West Virginia University

Export Control

Compliance Manual

January 2015
LETTER FROM E. GORDON GEE, PRESIDENT ................................................................. 1

I. OVERVIEW OF EXPORT CONTROL COMPLIANCE .............................................. 1
   A. MISSION STATEMENT OF THE WVU EXPORT CONTROL OFFICE ............... 1
   B. POLICY STATEMENT ..................................................................................... 1
   C. SCOPE OF EXPORT CONTROL COMPLIANCE PROGRAM ......................... 1
   D. PURPOSE BEHIND UNITED STATES EXPORT CONTROL LAWS .................. 2
   E. SCOPE OF U.S. EXPORT CONTROL LAWS ................................................... 2
      “Export” ..................................................................................................... 2
      “Deemed Export” ....................................................................................... 3
      “U.S. Person” ............................................................................................. 3
      EMBARGOED AND SANCTIONED COUNTRIES ......................................... 3
      DENIED PARTIES .................................................................................... 3
      ANTI-BOYCOTT LAWS ............................................................................. 3
      ANTI-CORRUPTION LAWS ..................................................................... 3
   F. EXPORT CONTROL COMPLIANCE PROGRAM KEY PERSONNEL ............... 4
   G. AGENCIES THAT CONTROL U.S. EXPORTS ............................................... 4
      1. DEPARTMENT OF STATE – DIRECTORATE OF DEFENSE TRADE CONTROLS (DDTC) .... 4
      2. DEPARTMENT OF COMMERCE – BUREAU OF INDUSTRY AND SECURITY (BIS) .... 4
      3. DEPARTMENT OF THE TREASURY – OFFICE OF FOREIGN ASSETS CONTROL (OFAC) .... 5
      4. OTHER AGENCIES ............................................................................... 5
   H. IMPORTANCE OF COMPLIANCE – POTENTIAL COST OF VIOLATIONS .......... 5
   I. INDIVIDUAL RESPONSIBILITY OF WVU PERSONNEL ............................... 5

II. APPLICABILITY OF EXPORT CONTROLS .............................................................. 6
   A. IDENTIFYING EXPORT CONTROL ISSUES ................................................. 6
   B. EXPORT CONTROL INDICATORS ................................................................ 6
   C. EXAMPLES OF CLAUSES OF CONCERN ................................................. 7
   D. BE ALERT FOR “RED FLAGS” ................................................................... 7
   E. RESTRICTED PARTIES SCREENING ............................................................ 8

III. HANDLING A SUSPECTED VIOLATION OR PROBLEM ...................................... 9
    SUSPECTED VIOLATION PROTOCOL ............................................................ 9

IV. RECORDKEEPING ............................................................................................. 10
    DOCUMENTING COMPLIANCE STEPS AND EXPORT DECISIONS .................. 10

V. TRAINING AND ACCOUNTABILITY .................................................................... 10
   A. GENERAL .................................................................................................. 10
B. Initial Training ................................................................. 10
C. Annual Basic Refresher Training and Program Update .......... 11
D. Targeted Training for Certain WVU Personnel ..................... 11
  Training for WVU Personnel on Export-Controlled Projects .......... 11
  Detailed Training for New WVU Personnel with Export Responsibilities .......... 11
  Refresher Training for All WVU Personnel with Export Responsibilities .......... 11
  Technology Control Plan Training ........................................ 11
E. Notification of Changes in Export Control Laws and Regulations .... 11
F. Audits ............................................................................. 12
  Internal Compliance Audits .............................................. 12
  External Compliance Audits .............................................. 12
G. Duty to Report .................................................................. 12
H. Supporting Product Classification/Commodity Jurisdiction Requests .. 12

VI. Procedures under the Policy .................................................. 12
A. Hiring of Non-Immigrant Workers: Visa Applications .............. 13
B. International Travel ........................................................... 14
C. Export Control Screening of Externally Funded Research Grants and Contracts .......... 16
D. International Visitors to the University Campus ...................... 16
E. Legal Agreements and Business Transactions with Foreign Parties .......... 17
F. Purchasing or Receiving Export Controlled Items .................... 17
G. Property Management ...................................................... 18
H. Shipping and Marking Procedures ....................................... 18
I. Marking Procedures for Electronic Communications ................. 18

VII. WVU Organizational Chart .................................................. 18

VIII. Summary of Responsibilities ............................................... 18

IX. Glossary of Terms ............................................................. 20

X. Forms and Additional Information ......................................... 23

Appendix 1 ........................................................................... 25
A. Anti-Boycott Protections .................................................... 25
  Avoiding and Reporting Illegal Boycotts .................................. 25
  Negative and Positive Obligations ........................................ 25
B. Anti-Bribery Protections ..................................................... 26
  Prohibited Payments ........................................................ 26
  Limited Exceptions for Common Business Practices and Payments .......... 26
THIRD PARTY PAYMENTS CAN CREATE LIABILITY .............................................................26
HIGH RISK PROJECTS ................................................................................................27

APPENDIX B ..................................................................................................................28
A. WVU EXPORT CONTROL FORM FOR INTERNATIONAL TRAVEL ......................28
B. EXPORT ADMINISTRATION REGULATIONS TMP EXCLUSION .........................29
C. BEST PRACTICES .......................................................................................................31
D. WVU DEEMED EXPORT VERIFICATION FOR NON-IMMIGRANT VISAS ..............34
E. ELECTRONIC DEVICES LOST/STOLEN ON INTERNATIONAL TRAVEL ..........38
Dear Faculty, Staff, and Students,

As West Virginia University continues to ascend the ranks of respected research and academic institutions, our endeavors have become more complex and globalized. Global engagement and innovative, boundary-testing research are crucial to the University’s continued growth, and with these undertakings come important legal obligations. The federal government has enacted export control laws that protect U.S. national security interests. These laws and regulations help ensure that whenever certain information or items are shared outside the U.S. or with foreign nationals in the U.S., the United States and its citizens remain safe at home and abroad.

