here to enter text.

Statement
I understand that my participation on the research project(s) listed may involve the receipt or use of export-controlled technology, items, software or technical data, and that it is unlawful to transfer, send or take export-controlled materials or technology out of the United States. Furthermore, I understand that I may not disclose, orally or visually, or transfer by any means, export-controlled technology or technical data to a non-U.S. person located inside or outside the U.S. without a license or applicable exemption as determined by NDSU’s Export Control Administrator.

The export controlled materials or technology of this project may not be exported to:
- Foreign countries and/or any foreign person, unless the University either obtains a license or determines that an exemption applies and the University informs me of the same.
- Any and all embargoed destinations designated by the Office of Foreign Assets Control http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx
- Anyone found on the Specially Designated Nationals (SDN) list http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx
- Proscribed countries or their citizens located in the United States as listed in 126.1 of the ITAR (if applicable) https://www.pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_126.pdf
- Any person or entity on the Denied Entity List, if EAR is applicable. http://www.bis.doc.gov/entities/default.htm

The Export Control Administrator (NDSU.ExportControls@ndsu.edu or 1-6455) can assist with the screenings listed above.

Responsibilities and Potential Penalties
Researchers may be held personally liable for civil/criminal violations of the U.S. export control regulations. The penalties for unlawful export and disclosure of export controlled information under the various export control regulations can result in civil fines in excess of $1,000,000 and criminal penalties of up to $250,000 in fines and/or up to 10 years in prison.

As a result, you should have a clear understanding of the requirements, and exercise reasonable care in using and sharing export-controlled information, technology, software, or items with others. This TCP has been developed to help you assess, address, and understand your export control obligations, as well as to control access to the export-controlled aspects of this project.

Certification
I hereby certify that I have read and understand this Certification. I understand and agree to follow the procedures outlined in the TCP and that I could be held personally liable if I unlawfully disclose (regardless of form or format) Export Controlled equipment, technology or information to unauthorized persons. I agree to address any questions I have regarding the designation, protection or use of Export Controlled equipment, technology or information to the NDSU Export Control Administrator.

Signature ____________________________ Date ____________

Printed Name ____________________________

PI Initials/Date ____________________________ Export Control Initials/Date ____________________________

63
BRIEFING CERTIFICATION FOR ADDITIONAL PROJECT PERSONNEL IN THE SAFEGUARDING OF EXPORT-CONTROLLED EQUIPMENT, MATERIALS, SOFTWARE, TECHNICAL DATA OR TECHNOLOGY

Must be read and signed by all users (including PI) prior to access of any export-controlled materials or data

Project Title: Click or tap here to enter text.
PI Name: Click or tap here to enter text.
Participant Name: Click or tap here to enter text.
Sponsor: Click or tap here to enter text.

Export Control Compliance:
A Visual Compliance Screening was conducted on the above named individual on:

Date: __________________________ Signature __________________________

Approved □  Disapproved □

Statement

I understand that my participation on the research project(s) listed may involve the receipt or use of export-controlled technology, items, software or technical data, and that it is unlawful to transfer, send or take export-controlled materials or technology out of the United States. Furthermore, I understand that I may not disclose, orally or visually, or transfer by any means, export-controlled technology or technical data to a non-U.S. person located inside or outside the U.S. without a license or applicable exemption as determined by NDSU’s Export Control Administrator.

The export controlled materials or technology of this project may not be exported to:

- Foreign countries and/or any foreign person, unless the University either obtains a license or determines that an exemption applies and the University informs me of the same.
- Any and all embargoed destinations designated by the Office of Foreign Assets Control [http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx](http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx)
- Anyone found on the Specially Designated Nationals (SDN) list [http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx](http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx)
- Proscribed countries or their citizens located in the United States as listed in 126.1 of the ITAR (if applicable) [https://www.pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_126.pdf](https://www.pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_126.pdf)
- Any person or entity on the Denied Entity List, if EAR is applicable. [http://www.bis.doc.gov/entities/default.htm](http://www.bis.doc.gov/entities/default.htm)

The Export Control Administrator ([NDSU.ExportControls@ndsu.edu](mailto:NDSU.ExportControls@ndsu.edu) or 1-6455) can assist with the screenings listed above.

Responsibilities and Potential Penalties

Researchers may be held personally liable for civil/criminal violations of the U.S. export control regulations. The penalties for unlawful export and disclosure of export controlled information under the various export control regulations can result in civil fines in excess of $1,000,000 and criminal penalties of up to $250,000 in fines and/or up to 10 years in prison.

PI Initials/Date  Export Control Initials/Date
BRIEFING CERTIFICATION FOR ADDITIONAL PROJECT PERSONNEL IN THE SAFEGUARDING OF EXPORT-CONTROLLED EQUIPMENT, MATERIALS, SOFTWARE, TECHNICAL DATA OR TECHNOLOGY

Must be read and signed by all users (including PI) prior to access of any export-controlled materials or data

As a result, you should have a clear understanding of the requirements, and exercise reasonable care in using and sharing export-controlled information, technology, software, or items with others. This TCP has been developed to help you assess, address, and understand your export control obligations, as well as to control access to the export-controlled aspects of this project.

**Certification**

I hereby certify that I have read and understand this Certification. I understand and agree to follow the procedures outlined in the TCP and that I could be held personally liable if I unlawfully disclose (regardless of form or format) *Export Controlled equipment, technology or information* to unauthorized persons. I agree to address any questions I have regarding the designation, protection or use of *Export Controlled equipment, technology or information* to the NDSU Export Control Administrator.

______________________________
Signature

______________________________
Date

______________________________
Printed Name
NDSU TCP – Departure Statement – to be completed when an individual no longer requires access to controlled information/items either at the end of the project or his/her departure prior to the end of the project.

Export Administration Regulations and/or ITAR Termination/Departure Statement
Review the following text. Complete the signature confirmation below and return to: 1735 NDSU Research Park Dr.
Fargo, ND 58102
Phone: 701.231.6455
Fax: 701.231.8098
Email: ndsu.exportcontrols@ndsu.edu

Technology and Technical Data

Export Administration Regulations
As defined in the Export Administration regulations 15 CFR §772.1 et seq.:

“Specific information necessary for the “development”, “production”, or “use” of a product. The information takes the form of “technical data” or “technical assistance”. Controlled “technology” is defined in the General Technology Note and in the Commerce Control List (Supplement No. 1 to part 774 of the EAR). “Technology” also is specific information necessary for any of the following: Operation, installation (including on-site installation), maintenance (checking), repair, overhaul, refurbishing, or other terms specified in ECCNs on the CCL that control “technology.”

N.B.: Technical assistance—May take forms such as instruction, skills training, working knowledge, consulting services.

Note 1: “Technical assistance” may involve transfer of “technical data”.

Note 2: “Technology” not elsewhere specified on the CCL is designated as EAR99, unless the “technology” is subject to the exclusive jurisdiction of another U.S. Government agency (see §734.3(b)(1)) or is otherwise not subject to the EAR (see §734.4(b)(2) and (b)(3) and §§734.7 through 734.11 of the EAR).”

“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 memories.”

This definition does not include basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community or information released in catalog courses and associated teaching laboratories of academic institutions.

ITAR
As defined in 22 CFR §120.10, technical data is:

(1) Information, other than software as defined in 22 CFR §120.10(a)(4), 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 as defined in 22 CFR §121.8(f) directly related to defense articles;

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 § 120.11. It does not include basic marketing information on function or purpose or general system descriptions of defense article.

I certify that I have not given or disclosed, nor will I disclose, to any unauthorized person any documents, reports, or other Technology or Technical data, considered to be export controlled or sensitive information associated with NDSU research. I acknowledge that if concerns arise; I may be contacted.