A critical component of West Virginia University’s mission is supporting fundamental research, as well as developing relationships and participating in the worldwide academic community to further the pursuit of knowledge. As a public institution of higher education, West Virginia University has many international scholars, employs many foreign nationals, collaborates with international partners on research, education and services, and hosts foreign visitors in connection with international exchange programs, international students, and other business and collaboration agreements. These are all important. West Virginia University intends to welcome its international scholars, collaborate with foreign nationals, and host international visitors, both long and short term, in the most open and inviting manner possible while also ensuring compliance with U.S. laws and regulations governing the export of certain items and information.

West Virginia University’s policies and procedures for export control compliance are defined in this Manual, which is intended as a guide to facilitate compliance with U.S. export control laws and regulations. I also encourage you to review the more condensed export control procedures available on the West Virginia University Export Control Office’s web site: http://oric.research.wvu.edu/export_control, which cover some of the most frequently encountered issues on campus in a quick-reference manner. Finally, the University’s Export Control Office is a very helpful resource and I encourage you to contact them with all questions or concerns related to these issues.

Cordially,

E. Gordon Gee
I. Overview of Export Control Compliance

A. Mission Statement of the WVU Export Control Office

The Export Control Office of West Virginia University (“ECO”) will work to ensure that all West Virginia University (“WVU” or “the University”) activities comply with applicable federal export control laws and regulations, to maintain and continuously improve the WVU Export Control Compliance Program to enable the University to effectively comply with federal export control laws and regulations as such laws and regulations evolve, and to effectively communicate to the WVU community the importance of compliance with federal export control laws and regulations and associated responsibilities.

B. Policy Statement

As part of its mission to maintain excellence in higher education and research, WVU must be dedicated to compliance with U.S. export laws. For that reason, WVU has adopted a policy that makes export control compliance an integral part of our collective undertaking:

*It is the policy of West Virginia University that all personnel—faculty, staff, employees, visiting scholars, postdoctoral fellows, graduate and undergraduate students, volunteers, and all other persons retained by or working at the University—will fully comply with all U.S. laws and regulations while teaching, conducting research, or providing service activities at or on behalf of the University, wherever located. Therefore, all personnel are required to fully comply with the U.S. export control laws and regulations that govern the transfer of information, technology, hardware, software, and funds to institutions, commercial entities, and persons outside of the U.S., as well as to non-U.S. Persons within the U.S.*

C. Scope of Export Control Compliance Program

This Export Control Compliance Manual governs and applies to the activities of all personnel—faculty, staff, employees, visiting scholars, postdoctoral fellows, graduate and undergraduate students, volunteers, and all other persons retained by or working at the University, wherever located (collectively referred to as “WVU Personnel”). The sorts of activities that may involve export control issues include, but are not limited to, the following:

- Performing or planning to perform research involving export controlled subject matter or equipment.
- Hiring or planning the hiring of foreign nationals.
- Traveling internationally for University-related business or traveling, for any reason, to an embargoed country with University-owned equipment (e.g., laptop computers, smart phones, tablets) or having access to University e-mail, computer networks, or files while abroad.
- Shipping technology, equipment, samples, or software outside of the U.S.
- Exporting or receiving export controlled technology, equipment, or software from another party.
• Participating in research in which the sponsor restricts publication or the participation of foreign nationals.
• Inviting or hosting visitors to the University who are foreign nationals not already residing in the U.S.
• Engaging in business activity or legal agreements with foreign entities.
• Purchasing items from entities in foreign countries.

Please contact the ECO directly with any questions or concerns.

D. Purpose Behind United States Export Control Laws

Since the 1940s, the U.S. has used export control laws and regulations to govern the export of information, commodities, technology, and software deemed strategically important to the U.S. for reasons of national security, foreign policy, or the protection of the economy and commerce. These laws protect U.S. national security, support U.S. foreign policy, control proliferation, and work to prevent terrorist activities. They also seek to avoid increasing the military capabilities of certain individuals, groups, and foreign countries by controlling defense articles and services and items that can be used for defense purposes to ensure the safety of our armed forces in conflict.

While institutions of higher learning generally do not manufacture goods and provide services intended to be exported, institutions like WVU do work extensively with technical data, advanced instrumentation and equipment, software, and various subject matter and materials subject to export control restrictions. Although there are certain export control exceptions that apply to institutions of higher learning, universities must strictly comply with these complex laws and regulations or face severe civil and criminal penalties.

E. Scope of U.S. Export Control Laws

U.S. export control laws regulate the export of commodities, technical data, services, and information to foreign persons, entities, and countries. These laws also enforce embargoes and prohibit participation in unapproved boycotts and bribery of foreign officials. Several key definitions and concepts are integral to understanding the scope of these laws.

“Export”

U.S. export control laws broadly define the term “export.” Due to the broad definition, the scope of these laws is not always intuitive. Any item that is transferred from a U.S. Person to a foreign person is an export. These laws apply to U.S. Person and entities while they are in the territorial boundaries of the U.S. and also in foreign countries. Items in this context can be physical items, software, technology, or technical information. Certain items with potential military uses, such as software and encryption codes, are strictly controlled. Items can be transferred or exported by a wide variety of methods, including by mail, physical shipment, fax, uploading/downloading via the web, e-mail, phone or face-to-face conversation, or visual observation.
“Deemed Export”

According to the U.S. government, any export controlled knowledge or information transferred to a non-U.S. Person in the United States is deemed to be an export to the person’s country of citizenship. This is especially important in a university given the open dissemination of knowledge and number of non-U.S. Persons employed and studying on campus.

“U.S Person”

A U.S. Person is a (1) U.S. Citizen, including U.S. companies and entities like WVU; (2) U.S. Permanent Resident Alien; or (3) Political Refugee protected under the Immigration and Naturalization Act. An non-U.S. Person is any person or entity that does not fall under one of the three categories listed above.

Embargoed and Sanctioned Countries

Export laws also support embargoes against certain embargoed or sanctioned countries. U.S. embargos may prohibit travel to, contact with, or business transactions with parties in specified countries or they may strictly limit travel to the country, as is the case with Cuba, Iran, Syria, Sudan, and North Korea. Many of these economic and trade sanctions support United Nations or other international mandates. In addition to these sanctions, U.S. Persons cannot do business with certain foreign nationals suspected of terrorism or who have ties to terrorist organizations.

Denied Parties

The U.S. government maintains several lists of denied persons, entities, and organizations. The export control restrictions on these parties vary depending on the potential of an export control violation resulting from doing business with the party. Finding a potential collaborator or business partner on one of the denied parties lists does not necessarily mean a transaction cannot proceed, although it is a “red flag” and does indicate a transaction carries greater risk of violation and may require a license from the federal government.

Anti-Boycott Laws

U.S. laws prohibit U.S. Persons from participating in boycotts of countries friendly to the United States. These laws prohibit U.S. Persons from participating in illegal boycotts and require U.S. Persons to report any invitation to participate in an illegal boycott.

Anti-Corruption Laws

In addition to anti-boycott controls, U.S. law forbids U.S. Persons from offering or giving a payment or thing of value to a foreign government official with the intent to improperly influence that individual.
Please see the additional information in Appendix 1 for detailed information about Anti-Boycott and Anti-Bribery laws and compliance.

F. Export Control Compliance Program Key Personnel

West Virginia University established the Export Control Office (“ECO”) to help WVU Personnel understand and comply with export control laws. The ECO currently consists of an Export Control Officer and an Export Control Analyst. The Export Control Officer, who is responsible for overseeing all activities of the office, reports to the Assistant Vice President for Research Administration and serves as the “Empowered Official” for export control compliance for WVU. The Export Control Analyst serves as the main point of contact for the office; maintains the WVU Export Control Web site, databases, and forms; provides training; and performs the screening for activities involving foreign persons and entities.

Detailed contact information for the Export Control Office can be found on the ECO Web site.

G. Agencies that Control U.S. Exports

The three main government agencies that administer and enforce U.S. export law are the Department of State, the Department of Commerce, and the Department of the Treasury. Additional agencies are responsible for very specific subsets of export control regulations.

1. Department of State – Directorate of Defense Trade Controls (DDTC)

The DDTC at the State Department controls “defense articles” and “defense services” pursuant to the Arms Export Control Act (AECA).\(^1\) The International Traffic in Arms Regulation (ITAR)\(^2\) implements the AECA. In general, the DDTC regulates items and services designed, modified, or adapted for military application. Because of the inherent military value of these items, they are strictly controlled.

2. Department of Commerce – Bureau of Industry and Security (BIS)

The BIS controls “dual use” items—those that have both commercial and military or proliferation applications—under the Export Administration Act (EAA),\(^3\) the International Emergency Economic Powers Act (IEEPA),\(^4\) and the Export Administration Regulations (EAR).\(^5\) Since the EAA lapsed in 2001, the EAR has been continued by Executive Order\(^6\) under the IEEPA granted power. Because many controlled items are mainly commercial in nature and do not have obvious military uses, the precise level of control depends on the specific item.

---

3. Department of the Treasury – Office of Foreign Assets Control (OFAC)

The OFAC 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, or economic interests of the United States. The OFAC acts under the IEEPA, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under U.S. jurisdiction.

4. Other Agencies

Various other agencies administer limited controls on the export of certain types of items and technologies, such as: (i) Department of Justice (anti-corruption laws); (ii) Nuclear Regulatory Commission (nuclear equipment and materials); (iii) Department of Energy (nuclear technology and high-energy lasers); and (iv) Food and Drug Administration (pharmaceutical development and medical devices).

A good rule of thumb when thinking about the primary agencies that may be involved is that the Department of State controls items and services that are inherently military, the Department of Commerce regulates dual-use items, and the Department of the Treasury focuses on financial transactions and sanctions.