Full Name: Signature:

Date:

Email address for future contact if necessary (non - NDSU domain)
Closure of an active Technology Control Plan requires the PI and any co-PI(s) to affirm that controlled data/information is authorized to be disseminated/published or properly archived to avoid unauthorized disclosure. Please complete once a project is fully closed out. Return the document to:

1735 NDSU Research Park Dr.
Fargo, ND 58102
Phone: 701.231.6455
Fax: 701.231.8098
Email: ndsu.exportcontrols@ndsu.edu

A closeout review will be scheduled thereafter.

---

### Section A. Technology Control Plan Information

Project Title: ____________________________________________

Principle Investigator (PI): ________________________________

---

### Section B. Access and Distribution Status

**Publication Status**

- [ ] The sponsor has allowed all of the data/information generated from this project to be published or presented openly.

- [ ] The sponsor allowed some of the data to be published or presented openly.

- [ ] All of the data generated from this project remained restricted.

**Student Thesis**

- [ ] This work supported student thesis project(s) which remain confidential.

  If yes, Name of Student: ________________________________

- [ ] This work supported student thesis project(s) which were approved for open publication.
If yes, Name of Student: ____________________________

☐ This work did not support student thesis project(s).

**Current/Future Data Access Status**

☐ Our research team retains restricted data or equipment for the purpose of data/record retention, but has no plans to continue research with it at this time. (Describe secure storage parameters in Section C below).

☐ Our team no longer possesses any data or equipment that require controls on physical access for export control purposes. (Describe disposal procedures in Section C below).

**Current/Future Physical Access**

☐ I have evaluated the possession of badge/key/physical access to any areas that were specifically segmented for the project.

☐ Equipment or hard copy data I am retaining is locked in an appropriate location under at least two levels of security with access limited to approved persons with need-to-know.

☐ All equipment/hardware received and/or generated has been returned to the sponsor.

**Continuation Efforts**

☐ I plan to continue this work for other projects (funded or unfunded) Explain:

☐ I plan to utilize discoveries/developed equipment and process modifications/data and data derivatives from this project for future work. Explain:

---

**Section C. Disposition**

---

**Retention - The research team will keep (Check all that apply)**

<table>
<thead>
<tr>
<th>Category</th>
<th>Retention Period - (specific length, date or indefinite)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlled Equipment/Test Articles</td>
<td>______________________________________________________</td>
</tr>
<tr>
<td>Hard Copy Controlled Data/Information</td>
<td>______________________________________________________</td>
</tr>
<tr>
<td>Electronic Controlled Data/Information</td>
<td>______________________________________________________</td>
</tr>
<tr>
<td>Other - Explain:</td>
<td>______________________________________________________</td>
</tr>
</tbody>
</table>

Storage – for those items indicated above that will be retained, outline the security measures.

Physical Items: ______________________________________________________

Electronic data/information: ___________________________________________
Disposal - plan for disposal after an appropriate record retention period.

Physical Items (hardcopy documents must be securely destroyed by cross-cut shredding or another method that ensures information cannot be reconstructed.)

Electronic data/Information (Once a system housing export-controlled data has reached the end of its usable life, its hard drive or other non-volatile media should be securely wiped using SDelete, DBan, or other secure overwriting utility. Information on shredding software can be found at http://dban.sourceforge.net/. NDSU IT staff may also be engaged in any electronic data destruction or deletion process to ensure appropriate disposal. Digital deletion of the entire device is the preferred solution).

Section D. Technology Control Plan Closure Acknowledgement Statement

At this time, this project is closed. Data that was not allowed to be put into the public domain has been either destroyed, returned to the sponsor, or securely stored per the provisions above. I will not begin work with this data without prior approval from the sponsor and the NDSU Export Control Administrator (ECA). If I plan to utilize controlled data from this project for any new purpose, or suspect unauthorized access or use, I will contact the ECA (ndsuelexportcontrols@ndsu.edu) for assistance in creating a new Technology Control Plan. I understand that I will be contacted by the ECA to schedule and complete a close out review of this project plan.

Principle Investigator Signature and Date: ____________________________

Co-Principle Investigator Signature and Date: ____________________________
NDSU’s Export Control Office:  
International Travel Briefing

Traveling Outside the U.S.? You are about to Become an “Exporter”

- Any tangible items that you are taking to a foreign country are considered “exports” by the United States Government, even if you are planning on bringing the items back upon your return.
- Technical information located on your laptop’s hard drive or in a hard copy notebook is considered to be an export of “technology”/ “technical data”, once the laptop or notebook leaves the U.S.
- Even technical know-how that is in your head, if shared with a foreign national, is considered to be a type of export.

When you leave the United States, you need to know your responsibilities under export control regulations. In particular if you are traveling with your laptop or any other electronic devices these items along with the underlying technology, any data on your device, proprietary information, confidential records, and encryption software are all subject to export control regulations. Some foreign governments have regulations that permit the seizure of travelers’ computers and the review of their contents. U.S. Customs officials are also authorized to review the contents of travelers’ laptops without probable cause and can be held until your return.

Export controls issues can arise in a variety of surprising circumstances; are not always intuitive; and the laws are fact-specific, complex, and continually changing. Given this complexity, the NDSU community should seek guidance from NDSU’s ECA when dealing with export control questions and concerns:

Lynn Titus Jr., Export Control Administrator: (701) 231-6455 / ndsu.exportcontrols@ndsu.edu / NDSU’s Research 1

Building. See also http://www.ndsu.edu/research/export_controls/miscellaneous/international_travel.html, to be directed to an appropriate authority regarding your questions, concerns, or to make reports of unscrupulous activities abroad or in the United States or its territories.

BRIEFING

The FBI considers the following to be threats to our national security, regardless of the country involved:

Any foreign intelligence activity that is:

- targeting U.S. intelligence and foreign affairs information and U.S. Government Officials or official representatives
- directed at critical technology
- directed at the collection of U.S. industrial proprietary economic information
- directed at the collection of information relating to defense establishments and national preparedness
- involving the proliferation of special weapons of mass destruction
- involving perception management and active measures

If you become aware of or suspect any foreign intelligence activity aimed at the above list, notify your local in-country FBI office.
PRIOR TO DEPARTURE

1. You may also want to contact the Department of State recorded messages at 202-647-5225.

2. Carefully complete your Visa application, as it will be scrutinized. If you are a naturalized U.S. citizen returning to the country of your origin, your citizenship may be questioned.

3. Ensure that items you carry with you are not controversial or prohibited. Political material or anything that could be considered pornographic should not be carried. If you carry prescription drugs with you, be certain that they are clearly marked and bring only necessary quantities.

4. Carrying letters, packages or gifts to individuals in other countries should be avoided. You may be viewed as a courier attempting to bring the material for subversive or illegal purposes.

5. DO NOT TAKE CONTROLLED MATERIAL with you as you travel.

6. Limit the amount of identification that you take. If you have several forms of Government ID (i.e. University ID, building pass), bring only one ID with you (or the minimum required for entry and exit). Make a photocopy of any ID or credit card you will be bringing and leave the copy at home. Write down your passport number and keep it separate from your passport. Do the same with your address and telephone.

7. The carrying of laptop computers is discouraged, but not prohibited. Consult your sponsor’s contracting officer before you take your laptop or similar computing equipment.

UPON ARRIVAL

1. (If required) an accurate declaration of all money and valuables should be made at entry. Some countries give the traveler a copy of the declaration, which must be surrendered upon leaving. It is important to keep receipts of all money exchanges, these frequently are required upon departure. Undeclared sums of U.S. or other currency are likely to cause difficulty with authorities and may be confiscated upon departure.

2. (If required) Declare such items as cameras, radios, etc., to preclude possible explanations, customs charges, or confiscation when you leave.

3. In some cases, especially non-westernized countries like Cuba, Syria, N. Korea, etc. you should contact the American Embassy or Consulate prior to your arrival, and provide your local address and the probable length of your visit.