H. Importance of Compliance – Potential Cost of Violations

Violations of U.S. export laws carry substantial penalties for individuals and institutions who violate them—including severe fines and prison time. Export control law violations carry strict liability, meaning it is not necessary to act with knowledge or intent to violate the law. However, acting with knowledge and intent can lead to criminal penalties under the EAR, which can reach one million dollars and twenty years imprisonment per violation. Likewise, violations of the ITAR and statutes enforced by the OFAC may result in penalties of up to one million dollars and twenty years imprisonment per violation. Civil penalties, which may be imposed on top of other liability or penalties, can range from $250,000 or twice the value of the export or transaction, whichever is greater (EAR and OFAC), to $500,000 (ITAR).

In addition, individuals, entities, and universities may be subject to administrative penalties including denial of export privileges and forfeiture of the offending article(s) and proceeds. Universities that violate export control laws and regulations are at risk of losing federal research funding as well as damaging the university’s reputation, resulting in loss of future funding opportunities.

I. Individual Responsibility of WVU Personnel

It is the personal responsibility of all WVU Personnel to be aware of and comply with all export control laws and regulations, as well as related WVU policies and procedures. As noted above, while the institution can be severely penalized for violations, export control laws and regulations provide that the person(s) responsible for violating the law may be held individually responsible
and may suffer civil and even criminal penalties in certain instances. If WVU Personnel believe they are or may become involved in any activity to which export control restrictions could possibly apply, they should immediately contact the ECO for assistance.

II. Applicability of Export Controls

A. Identifying Export Control Issues

Since not all of WVU’s various activities are subject to export controls and not every research project involves export controlled technology, it is important for WVU Personnel to ensure they are aware of what activities and projects are export controlled and what specific export control procedures and requirements apply. To assist in that effort, the ECO will notify the relevant WVU Personnel of any activities and projects determined to be subject to export controls and identify the requisite action for each. All WVU Personnel must always be on the lookout for signs that the project, activity, technology, or item they are involved with may be subject to export control laws and regulations. As explained in more detail below, WVU Personnel have an important role to play in identifying and properly addressing export control issues.

Some examples of potential transactions covered by U.S. export control laws and regulations are

- Disclosing information or sending export controlled items to an individual or institution outside the United States or to a non-U.S. Person in the United States.
- Sharing export controlled technical data or technology with a non-U.S. Person (e.g., a collaborator or co-worker) in person, by phone, live-Web support, e-mail, or at a conference, whether in the United States or abroad.
- Publishing technical data, such as research results, specifications, or drawings, on a Web site, even if the site is hosted in the United States.
- International travel related to university business.
- Hiring non-U.S. Persons.
- Hosting non-U.S. visitors on campus.
- Doing business with individuals or entities in embargoed countries or on a federal restricted party list.

B. Export Control Indicators

The following are some indicators that a project, item, or technology may be subject to export controls:

- Bans or restrictions on publication or public disclosure of research results (i.e., restrictive clauses in contracts and requests for proposals (“RFP”)).
- Indications or statements that controlled technology and information will be supplied by the sponsor (i.e., references to export regulations in contracts or RFPs and request specifics from sponsor).
- Encryption source code or object code will be exported.
- Results of research could be used for military purposes, including development of weapons of mass destruction.
• Restrictions in contracts or RFPs on non-U.S. Persons participation.
• Shipping items outside the United States.
• Sponsor is a foreign entity.
• Transaction involves an embargoed or sanctioned country.

C. Examples of Clauses of Concern

Contracts should be reviewed carefully to identify any restrictions on publications, references to export regulations, and involvement of foreign nationals. Samples of clauses that should raise concerns are listed below. Note that this list is not all-inclusive.

DFARS 252.204-7000 – Disclosure of Information. Prevents the release of any data without sponsor approval. Clause is included in boilerplate for most of DOD and continues to be the problematic for universities. Especially problematic to have removed when it is included in subcontract from industry.

FAR 52.227-14 – Rights in Data – General. Government has unlimited rights in data first produced or delivered under the contract. Contractor has the right to assert copyright in data first produced in the performance of the contract with prior Government approval.

FAR 52.227-17 – Rights in Data – Special Works. Prevents the release, distribution and publication of any data first produced in the performance of the award.

ARL 52.004-4400 – Approval of Foreign Nationals Performing under Contract required.

Army Corps. of Engineers 52.0000-4017 – Approval of Foreign Nationals Performing under Contract required.

AFMC 5352.227-9000 – Export Controlled Data Restrictions. Requires export control license before foreign nationals can work on research program.

D. Be Alert for “Red Flags”

Often, avoiding violations is as simple as being alert to “red flags” that may signal that a project or activity presents a risk of a violation. The best and safest approach to compliance is to stay vigilant for common signals that may indicate that an individual is trying to obtain U.S. export controlled material or information unlawfully. Under the law, each person has an affirmative duty to know certain information related to our transactions. Ignoring the export control laws or avoiding “bad” information undercuts our ability to comply and increases the likelihood of a violation and the severity of the consequences. As previously mentioned, export control laws carry with them strict liability, so ignorance of the laws is not an excuse and will not mitigate penalties from the federal government.

It is important to recognize potential red flags to prevent a violation of export control laws. If there is a red flag or any doubts regarding the legality of the transaction, do not continue the transaction. Stop all actions related to the transaction and contact the ECO immediately.
Some red flags that WVU Personnel or the ECO may encounter are listed below:

- The name or address of the individual, business, or institution in question is similar to a name that comes up on a screening list. Note that individuals may go by several names or share addresses.
- A person is reluctant to offer information about the end-use of an item. For example, when asked about a product’s end-use or upon informing the person that WVU requires a certification of end use, they hesitate or do not call back for several days.
- The items, technical data, or know-how being sought from WVU do not fit the other person’s line of business or stated mission, such as an agricultural institution inquiring about WVU expertise in satellites.
- The items, technical data, or know-how being sought from WVU are incompatible with the technical level of the country it will be shipped to, such as a person interested in working on sophisticated manufacturing technology who lives in a country without a robust manufacturing sector.
- The person, business, or institution in question has little or no background involving the items, technologies, or capabilities they seek to acquire from WVU.
- The person, business, or institution in question is unfamiliar with the basic functionality or uses of the items, technologies, or capabilities they seek to acquire from WVU.
- The person, business, or institution in question is vague about delivery dates or wants deliveries made to odd destinations, such as Post Office boxes, remote locations, or destinations that are far away from their place of business.
- The person, business, or institution in question gives a freight forwarder as the product's final destination.
- The shipping route is abnormal, such as a transaction with a reported final destination in France routing the delivery through India.
- The person, business, or institution in question requests unusual packaging, such as asking for an unmarked box or providing their own packaging materials.
- The person, business, or institution in question is evasive or makes contradictory statements about a project’s intended collaborators, such as stating that it will involve researchers at a business in Colorado but making frequent references to their engineering facility in China.

E. Restricted Parties Screening

Various government agencies maintain lists of prohibited and sensitive end-users. Licenses generally are required to ship any items to these end-users or to carry out a transaction in which a prohibited or sensitive end-user is involved in any way.

In order to ensure that WVU is not doing business with people or companies who have been debarred, denied export privileges, or are otherwise on one of the numerous government “prohibited lists,” WVU Personnel must work with the Export Control Office to screen participants who will be involved with export-controlled projects or export transactions.

The ECO has licensed software that searches all government lists simultaneously. Using that software, the ECO screens parties involved in an export transaction against the lists of restricted
persons and entities to ensure that the export is not prohibited. These publically available lists include the following:

- The BIS Entity List of entities involved in proliferation activities.
- The BIS Unverified List of entities that may be involved in improper diversion of items to illegal end-uses or end-users.
- The BIS Denied Persons List.
- The DDTC’s List of Debarred Parties.
- The State Department’s lists of countries subject to Nonproliferation Sanctions.
- The OFAC’s list of sanctioned or embargoed countries.
- The OFAC’s List of Specially Designated Nationals and Blocked Persons.
- Any other list of prohibited parties or sensitive destinations generated by WVU (e.g., parties or entities which WVU has had concerns in the past—a “grey” list).

If any of the screenings return a match on one of the applicable lists, the transaction will be placed on hold. The ECO will then determine whether and under what conditions the transaction may proceed and, if the transaction can proceed, obtain all necessary authorizations and provide any applicable instructions. It may be necessary to apply for a license from the government, depending on the parties and technology involved. This can take up to ninety days.

III. Handling a Suspected Violation or Problem

If there is any reason to believe that a violation or possible violation of U.S. export control laws or regulations has occurred, or is about to occur, immediately contact the ECO. It is extremely important that any concern be brought to the immediate attention of the ECO, so that the problem can be properly addressed.

Suspected Violation Protocol

1. Contact the ECO.

2. Stop the transaction immediately. If the transaction involves a shipment of goods, stop the shipment. If the transaction involves communication with a foreign person, terminate the communication.

3. With the help of the ECO, document the suspected violation and retain all relevant records. Such documentation and records can help mitigate the potential consequences and help WVU determine the steps of the transaction that led to the suspected violation so they may be properly addressed.

4. Maintain confidentiality. After properly reporting the incident to the ECO, keep the matter confidential by not sharing it with others. This will allow WVU to accurately assess the situation.
IV. Recordkeeping

Documenting Compliance Steps and Export Decisions

A well-documented export control procedure is an integral part of complying with export laws and mitigating any possible consequence of a violation. For this reason, the ECO shall retain all records relevant to export transactions for a period of five years. All WVU Personnel shall provide all relevant records to the ECO for retention. Following these procedures is an important part of the compliance process and allows the ECO to document export transactions.

Under U.S. export laws, records must be kept for a minimum of five years from the date of export, re-export, transfer, or expiration of certain export authorization (e.g., license or technical assistance agreement (“TAA”)). The documentation that must be maintained regarding the export of products, technical data, or services by WVU Personnel includes the following:

- Memoranda, notes (e.g., meeting presentations and notes), correspondence (e.g., e-mails and letters), contracts, invitations to bid, acquisition or repair documents and reports, and other records pertaining to imports and exports.
- Technical data transactions (e.g., e-mails, facsimiles, phone conversations).
- Transcripts of any defense service provided (e.g., basic information, operation and maintenance training, and any engineering or repair services).

While the ECO is responsible for the retention of export records, it is the responsibility of WVU Personnel to forward all relevant export documentation to the ECO for archiving, including:

- Import and export licenses, applications, and shipment placed against each license.
- License provisos and records showing that the provisos were briefed to WVU Personnel with association to the license.
- Records of all Technical Assistance Agreements.
- Records regarding the use of EAR or ITAR exemptions, including a description of the technical data exported under an exemption, the name of the recipient end-user, the date and time of the export, and the method of transmission.