4. Use of public transportation is recommended rather than driving yourself, because involvement in traffic accidents can be problematic. Taxis are the preferred mode of transportation. State Department travel advisories provide updated information regarding public transportation concerns in the country you are visiting.

YOUR ACTIVITIES AND BEHAVIOR

1. In all of your activities, show discretion and common sense. MAINTAIN A LOW PROFILE. Refrain from any behavior that may make you conspicuous or a potential target. NEVER engage in any illegal activity, excessive drinking or gambling. Use your best judgment to carefully avoid any situation that may allow a foreign intelligence agency the opportunity to coerce or blackmail you.

2. Do not discuss controlled or sensitive information in any vehicle, restaurant, hotel room, hotel lobby, or other public place. In any public place, your conversation may be overheard, or you may be monitored. If you need to call the U.S.
to discuss controlled or sensitive information, locate a secure telephone by contacting the in-country FBI office or the U.S. Embassy.

3. If you locate any possible surveillance equipment, such as microphones, telephone taps, miniature recording devices, or cameras, do not try to neutralize or dismantle it. Assume the device is operable and that active monitoring is ongoing. Report what you have found to the U.S. Embassy or Consulate. When you return, advise your local FBI agent.

4. Never leave luggage or briefcases that contain controlled or sensitive information unattended (whether in the US or US Territory or not). This includes leaving your briefcase in your hotel room. We encourage you to keep your briefcase containing sensitive information in your immediate possession at all times.

5. Foreign Intelligence Services may place you under physical surveillance or you may suspect that you are being watched. It is better to ignore the surveillance than attempt to lose or evade it. In any event your actions should be prudent and not likely to generate suspicion. Good precautionary measures are to use well-traveled highways and avoid establishing routine schedules.

6. Never try to photograph military personnel, installations, or other “restricted areas”. It is best to also refrain from photographing police installations, industrial structures, transportation facilities and boarder areas.

7. Beware of overly friendly or solicitous people that you meet. Do not establish personal or intimate relationships with these individuals as they may be employed by the intelligence service. Do not share any work related information with any person who does not have a need to know.

8. Do not accept packages and agree to transport them back to the U.S. Even if your friends, relatives, and professional contacts, make the request, do not accept the package.

9. If you will be on an extended visit and expect to be writing or receiving mail, remember that it may be subjected to censorship. Never make references to any controlled or sensitive information.

10. Avoid any areas where there is political or ethnic unrest, demonstrations or protests.

11. Should you be detained or arrested for any reason by the police or other officials, be cooperative, and contact the U.S. Embassy or Consulate immediately. Do not make any statements or sign any documents you do not fully understand until you have conferred with an Embassy representative.

12. Do not leave documents in hotel safes.

13. You may keep this travel briefing document for reference, but do not carry it with you.

**UPON YOUR RETURN**

Contact your local FBI agent to report suspicious foreign contacts and any unusual incidents. If you have a security clearance through a third party, you may need to receive a security debriefing if you have been abroad for more than a certain number of days that is established by the third-party security office. You are required to report all contacts with individuals of any nationality, either within or outside the scope of your official activities in which:

- Illegal or unauthorized access is sought to controlled or sensitive information.
- You are concerned that you may be the target of an actual or attempted exploitation by a foreign entity.

Note: This document was adapted from several “Defensive Security Briefings” found at national laboratories around the USA.
Plan Ahead to Avoid Violations – Work With Your Export Control Office

Just because an item is listed on the CCL does not mean that you cannot take it with you to your destination country. Export restrictions on CCL items vary, depending upon your destination country, those to whom you expect to release such items, and how you expect they will use them. Even if a license is indicated for your export, it is usually possible to find a documented reason why technical information can be excluded from regulation or a license exception for exported tangible items. Similar forgiveness can often be found in regulations that other agencies apply to your travels, such as the sanction programs.

Working with your Export Control Office well ahead of your international journey is the best way to ensure that your exported goods and information can be taken / sent without a license or violation of the export control and sanction program regulations. If any Risk Factor above is present in your planned travel, please contact:

Lynn Titus Jr., Export Control Administrator
(701) 231-6455 / ndsu.exportcontrols@ndsu.edu / NDSU’s Research 1 Building.
See also http://www.ndsu.edu/research/export_controls/miscellaneous/international_travel.html.

Three Noteworthy Federal Agencies that Have Jurisdiction over You and Your Exports:

- The Department of State’s Directorate of Defense Trade Controls (DDTC), which implements and enforces strict controls upon tangible items and technical data that are determined to have been “specifically designed, developed, configured, adapted or modified for a military application.” Such items and data can be found listed on the U.S. Munitions List in the DDTC’s International Traffic in Arms Regulations.

- The Department of Commerce’s Bureau of Industry and Security (BIS), which implements and enforces regulations that prohibit the release of certain commodities and information to certain countries or to their citizens (regardless of their location), if it is believed that there is a potential for such items to be used to undermine U.S. security, policy, or other vital interests. Such items are often referred to as “dual-use” items and can be found on the Commerce Control List (CCL) in BIS’s Export Administration Regulations (EAR). Note that many items on the CCL are commercially available in the U.S.

- The Department of the Treasury’s Office of Foreign Assets Control (OFAC), which prohibits varying types of transactions (e.g., financial, commercial, and even academic) and activities with or in foreign countries (or with their citizens, regardless of location) through its sanction programs, which are designed to encourage other countries’, entities’, or individuals’ cooperation with U.S. policies and interests worldwide.

I’m Just a University Employee. Why Should I Have to Worry About These Agencies’ Regulations?

- Depending upon their areas of expertise, NDSU employees may work with items and foreign countries covered by DDTC, BIS, and OFAC regulations.

- US Customs officials are authorized to search or retain electronic devices and other items leaving the U.S., even without probable cause, to look for violation of export control and sanction program regulations.

- Other universities and/or their employees have, by violating export control or sanction program regulations, exposed themselves to steep financial penalties and incarceration.
Risk Factors Contributing to Violations

If any of these factors apply to your planned travel, please contact the NDSU Export Controls Office before you travel by using the contact information provided below.

- **Sanctioned Countries**
  - Will you be traveling to a country subject to OFAC sanctions?
  - Each sanction program is different from the other. Some programs broadly prohibit imports and exports of goods, technology and services from/to certain countries. Other programs only prohibit transactions with certain listed entities and individuals. Sanction programs change over time, sometimes rapidly, as world events affect the U.S. Government’s relationship with other countries and governments.
  - Before you travel, visit the OFAC website to determine whether you will be visiting a sanctioned country.

- **Restricted People and Entities**
  - Do you expect to enter into transactions with persons or entities that the federal government has determined must be excluded from such transactions?
  - We recommend that you search a Consolidated Screening List for the foreign parties with whom you expect to interact professionally during your international travel.

- **Defense Articles and Data**
  - Will you be taking to any foreign country tangible items or information related to research or other activities that support defense-related projects or objectives? One should note that the DDTC presently considers not only things like missiles and fighter jets to be defense articles, but also spacecraft designed for scientific objectives. This includes scientific satellites and other space-related equipment, including support apparatus, such as launch platforms and telemetry stations.