V. Training and Accountability

A. General

The ECO shall be responsible for designing and implementing the export control training program for WVU Personnel. All WVU Personnel shall be responsible for attending training and reporting suspected violations.

B. Initial Training

Upon the implementation of this program, WVU Personnel shall undergo training designed to assure they understand and are following the steps necessary for compliance. All new hires shall be trained in accordance with their work assignment.
C. Annual Basic Refresher Training and Program Update

Refresher training will be conducted annually for WVU Personnel. In addition, the Export Control Compliance Manual shall be reviewed by the ECO on an annual basis and updated as necessary.

D. Targeted Training for Certain WVU Personnel

In addition to the initial and annual refresher training, certain WVU Personnel may receive targeted training designed to address export control issues that they may be more likely to encounter on a regular basis given the position and the nature of work.

Training for WVU Personnel on Export-Controlled Projects

Before beginning work on an ITAR-controlled project or an EAR-controlled project which requires export licenses, WVU Personnel shall receive export control training, with an emphasis on the particular export control issues associated with the project, tailored to their role on the project.

Detailed Training for New WVU Personnel with Export Responsibilities

New WVU Personnel with export transaction responsibilities shall receive detailed training regarding their responsibilities for export control compliance. The WVU Personnel shall be identified by the ECO.

Refresher Training for All WVU Personnel with Export Responsibilities

The ECO shall annually provide refresher training to all WVU Personnel with responsibility for export transactions. Such training may be provided by in-house or external consultants.

Technology Control Plan Training

All export-controlled projects must have a Technology Control Plan (“TCP”) in place that describes the specific procedures and controls that will be implemented on that project to ensure export control compliance. The Principal Investigator shall work with the ECO to ensure all involved WVU Personnel have been trained on the plan and understand the restrictions. All involved WVU Personnel shall sign a statement that they have received export control training and that they understand and shall abide by the technology control plan.

E. Notification of Changes in Export Control Laws and Regulations

Between trainings, the ECO shall notify WVU Personnel of relevant changes to export control laws and regulations by posting updates to the ECO Web site. Export control laws and regulations are continuously evolving as a result of export control reform and new technology development. WVU Personnel should contact the ECO with any questions and frequently visit the Web site for information.
F. Audits

WVU’s compliance with U.S. export control laws and regulations and this manual is subject to periodic audits. All WVU Personnel are required to cooperate fully with these audits. Both internal and external compliance audits may be used.

Internal Compliance Audits

The ECO will design and perform an internal audit of WVU’s compliance with these procedures and U.S. export control laws no less than annually.

External Compliance Audits

At the discretion of the Empowered Official, WVU’s compliance with this policy and U.S. export control laws may be audited by an outside law, consulting, or other firm. The results of this audit will be reported to the WVU Vice President for Research.

G. Duty to Report

The duty to report questions, problems, concerns, and suspected violations as described in the suspected violations section is an ongoing requirement for all WVU Personnel. As outlined above, WVU Personnel must report export-related issues to the ECO.

If any WVU Personnel are contacted by an outside party regarding WVU’s export control policies or procedures, do not respond to the inquiry. Please contact the ECO, who will respond.

H. Supporting Product Classification/Commodity Jurisdiction Requests

From time to time, WVU Personnel may be asked to provide the ECO with information that will assist with a Commodity Jurisdiction Request or the Classification/Licensing of relevant items or technical data. Part of making an accurate request for a license or a Commodity Jurisdiction Request involves understanding the nature of the technical data, software, or identity of the final item in which the technical data, software, or services will be used.

The information that must be provided in connection with a Product Classification or Commodity Jurisdiction Request includes

- Description of the article or service;
- History of the item’s design, development, and use; and
- Documents related to the item.

VI. Procedures under the Policy

In general, when planning to engage in activities which have the potential to involve an aspect of export control, WVU Personnel need to contact the ECO well in advance of the planned activity to confirm the applicable procedures and any steps necessary to ensure compliance.
The specific procedures required to comply with export control laws and regulations will differ depending on the type of activity or nature of the item or technology in question, and the applicable export controls requirements. In some cases, the ECO will need to work with the relevant WVU Personnel to determine special procedures based on the particular facts and circumstances.

Below are some of the common activities for which WVU has established standard procedures.

A. Hiring of Non-Immigrant Workers: Visa Applications

As part of the process for hiring non-immigrant workers, the ECO screens H-1B, J-1, and O-1 visa applicants in connection with the completion of U.S. Citizenship and Immigration Services Form I-129. At the present time, WVU does not regularly screen international students as part of the visa application process. Before a WVU unit can hire a non-immigrant worker under any of the above-listed visas, the following shall be provided on the WVU Deemed Export Verification for Non-Immigrant Visas Form:

- Full legal name;
- Citizenship;
- Place of birth;
- Supervisor at WVU;
- Projects and/or equipment assigned, if known;
- Dates of employment at WVU;
- Copy of a valid passport; and
- Current curriculum vita.

The export control screening will include a “restricted parties screening” of the applicant; the foreign affiliation of the applicant; and the country of citizenship of the applicant, as well as a technical screening of the project or equipment, if any, to be assigned to the applicant if hired. “Restricted parties screening” involves comparing the information provided by the applicant to various publically available lists of individuals, entities, and organizations that have been identified by the U.S. Government as posing export control risks. Screening results that include a match to a restricted party or a country deemed to pose a higher risk (i.e., embargoed or sanctioned) will require further analysis by the ECO.