- **Commerce Control List Commodities and Technical Information**
  - Will you be taking with you Commodities or technical information found on the CCL?
  - The only way to know for certain is to perform a keyword search on Title 15, Part 774 (a/k/a the “Commerce Control List”), which can be found in a searchable format at the GPO Access website. If provided sufficient notice before your international trip, your Export Control Office can assist with such a search.
  - Risk of finding your items restricted for export by the CCL increases when:
    - Your travel will take you to one or more of the “T5” Countries, which consist of Cuba, Iran, North Korea, Syria and Sudan. Some or all of these countries are subject to not only heightened BIS export restrictions, but also to heightened export and transaction restrictions imposed by OFAC and DDTC.
    - You will be taking items related to your work at NDSU, including: a) **tangible items**, such as samples, prototypes, and equipment; and/or b) **unpublished research technical data**; AND you work in the following areas:
- Chemical, Biotechnology and Biomedical Engineering
- Materials Technology
- Remote Sensing, Imaging and Reconnaissance
- Navigation, Avionics and Flight Control
- Robotics
- Propulsion System and Unmanned Air Vehicle Subsystems
- Telecommunications/Networking Nuclear Technology
- Sensors and Sensor Technology
- Advanced Computer/Microelectronic Technology
- Information Security/Encryption
- Laser and Directed Energy Systems
- Rocket Systems
- Marine Technology

- Risk of finding your items restricted for export by the CCL decreases when:
  - You will be traveling to countries sharing a relatively friendly, cooperative relationship with the U.S., such as with the countries that belong to N.A.T.O. and other treaty-based groups.
  - Your work is in a field that is not fundamentally “technical”, such as a discipline traditionally included in the humanities. However, beware of electronic and medical equipment exported in support of your overseas work, and don’t forget that OFAC sanction regulations may still apply to your destination and your activities there.
  - The tangible items that you are taking are: (a) personal effects that most people need and use when they travel outside the U.S., and/or (b) such items will be under your effective control throughout your travel and will return to the U.S. with you within one year or less.
  - The work-related information that you take with you (e.g., on your laptop or other media)
    A. is already published and generally accessible to the interested public
    B. is available to anyone wishing to take a university catalog course
    C. was generated by basic or applied science and engineering and is the type of information that is ordinarily published and shared broadly within the scientific community (often referred to as the results of “fundamental research”).

- A Common Question: What about my laptop, smart phone, or data storage device?
  - Short answer: It depends upon a device’s features, the software or data that you have loaded on it, who owns it, the purposes for which you are taking it, and where you want to take it.
  - Fortunately, many of these items are listed on the CCL under Export Control Classification Number (ECCN) 5A992 and can be taken to most countries, except for those subject to embargoes and other heightened export controls.
  - The software that operates or is used on these items, including mass-market and open-source products, also can be found on the CCL (ECCN 5D992) and are controlled separately from the hardware on which they’re used. If possible, we recommend traveling internationally with personally-owned laptops containing only software, technical data, and personal information considered essential for the trip.
Newer, more advanced computing and communication devices (as well as associated software), especially those that provide exceptionally strong levels of encryption, may be difficult to take to other countries, especially the T5 countries. If you know or suspect that your electronic devices are more advanced than the average, it would be a good idea to determine what the items’ ECCNs are by asking the manufacturer and working with your Export Control Office.

Even though the CCL may indicate that a license is required to export your laptop to a particular country, a license exception can often be found that will allow you to export it on a temporary basis. For example:

- Depending upon the country, you may be allowed to travel with a NDSU-owned laptop under a temporary export (TMP) license exception, if the laptop and your use of it qualify under BIS’s definition of a “tool of the trade.”

- In other instances, you may only be able to take a laptop to another country if it qualifies for a baggage (BAG) license exception which, among other things, requires that the laptop be owned by the traveler.

- When taking equipment and other export-controlled items to other countries under a license exception, you should understand the conditions under which the exception can be used. It is also a good idea to take with you a letter from your Export Control Office indicating that the license exception is being invoked for your temporary export.

**Taking Electronic Devices**

Researchers commonly travel with commercially available electronic devices such as laptops, PDAs, iPads, cell phones, drives, and other digital storage devices. These items often come with pre-loaded encryption software which is subject to the Department of Commerce, Export Control Regulations (EAR). Many of these items can be temporarily exported under the EAR license exception “Temporary exports-Tools of the Trade” (TMP) or Baggage (BAG).

The TMP License Exception provides that when laptops, PDAs and other digital storage devices (and related technology and software) are being used for professional purposes, returned within 12 months, kept under effective control of the exporter while abroad (i.e., kept in a hotel safe or other secured space or facility) and other security precautions are taken against unauthorized release of technology (i.e., use of secure connections, password systems, and personal firewalls), then the TMP License Exception might apply.

The baggage (BAG) license exception covers personal items that are owned by the researcher and intended only for their personal use. These License Exceptions do not apply to Cuba, Iran, North Korea, Sudan, or Syria. You must contact the NDSU Export Control Administrator before using either of these License Exceptions, as they are subject to record-keeping requirements.

**Sharing Information While Traveling**

You can freely take with you and exchange with anyone the results of fundamental research conducted on the NDSU campuses. However, if your work involves technical data controlled for defense of non-defense work a license from the Department of State may be required. Contact the NDSU Export Control Administrator for more information.

**Encryption – Publicly Available**
NDSU does not provide encryption software on their computers or laptops. Within Windows 10 and Windows 7 there is a “bit locker” for full disc encryption; however, if you choose to utilize this option for encryption and you lose your password, NDSU staff will not be able to gain access to the encrypted material.

Countries that Restrict the Import of Encryption Products

Because encryption products can be used for illegal purposes many countries may ban or severely regulate the import and export of encryption products. The import of your laptop with encryption software to certain countries could violate the import regulations of the country to which you are traveling, and could result in your laptop being confiscated, fines, or in other penalties.

Encryption – Developed at NDSU

NDSU researchers, including faculty, staff and students, who are developing encryption software need to be aware of export control implications.

In most instances, encryption code developed at NDSU falls under the Fundamental Research Exclusion (FRE) and is not subject to export control laws and regulations. However, the FRE can be eroded if restrictions on the research exist. It is important that researchers make available any encryption code developed during the course of their research on a publicly-available website as quickly as possible. Access to the code should be open and not subject to login or password requirements. Failure to make the code publicly available in a timely way may trigger the application of export control laws, including restrictions on “deemed exports” to non-U.S. citizens within the U.S.

“Strong” Dual-Use Encryption Code

While most encryption code should be posted immediately to a publicly accessible website, researchers must inform an export control administrator before making software available if it falls under the definition of “strong encryption software”. Strong dual-use encryption, is defined in the Export Administration Regulations, Part 774, Commerce Control List, Category 5 (Part 2) Information Security at 5A002 (encrypted hardware) and 5D002 (encryption software).

The above content is offered as guidance to individuals. It is intended as a general overview of issues related to the export of encryption software and is not exhaustive. Questions about the application of export control regulations to specific situations should be directed to NDSU Export Control Administrator.
CERTIFICATION ON THE HANDLING OF EXPORT-CONTROLLED ITEMS/INFORMATION
NOTE: this form is not a blanket form for all activities, and must be submitted with each instance of request/certification.

Overview. This NDSU project/activity involves the use of export-controlled information. As a result, the project/activity comes under the purview of either the State Department’s International Traffic in Arms Regulations (ITAR) at http://pmdtct.state.gov/regulations_laws/itar_official.html, or the Department of Commerce’s Export Administration Regulations (EAR) at http://www.access.gpo.gov/bis/ear/ear_data.html, or both. Under the EAR, the ITAR, and other export control regulations, it is unlawful to send or take export-controlled items or information out of the U.S. This includes transferring or disclosing information orally or visually, or transferring export-controlled items or information to a foreign person inside or outside the U.S. without proper Federal authorization. Export licenses may be required for foreign nationals to access export-controlled information. A foreign person is a person who is not a U.S. citizen or permanent resident alien of the U.S. (Note: the laws make no exceptions for foreign graduate or post-doctoral students.) Pertinent technical information, data, materials, software, or hardware (etc.) generated from this project/activity must be secured from use and/or observation by unlicensed non-U.S. citizens. Security measures will be appropriate to the classification involved, and include, but are not limited to, the execution of a Technology Control Plan (TCP).