The completed and signed Deemed Export Verification must be submitted to the ECO in a timely manner as part of the non-immigrant worker’s visa application or renewal. Any questions related to the timing and submission of these forms should be directed to the ECO: exportcontrol@mail.wvu.edu or 304-293-3084. If the hiring unit has any reason to believe that export controlled material may be involved in the projects or equipment to be assigned to the applicant if hired, the hiring unit must submit the completed forms to the ECO at least three months in advance in case a federal license will be needed to complete the hiring process.
B. International Travel

An export control screening is required for WVU Personnel on international travel related to WVU business. The nature of the screening depends on the specific details of the intended travel: the location(s) to be visited, the purpose of the trip, and what the travelers will be taking with them.

Travel to certain countries (e.g., Iran, Cuba, North Korea, Sudan, and Syria) involves greater risk of export control violations because of more restrictive regulations. This includes personal travel to an embargoed or sanctioned country by WVU Personnel who intend to take WVU equipment or who will be accessing WVU-related computer networks, including e-mail, while in an embargoed or sanctioned country.

Follow the Travel Screening Decision Tree on the next page to determine whether to complete the International Travel Screening Form. All international travel for WVU business or with WVU-owned equipment requires a current copy of the Best Practices form on file with the ECO.

If the Travel Screening Decision Tree indicates that the international travel form is necessary, the WVU Personnel must submit the travel forms no later than two weeks prior to departure. The ECO cannot guarantee screenings for travel forms submitted later than two weeks prior to departure. If WVU Personnel are traveling to an embargoed or sanctioned country or if the travel may involve export controlled subject matter or equipment, contact the ECO at least three months in advance of travel in case a license is required.

All WVU Personnel accessing WVU e-mail when traveling abroad must comply with the current version of Best Practices to Maintain Security of Controlled Technology or Technical Data During International Travel. All WVU Personnel will be asked to submit once per fiscal year to the ECO a signed “Best Practices to Maintain Security of Controlled Technology or Technical Data During International Travel” document affirming that the traveler has read and understood the content.
International Travel Screening Decision Tree

Is the purpose of travel for WVU related business or for personal reasons?

- WVU
  - Complete travel screening forms and submit to the Export Control Office at least two weeks prior to departure.

- Personal
  - Will WVU owned equipment accompany the traveler or will the traveler access WVU email or other WVU networks while abroad?
    - No
      - Travel screening forms are not necessary to complete.
    - Yes
      - Travel to such countries may require a federal license which could take up to three months.

Will the traveler visit Cuba, Iran, North Korea, Sudan, Syria or any other embargoed or sanctioned country?

- No
  - Provide the Export Control Office a list of the WVU owned equipment at least two weeks prior to departure and sign the Best Practices form for International Travel once per fiscal year and submit to the Export Control Office.

- Yes
  - Complete travel screening forms and submit to the Export Control Office.
    - Complete travel screening forms and submit to the Export Control Office. Travel to such countries may require a federal license which could take up to three months.
**C. Export Control Screening of Externally Funded Research Grants and Contracts**

The ECO will work closely with the Office of Sponsored Programs (“OSP”) to screen for export control restrictions in externally funded research grants and contracts. An export control screening can be triggered by a variety of research scenarios, including a research sponsor’s insistence on having the right to restrict publications, review publications before approving them, or prohibit the involvement of non-U.S. Persons in the work.

The OSP has primary responsibility for identifying grants and contracts that require export control screening. Upon making such a determination, the OSP will notify the Principal Investigator of the grant or contract in question that an export control screening is required. The OSP will forward a copy of the statement of work of the flagged grant or contract to the ECO and instruct the principal investigator to contact the ECO to facilitate an export control screening of the project. The OSP will not allow the affected grant or contract funding to proceed until the ECO conducts the required screening; the principal investigator acknowledges the results of the screening in writing; and the principal investigator agrees in writing to abide by any written instructions or technology control plan (“TCP”) issued by the ECO.

**D. International Visitors to the University Campus**

West Virginia University has policies and procedures which govern the presence of international visitors on campus. These visitors may include short term visiting scholars; foreign government delegations; foreign company executives or researchers; and participants in short courses, seminars, or conferences. All WVU Personnel seeking to invite international visitors shall adhere to the Visiting Scholars Guidelines as well as the export control guidance issued in this document.

A “deemed export” is the disclosure of information by verbal or visual means of any export controlled item or technical data to any non-U.S. Person. This means that exports can potentially occur during business meetings, briefings, or visits where a non-U.S. Person is present. All WVU Personnel shall ensure that export-controlled items and technical information are only provided to non-U.S. Person in accordance with applicable export control laws.

To identify and address potential export control issues, WVU Personnel inviting a non-U.S. Person not currently residing in the U.S. to the WVU campus or accepting a request for a visit to the WVU campus from such a person shall contact the ECO. Visitors needing screened also include non-US person international students who are not officially registered with the WVU Registrar. The WVU Personnel who will host the visit shall notify the ECO and provide the required information about the proposed visit at least two weeks in advance so the activity can be screened for export control restrictions. While the ECO may request additional information, the typical information required for an export control screening includes:

- The legal full name of the visitor(s);
- The country of citizenship of the visitor(s);
- The visitor’s employer/affiliation;
- The purpose of the visit and what the visitor(s) will see/use during the visit;
• A copy of the passport of the visitor(s) if available;
• The dates when the visitor(s) will be on the WVU campus; and
• The name(s) of the WVU Personnel who is hosting the visitor(s).