Reasonable Care. Faculty, students, researchers, and other NDSU personnel may be held personally liable for violations of the ITAR and the EAR. Individuals who will have access to export-controlled information must exercise all reasonable care when handling and sharing export-controlled information/items, and ensure (when/where applicable) that they follow and enforce the TCP enacted for this project/activity. Contact NDSU’s Export Control Administrator (ECA) immediately if you anticipate, suspect, or have knowledge of any NDSU non-compliance (past, present, or future) with U.S. export controls laws and regulations.

Penalties. Each Federal agency has its own procedures for enforcement, but violations (unlawful export and disclosure of export-controlled information and items) of any of these regulations can result in significant institutional and personal penalties, including fines of up to $1,000,000 per violation; incarceration for up to 20 years; and the loss of future exporting privileges. By working with NDSU’s Export Control Administrator and striving for export control compliance, risk can be minimized for both individuals and NDSU.

<table>
<thead>
<tr>
<th>Responsible Individual:</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td></td>
</tr>
<tr>
<td>Department/Unit:</td>
<td>Telephone:</td>
</tr>
<tr>
<td>Mailing Address:</td>
<td>Email:</td>
</tr>
<tr>
<td>Project Title:</td>
<td>Project Number:</td>
</tr>
<tr>
<td>Sponsor (if applicable):</td>
<td></td>
</tr>
</tbody>
</table>

CERTIFICATION: By signing below, I hereby certify that I have read and understand this certification, and that I understand my overall export compliance responsibilities hereto (as described in this document and in “NDSU’s Export Controls Compliance Manual,” available at www.ndsu.edu/research/exportcontrols). I understand that I may be held personally liable if I unlawfully export and/or transfer/disclose, in any form or format, export-controlled information and items to unauthorized persons. I agree to address any questions or concerns I have regarding the classification, designation, protection, or use of export-controlled items/information with NDSU’s ECA.

/s/__________________________ __________________________
Signature of Certifying Individual (E-Signatures Legal and Enforceable) Date

RETURN TO NDSU’s EXPORT CONTROL ADMINISTRATOR: VIA E-MAIL / ONLINE / TO DEPT. 4000, RESEARCH 1 BLDG.

/s/__________________________
Signature of NDSU’s Export Control Administrator

Current Version: 4/19/17.

Export control laws are complex and fact-specific. Regulations, rules, and lists for specifying who or what is considered export-sensitive – and where export controls apply – are subject to change. The information contained herein is intended to provide a very brief outline of basic export control information. It should not be taken as formal legal advice, and NDSU cannot — and does not — warrant the legal sufficiency of the information contained herein.
Export control laws are complex and fact-specific. Regulations, rules, and lists for specifying who or what is considered export-sensitive – and where export controls apply – are subject to change. The information contained herein is intended to provide a very brief outline of basic export control information. It should not be taken as formal legal advice, and NDSU cannot – and does not – warrant the legal sufficiency of the information contained herein.
FULL-TIME BONA FIDE EMPLOYEE CERTIFICATION AND WRITTEN NOTIFICATION

For International Traffic in Arms Regulations (ITAR) controlled items, technology, and software ONLY.
NOTE: this form is not a blanket form for all activities, and must be submitted with each instance of request/certification.

Bona Fide Employee:
Name: 
Department/Unit: 
Mailing Address: 
Supervisor/Chair/Etc.: 
Name: 
Date: 
Telephone: 
Employee 
Email: 
Supervisor 
Email: 

The International Traffic in Arms Regulations (ITAR) is a set of Federal regulations that govern the export and re-export of defense articles, defense services, and related technical data from the United States to any foreign destination – or to any foreign person, whether located in the United States or abroad. Under a specific exemption (22 C.F.R § 125.4(b)(10)), the ITAR allows NDSU to disclose unclassified technical data in the U.S. to a foreign person who is the University’s bona fide and full-time regular employee IF:
- the foreign person is a full-time, bona fide, regular NDSU employee (not temporary/adjunct foreign national faculty, or foreign national student/post-doc researcher);
- the foreign person employee’s permanent abode throughout the period of employment is in the United States;
- the foreign person employee is not a national of a country to which exports are ITAR-prohibited (ITAR – 22 C.F.R. § 126.1);
- NDSU informs the individual in writing that the technical data may not be transferred to other foreign persons without the prior written approval of the Department of State’s Directorate of Defense Trade Controls (DDTC); and
- NDSU complies with certain additional legal requirements set forth in the ITAR.

To be eligible for this ITAR license exemption, certify to the following by checking each statement:

1. I am a regular, full-time, bona fide employee of NDSU.
2. My permanent abode throughout my employment with NDSU is in the United States.
3. I am not a national of a country to which exports are prohibited pursuant to ITAR § 126.1.
   a. My country of origin is: __________________________
   b. My country of most recent citizenship is: __________________________
   c. Other countries of citizenship (write “N/A” if not applicable):
4. Through this notification, I have been informed in writing by NDSU that unclassified, export-controlled technical data or items may not be transferred to other foreign persons without the prior written approval of the DDTC.
5. I will not transfer, disclose, and/or otherwise export to other foreign persons or foreign entities any information and items that have been identified as export-controlled (under ANY set of Federal export control laws and regulations).

CERTIFICATION: By checking the above boxes and signing below, I hereby certify that I have read and understand this certification, and that I understand my overall export compliance responsibilities hereto (as described in this document and in “NDSU’s Export Controls Compliance Manual,” available at www.ndsu.edu/research/exportcontrols). I understand that I may be held personally liable if I unlawfully export and/or transfer/disclose, in any form or format, export-controlled information and items to unauthorized persons. I agree to address any questions or concerns I have regarding the classification, designation, protection, or use of export-controlled items/information with NDSU’s ECO.

/s/ __________________________
Signature of Certifying Individual (E-Signatures Legal and Enforceable) 
________________________
Date

RETURN TO NDSU’s EXPORT CONTROL ADMINISTRATOR: VIA E-MAIL / ONLINE / TO DEPT. 4000, RESEARCH 1 BLDG.

Current Version: 04/21/17.
Export control laws are complex and fact-specific. Regulations, rules, and lists for specifying who or what is considered export-sensitive – and where export controls apply – are subject to change. The foregoing information is intended to provide a very brief outline of basic export control information. It should not be taken as formal legal advice, and NDSU cannot – and does not – warrant the legal sufficiency of the information contained herein.
Export control laws are complex and fact-specific. Regulations, rules, and lists for specifying who or what is considered export-sensitive – and where export controls apply – are subject to change. The foregoing information is intended to provide a very brief outline of basic export control information. It should not be taken as formal legal advice, and NDSU cannot – and does not – warrant the legal sufficiency of the information contained herein.
To: University Export Compliance Administrator
From: Insert Name of NDSU PI or Employee.
Date: Click here to enter a date.

Re: Export License Exception for Temporary Exports/Re-exports*

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 Department of Commerce’s Export Administration Regulations (EAR) makes an exception to licensing requirements for the temporary export or re-export 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 here (Brand/model, NDSU inventory number, if available. Photographs may be included.)

By my signature below, I certify that:

1. I will ship or hand-carry the items, technology, or software to insert name of country(s) traveling to as a “tool of the trade” to conduct NDSU 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 NDSU’s Export Compliance Administrator.

6. I will not ship or hand carry an item, technology or software incorporating NDSU developed non-commercial encryption source code outside of U.S borders without receiving written approval from NDSU’s Export Control Administrator;
7. The items, technology or software described above are not defense articles or technical data controlled under the ITAR and will not be used for nuclear research, military purposes, or the development of weapons of mass destruction;

8. The technology will not be used for foreign production purposes or for technical assistance unless authorized by the Bureau of Industry and Security; and

9. I will promptly report the loss, theft, unauthorized access, or compromise of NDSU property listed in this Certification to NDSU’s Export Control Office at 701-231-6455, or by email at ndsu.exportcontrols@ndsu.edu.

*Keep a signed copy with you when traveling abroad*
To: University Export Compliance Administrator
From: Insert Name of NDSU PI or Employee.
Date: Click here to enter a date.

Re: Export License Exception for Temporary Exports/Re-exports

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 Department of Commerce’s Export Administration Regulations (EAR) makes an exception to licensing requirements for the temporary export or re-export 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 here (Brand/model, if available; photographs may be attached)

By my signature below, I certify that:

1. I personally own the items, technology, or software I am taking abroad to insert name of country(s) traveling to;
2. I am not shipping the items as unaccompanied baggage;
3. The items, technology, or software are intended for necessary and appropriate personal use or use by a member or my immediate family travelling with me;
4. The items, technology, or software are not intended for sale or other disposal
5. I will return the items, technology, or software to the U.S.
6. 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);
7. 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;
8. The items, technology or software described above are not defense articles or technical data controlled under the ITAR and will not be used for nuclear research, military purposes, or the development of weapons of mass destruction;
9. The technology will not be used for foreign production purposes or for technical assistance unless authorized by the Bureau of Industry and Security; and

10. I will not ship or hand-carry the items, technology or software to Iran, Syria, Cuba, North Korea, Libya or Sudan without consulting with NDSU’s Export Control Administrator;

Print Name

EMPL ID

Signature

Date

*Keep a signed copy with you when traveling abroad*
Sample Agreement (Article) Language to address export controls in various types of NDSU Agreements

The following language is intended to provide NDSU with sample or model language that it may adapt to the following types of agreements for export control purposes. Please note that this is merely sample language for guidance purposes: we recommend that NDSU Counsel carefully review this suggested language and conform it accordingly to how NDSU would normally prepare its contractual provisions.

- Fabrication/Service Contracts (where NDSU is performing a fee-for-service contract that falls outside of fundamental research)
- Lease Agreements (where NDSU is a landlord to an external party)
- Non-Disclosure Agreements (incoming NDAs/data being provided to NDSU)
- Master Service Agreements (where NDSU is procuring a service on behalf of the University)

Fabrication/Service Contracts

Article X: Export Controls

Where North Dakota State University is providing a fee-based service or is fabricating any item for [name Agreement party], a prior determination by the parties will be made as to whether the agreed-upon work is export controlled. Export controls may attach a) to the technology or process that is being used to perform the service; b) the end product or commodity (where applicable); c) proprietary technology or software that NDSU received from [name Agreement party or any other external party] that is necessary for the agreed-upon work; or d) materials used in the production or fabrication process. This determination shall occur and be mutually confirmed by the parties at least [X days] prior to the commencement of such work so that export control compliance can timely addressed.

As to any export controlled item which [name Agreement party] intends to provide the NDSU under this Agreement, [name Agreement party] shall provide NDSU with at least 30 days notification of its intent to provide such item(s) so that any necessary compliance measures can be undertaken on a timely basis.

Article X: General Export Control Compliance

[Note: many institutions include something like the following as part of an overall compliance definition/liability framework]

It is North Dakota State University’s policy to remain fully compliant at all times with all U.S. export control regulations, including but not limited to the Export Administration Regulations; International Traffic in Arms Regulations; and embargo sanctions under the Office of Foreign Assets Control (OFAC). Therefore, to the extent that [named Agreement party or any other party to this contract] does not comply with said regulations, North Dakota State University will not be held responsible or liable for such non-compliance.
Non-Disclosure Agreements

[Note: this language is intended to address incoming data or information that NDSU would need to address from an export control agreement.]

Article X: Export Controls

It is North Dakota State University’s policy to remain fully compliant at all times with all U.S. export control regulations, including but not limited to the Export Administration Regulations; International Traffic in Arms Regulations; and embargo sanctions under the Office of Foreign Assets Control (OFAC). Therefore, in the event that [name NDA party/sponsor] wishes to provide export controlled data or information to NDSU during the course of activity under this Agreement, [name party] must first notify NDSU of its intention to provide this data at least 30 days in advance of actually providing this data or information, and indicate who at NDSU will be the intended recipient. NDSU will then determine whether it can or cannot accept such data, the conditions for such receipt if agreed upon, and communicate said determination back to [name party/sponsor].

Lease Agreements

Article X: Export Controls

[Note: it is important to distinguish those situations where (a) the lease agreement is purely a landlord (NDSU)/tenant (unrelated) party situation vs. (b) situations where an NDSU employee is participating in the work that the tenant is doing (on behalf of NDSU), or the tenant’s work contemplates the use of NDSU resources beyond the lease agreement itself.] It is critical that any potential conflict of interest with regard to collaboration with a tenant, i.e. work being conducted on behalf of NDSU vs. private consulting etc., be vetted in advance, as this could affect the lease agreement as well.

Type (a)

It is North Dakota State University’s policy to remain fully compliant at all times with all U.S. export control regulations, including but not limited to the Export Administration Regulations; International Traffic in Arms Regulations; and embargo sanctions under the Office of Foreign Assets Control (OFAC). Therefore, to the extent that [named Lease Agreement party any other party to this lease Agreement] does not comply with said regulations during the term of this lease Agreement, North Dakota State University will not be held responsible or liable for such non-compliance.

Type (b)

It is North Dakota State University’s policy to remain fully compliant at all times with all U.S. export control regulations, including but not limited to the Export Administration Regulations; International Traffic in Arms Regulations; and embargo sanctions under the Office of Foreign Assets Control (OFAC). Therefore to the extent that NDSU personnel are collaborating or participating in any work being conducted in said leased premises, each party will remain strictly responsible for its own compliance with all U.S. export control regulations. In the event that [
named Lease Agreement party or any other party to this lease Agreement] does not comply with said regulations during the term of this lease Agreement, North Dakota State University will not be held responsible or liable for such non-compliance.

**Master Service Agreements/Contracts**

[Note: NDSU should contractually cover itself from an export compliance standpoint in those situations where it is hiring an external party to perform a particular service, for example, IT services or other infrastructure services. Presumably, also, all key vendors that fall into this category will have been screened against Visual Compliance prior to contract, to ensure that there is no export control exposure from that perspective.]

It is North Dakota State University’s policy to remain fully compliant at all times with all U.S. export control regulations, including but not limited to the Export Administration Regulations; International Traffic in Arms Regulations; and embargo sanctions under the Office of Foreign Assets Control (OFAC). Therefore, in the event that any party to this [Master Services Agreement/Contract] does not comply with said regulations during the term of this Agreement/contract, North Dakota State University will not be held responsible or liable for such non-compliance.

**MISCELLANEOUS**

The Parties acknowledge that the use and dissemination of the Technology and related information is restricted by United States Law, including 22 CFR 121.1 Category Xi(a)(3)(xvi). The Parties are both subject to United States laws and regulations controlling the export of technical data, computer software, prototypes, and other commodities (including the Arms Export Control Act, as amended and the Export Administration Act of 1979), and agree that their respective obligations hereunder are contingent on compliance with the applicable United States export laws and regulations. Each Party shall be responsible for its own use of Technology and the prototype, including any demonstration, and ensuring its compliance with all applicable laws. Company hereby warrants that neither it, nor any of its employees, are debarred or restricted in any manner from receipt and/or use of Technology and the prototype and that it accepts full responsibility for its compliance with all applicable laws and regulations. While the transfer of Technology, certain technical data and commodities may require a license from the cognizant agency of the United States Government, NDSU neither represents that a license is required nor that, if required, it shall be issued. This provision shall survive the expiration or any early termination of this Agreement.
Export Control International Shipment Review Form

Please prepare the following form and forward to the Export Control Office for review and approval prior to shipping.

Name: Click here to enter text.  
Department: Click here to enter text. 
Phone: Click here to enter text. 
Email: Click here to enter text. 

Date item to be shipped: Click to enter date. 

Shipping Company: Click here to enter text.  
Tracking number: Click here to enter text. 

1. Classification of Item(s), Technology and Software to be Shipped
   a. Describe the item(s) to be exported: Click here to enter text. 
   b. Is the item to be shipped a Biological Materials? ☐ Yes ☐ No 
      i. ☐ Human, ☐ Animal, ☐ Bacterial, ☐ Viral, ☐ Genetically Modified Organisms 
      ii. Is the item/material a biological agent or genetic element that involves an export controlled pathogen (See below for information on Export Control Classification Numbers 1C351, 1C352, 1C353, 1C354, 1C360, or Category XIV—Toxicological Agents, Biological Agents, and Associated Equipment)? ☐ Yes ☐ No 
      iii. Is the item/material a vaccine, immunotoxin, medical product or diagnostic and food testing kit (See below for information on Export Control Classification Number 1C991)? ☐ Yes ☐ No 
      iv. Is the item considered biological processing equipment (See below for information on Export Control Classification Number 2B352)? ☐ Yes ☐ No 
   c. Is the item(s), technology or software subject to the Export Administration Regulations (EAR)? ☐ Yes ☐ No 
      i. If yes, what is the Export Control Classification Number (ECCN)? Click here to enter text. 
      ii. What are the reasons for the control? Click here to enter text. 
   d. Is the item(s) or technical data subject to the International Traffic in Arms Regulations (ITAR)? ☐ Yes ☐ No 
      i. If yes, what is the ITAR category? Click here to enter text. 

For information regarding export control-listed pathogens, toxins and equipment and assistance with classifying the item/material visit http://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear, or http://www.ecfr.gov/cgi-bin/text-idx?SID=86008bdffjd1bf2e79cc5df41a180750a&node=22:1.0.1.13.58&rgn=div5, or contact the Export Control Office at ndsu.exportcontrols@ndsu.edu or 701-231-6455 

2. Shipping Destination Information 
   a. Country of destination/end-use: Click here to enter text.
b. Name(s) of recipient or recipient’s entity/corporation/business (known end-user/organization):  
   Click here to enter text.

c. National origin and/or citizenship of recipient (known end-user):  
   Click here to enter text.

3. Shipping Destination Controls
   a. Is an export license required based on the ECCN for the item/technology and its destination  
      (Country Chart)? □ Yes □ No
   b. Is a license exception available? □ Yes □ No
   c. Is the country of destination or the location of the end-user a country of concern because of embargoes  
      or sanctions? □ Yes □ No

4. Type/Reason for Export
   □ Temporary – will return within one year from date of shipment
   □ Repair and return
   □ Test and return
   □ Permanent
   □ Other  
   Click here to enter text.

   Exports may not be allowed to U.S. government sanctioned or embargoed countries or to an end-user in the  
   sanctioned or embargoed country.

5. Prohibited End-Use or End-User Review
   a. The export will be used for nuclear activity end use or by persons engaged in nuclear activities; missile  
      technology end-use; chemical or biological weapons end-use; or proliferation activities? □ Yes □ No
   b. The end-user is involved with terrorism or the financing or support of terrorism? □ Yes □ No
   c. Are Red Flag indicators are raised by the export transaction? □ Yes □ No
   d. A U.S. government agency instructed you not to transact business with this person/entity? □ Yes □ No
   e. Any party to the transaction asked you to participate in an international boycott (e.g., a request to refuse to  
      work with another person on the basis of race, religion, sex, or national origin)? □ Yes □ No

6. Restricted Party Screening – Contact the Export Control Office if assistance is needed with the screening.
   f. Has the proposed recipient been screened against the restricted party lists including: Denied Persons List;  
      Unverified List; Entity List; the Specially Designated Nationals List; Debarred List or the list of entities  
      subject to Nonproliferation Sanctions? □ Yes □ No
   g. If no, do not ship the item until screening has been completed.

7. Is the value of the item(s) being shipped more than $2,500? (Value is selling price or fair market value in U.S.  
   dollars) □ Yes □ No

8. Is there a MTA or other agreement in place with the recipient? □ Yes □ No

I certify that the information contained on this form is accurate and complete to the best of my knowledge and  
belief.

__________________________________________________________________________
   Signature                                                                 Date

Keep this document and all other export related documentation for five years from the date of shipment.

The ECA may be contacted by telephone at telephone at ndsu.exportcontrols@ndsu.edu or 701-231-6455.
Export Controls Brochure

- Educational Information - Information that is normally taught or released by the university as part of the normal instruction in a catalog course or in an associated teaching laboratory is considered Educational Information and, as provided for under the federal regulations (15 CFR §734.9), is NOT subject to export controls in most circumstances.

- Public Information Exclusion - Information that is already published or is out in the public domain is considered public information and, as provided for under the federal regulations (15 CFR §734.7 and 15 CFR §734.10), is NOT subject to export controls. Information presented at conferences, meetings, and seminars open to the public are not subject to export controls. Closed or Restricted conferences do not fall under the exclusion.

Examples of information in the public domain includes information included in published patents, websites freely accessible by the public, Books, newspapers, pamphlets, Publicly available technology and software.

8) Penalties for Violating Law and Regulations - Violations could result in substantial fines, seizure of items, revocation of import/export privileges, and imprisonment for willful (intentional) violations of the law. An individual and NDSU can be held liable for violations.

9) Export Controls Training - Training can be obtained through the Export Controls Office. You may also register for export control courses at https://www.citiprogram.org/. Other courses can be accessed at http://www.bisdac.gov/ and clicking on the compliance and training tab.

10) Export Controls Office - The Export Controls Office is here to help you with any export controls questions. You can get further information at NDSU Export Control Website.

Contact:
Export Controls Office:
Lynn Titus Jr., MCL, Export Control Office
701-231-6455, lynn.titus.jr@nds.edu

NDSU
1) Export controls are laws and regulations that govern the transfer of goods, technologies, services, data, and money to non-U.S. persons in the United States and abroad. Export controls are designed to protect the national security, economic interests, and foreign policy of the United States. Most exports fall under three categories:

A) International Traffic in Arms Regulations (ITAR) - State Department - Regulates Defense Articles, Technical Data, and Services

B) Export Administration Regulations (EAR) - Department of Commerce - Regulates equipment, materials, software, and technology with a "dual" civil/military use.

C) Office of Foreign Asset Controls (OFAC) - Department of Treasury - Regulates transactions with sanctioned countries and barred entities

2) Export Controls apply to everyone but the following disciplines or offices are more likely to trigger export controls:

A) Sciences, Technology, and Engineering

B) Sponsored or Non-Sponsored Research

C) Contracts, Agreements, and Purchasing

3) International Travel - An international travel request must be completed well in advance of international travel. The export control office will ask the following questions:

A) Where are you going?
B) What are you taking with you?
C) What will you be doing?
D) Who will you be interacting with?

Keep in mind that the export control office is required by the federal government to maintain records, conduct screenings, and may be required to obtain a license for the proposed travel.

4) Purchasing - If you want to purchase items from a foreign person or entity, you must notify the export control office in advance. The federal government requires the export control office to maintain records, conduct screenings, and the transaction may require a license. The following will determine the need for a license:

A) Item Classification
B) Location of the item
C) Info about Company Selling Item

5) Shipping - Prior to shipping or receiving anything internationally, the export control office must be notified. The federal government requires the export control office to maintain records, conduct screenings, and the transaction may require a license.

6) International Collaboration - Prior to collaborating with a foreign person or organization, the export controls office must be notified. The federal government requires the export controls office to maintain records, conduct screenings, and a license may be required.

7) Exclusions:

A) Fundamental Research - Fundamental Research is "any basic or applied research in science and engineering, the results of which are ordinarily published and shared broadly within the scientific community..." In order to qualify as Fundamental Research, the research must be conducted free of any publication restrictions or dissemination restrictions. The Fundamental Research Exclusion can be lost in certain circumstances.
https://www.ndsu.edu/research/integrity_compliance/export_controls/regulations/
Appendix 4: Legal Disclaimer

This NDSU “Export Controls Compliance Manual” attempts to provide relevant information about export controls and how they affect the academic and research enterprises at NDSU. It also outlines the Export Management and Compliance Program (EMCP) at NDSU. It does not claim to be a manual of university research administration, nor does it offer model policies. Export control laws are complex and fact-specific. Regulations, rules, and lists for specifying who or what is considered export-sensitive – and where export controls apply – are subject to change. The foregoing material is intended to provide a very brief outline of basic export control information. This Manual should not be taken as formal legal advice, and NDSU cannot – and does not – warrant the legal sufficiency of the information contained herein.

Appendix 5: Revision Record

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>By</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2014</td>
<td>Manual Drafted</td>
<td>By AnnaLisa Nash, Export Control Administrator (ECA)</td>
</tr>
<tr>
<td>December 2014</td>
<td>Final Manual Implementation</td>
<td>Approved by Vice President Dr. Kelly Rusch, RCA</td>
</tr>
<tr>
<td>May 2015</td>
<td>Updates</td>
<td>By AnnaLisa Nash, Export Control Administrator (ECA)</td>
</tr>
<tr>
<td>April 2017</td>
<td>Digital Manual Revision Updates</td>
<td>By Dr. Jolynne Tschetter and Lynn Titus Jr. (ECA)</td>
</tr>
</tbody>
</table>
SAMPLE LABELS

WARNING - ITAR CONTROLLED EQUIPMENT/MATERIALS IN USE OR IN STORAGE. ONLY AUTHORIZED PERSONNEL ALLOWED ENTRY OR ACCESS.

Violations of export laws are subject to severe civil and/or criminal penalties.

Contact Export Control at 701-231-6455
MARKING ITAR CABINETS/LOCKERS/ROOMS

The following statement, whenever possible, should be printed and placed on cabinets, safes, lockers, entry doors, etc.

The more visible the markings, the more likely the recipient of the information will be on notice that they have an obligation to treat the information as export controlled. The same should be done if ITAR controlled data is made available via a FTTP site or cloud based data room.

· WARNING - ITAR CONTROLLED EQUIPMENT/MATERIALS IN USE OR IN STORAGE. ONLY AUTHORIZED PERSONNEL ALLOWED ENTRY OR ACCESS.

Violations of export laws are subject to severe civil and/or criminal penalties.

Contact Export Control at 701-231-6455
MARKING AND SHIPPING LABELS

The following statement, whenever possible, should be printed on order confirmations, packing slips and/or commercial invoices accompanying the physical shipment, whether domestically or internationally:

For Domestic ITAR Product Shipments Only:

• **WARNING** - This shipment is subject to the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.), International Traffic in Arms Regulations, ITAR 22 C.F.R. 120-130. Violations of these export laws are subject to severe civil and/or criminal penalties. Dept. of State approval required prior to exporting.
DO MY PROPOSED RESEARCH ACTIVITIES QUALIFY AS FUNDAMENTAL RESEARCH?

Is the equipment, software, or technology involved in my research designed for, or can it be modified for military use or for use in outer space; or could it reasonably be used in the development of weapons of mass destruction?

YES

Does my research involve equipment, software or technology covered by ITAR (USML or EAR)?

YES

Does my research involve providing technical information or instructions concerning equipment, software or technology listed on the USML or CCL?

YES

Is my research basic or applied research in the areas of science and/or engineering at an accredited institution of higher learning in the U.S. and is the information resulting from that research ordinarily published and shared broadly within the scientific community?

YES

Does the results of my research contained source code for 64 bit encryption software; or mass market encryption products?

NO

Do my research activities involve exposure to foreign nationals within the U.S.; or transfers of goods, services, information or technology abroad; or travel outside of the U.S.?

YES

Is there reason to believe that information or software released by my research will be used in the development of a weapon of mass destruction?

YES

Are the results of my research published and generally accessible or available to the public through public venues, (i.e., conferences, libraries)?

NO

Fundamental Research Exclusion Applies!

NO

Export Control Regulations apply contact ECA.
ITAR/EAR Research Computing Encryption Procedures

Disable Network connections on Windows Computers:

1. Open Control Panel
2. Click Network and Internet
3. Click Network and Sharing Center
4. Click Change Adapter Settings
5. Right Click on Ethernet
6. Click Disable
7. Click OK
8. Right Click on any Wireless Adapters
9. Click Disable
10. Click OK
11. Close Network Connections Windows
12. Reboot

Setup VeraCrypt to encrypt files for transfer: can also be used to move files from computer to computer with portable drives. Works with Windows, Mac, and Linux Operating Systems, including Android and iOS.

1. Download and install VeraCrypt for your OS
2. Open Windows Explorer
3. Right Click and create a new text file where you would like to have the data stored
4. Name the file what you decide upon
5. Save and close the new text file (do not create any data in the text files as this will only be erased
6. Open the VeraCrypt application
7. Click Create Volume
8. Select Create an encrypted file container
9. Click Next
10. Select Standard VeraCrypt volume
11. Click Next
12. Click Select File
13. Browse to the location you saved your txt document
14. Select your txt document
15. Click Save
16. Click Yes, to replace your document
17. Make sure Never save history is checked
18. Click Next
19. Keep the defaults for encryption options
20. Click Next
21. Enter the size that you want to volume to be:
   a. Keep in mind whatever storage size you choose, your txt document will then become that size, also, the larger the size the longer it will take to encrypt and decrypt as well as transfer
22. Click Next
23. Enter and Confirm your password
a. Do not lose this password, there is no way to recover the data if the password is lost
24. Move the mouse cursor around in the VeraCrypt window to introduce randomness into the encryption algorithm. Once the bar is solid green click Format, this will format the volume in the file system indicated
25. You now have a file that is encrypted

Use VeraCrypt to transfer files: all parties that need to use the files encrypted need to use VeraCrypt to view or use those files

--- Put files on VeraCrypt encrypted volumes:

1. Open VeraCrypt
2. Click Select File
3. Browse to and select your txt file created earlier
4. Click Open
5. Select a Drive letter Q
6. Click Mount
7. Enter your password
8. Open Windows Explorer
9. Move files that you wish to transfer to your Q drive
10. When Finished - In VeraCrypt click Dismount all
11. The Q drive will be removed and the file will then be encrypted
   a. You can test this by opening the txt file with a file editor
12. Exit VeraCrypt

--- Receive files on VeraCrypt encrypted volumes:

1. Open VeraCrypt
2. Click Select File
3. Browse to and select the txt file received
4. Click Open
5. Select a Drive letter Q
6. Click Mount
7. Enter the password
8. Open Windows Explorer
9. Move files that you wish to transfer off the Q drive
10. When Finished - In VeraCrypt click Dismount all
11. The Q drive will be removed and the file will then be encrypted
   a. You can test this by opening the txt file with a file editor
12. Exit VeraCrypt

Transfer Files to External Organizations:

1. Speak with External Organizations to Establish the protocol that will be used to transfer files
2. Establish the password that will be used on the phone or some other way that does NOT include email
3. Move (DO NOT COPY) encrypted files from a non-networked computer to a computer with a network connection
4. Go to https://filetransfer.ndsu.nodak.edu
5. Login with your NDSU credentials
6. Enter the email address of the individual (or Organization) that you will be sharing the file with
7. Uncheck the Require authentication to access/download
8. Select a date that the file will be deleted off the server (default is three days)
9. Enter the number of downloads the file can be downloaded (default is unlimited)
10. Drag and drop the txt file
   a. Alternatively, click on Add files
   b. Browse to the file
   c. Select the file
   d. Click Open
11. Check the Auto-send when current uploads are complete
12. The file will be uploaded to the NDSU File Transfer server
13. The External organization as well as you will receive an email that indicates that the file is awaiting pickup

Possible Cleanup Tools:

- Use eraser to securely delete files from your computer https://eraser.heidi.ie/