In addition to following all guidance provided by the ECO for a particular visit, WVU Personnel hosting the international visitor(s) shall do the following, as applicable:

• Escort the visitor at all times;
• Prior to the meeting/visit, inform all staff members who may be involved of the limitations regarding the release of controlled technical data to the foreign visitor;
• Ensure that the conference room and other areas to be visited do not have any export control information readily visible to the visitor;
• Review all information to be disclosed or disseminated during the visit to ensure that no information is export controlled;
• Immediately report any incidents or suspected incidents, as well as any improper information requests from the visitor; and
• Ensure the visitor(s) only has access to publically available information.

E. Legal Agreements and Business Transactions with Foreign Parties

Engaging in legal agreements and business transactions with foreign parties may raise export control issues. Such activities can result in export control violations if the foreign parties involved appear on any of a number of U.S. Government-maintained screening lists (e.g., the Denied Persons List, the BIS Entity List, the Specially Designated Nationals List). Determining whether a given transaction violates the law requires conducting restricted parties screening—comparing the names of the foreign entities involved to the various U.S. Government-maintained lists. For this reason, all WVU Personnel planning to engage in legal agreements and business transactions, including procurement card transactions, with foreign persons and entities must contact the ECO for assistance prior to negotiating those legal agreements or effecting the transaction.

Upon receipt of the name(s) of the relevant foreign party(ies), the ECO will conduct a restricted parties screening and provide a written response, usually within two business days. This may take longer depending on the technology involved and the parties’ responsiveness. The response will either indicate that the screening revealed no matches and the proposed agreement or transaction move forward as planned or identify any match revealed by the screening and explain the next steps that need to be taken to ensure compliance with export control laws.

F. Purchasing or Receiving Export Controlled Items

All WVU Personnel planning purchases, including those with a procurement card, should consider whether the items to be procured may be subject to export controls. The ECO can assist in this determination if the company cannot provide the information.

If items to be purchased are subject to export controls, the WVU Personnel responsible for the purchase must notify the ECO via e-mail prior to issuing the purchase request (e.g., purchase
order or procurement card), and prior to receiving the controlled item. Prior to receipt of the export controlled item, the WVU Personnel responsible for the purchase shall work with the ECO to ensure that upon receipt it is properly marked with an appropriate notice and properly handled (e.g. stored in a secure area).

G. Property Management

Procedures related to property management are currently under development. Please contact the ECO directly with any questions related to property management.

H. Shipping and Marking Procedures

Procedures related to shipping and marking are currently under development. Please contact the ECO directly with any questions related to shipping and marking.

I. Marking Procedures for Electronic Communications

Procedures for marking electronic communications are currently under development. Please contact the ECO directly with questions related to procedures for marking electronic communications.

VII. WVU Organizational Chart

To view WVU’s Organizational Charts, please see the Web site for the Office of the Vice President for Administration and Finance here.

VIII. Summary of Responsibilities

<table>
<thead>
<tr>
<th>Position or Office</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>All WVU Personnel</td>
<td>All WVU Personnel are responsible for</td>
</tr>
<tr>
<td></td>
<td>• Complying with export control laws and regulations,</td>
</tr>
<tr>
<td></td>
<td>• Becoming aware of export control laws and regulations as they apply to universities,</td>
</tr>
<tr>
<td></td>
<td>• Participating in export control training, and</td>
</tr>
<tr>
<td></td>
<td>• Contacting the ECO about export control laws and regulations when questions arise and/or help is needed.</td>
</tr>
<tr>
<td>Faculty/Researcher</td>
<td>Faculty and Researchers have the primary responsibility for</td>
</tr>
<tr>
<td></td>
<td>• Working with the ECO to identify research activities where there are or may be export control issues,</td>
</tr>
<tr>
<td></td>
<td>• Notifying the ECO of any issues or request help identifying issues.</td>
</tr>
<tr>
<td></td>
<td>• Working with the ECO to accurately classify items and apply for licenses,</td>
</tr>
<tr>
<td></td>
<td>• Ensuring the appropriate protection of all export controlled information and technology in their possession or under their control by following a TCP, and</td>
</tr>
<tr>
<td></td>
<td>• Providing all export documentation, including all transfers related to export controlled materials or projects, to ECO for archiving.</td>
</tr>
<tr>
<td><strong>Office of Sponsored Programs (OSP)</strong></td>
<td>OSP and/or any other office or person negotiating contracts or sponsored research agreements have primary responsibility for</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• Identifying and negotiating to remove from agreements any language which attempts to place restrictions on the University’s ability to publish the research or to place restrictions on the participation or access by foreign nationals,</td>
</tr>
<tr>
<td></td>
<td>• Notifying the ECO in the event that such restrictions are accepted, and</td>
</tr>
<tr>
<td></td>
<td>• Notifying the ECO in the event that awarded grants or contracts contain or may contain export controlled technology or information.</td>
</tr>
<tr>
<td><strong>Department/College</strong></td>
<td>Chairs, Directors, and Deans are responsible for</td>
</tr>
<tr>
<td></td>
<td>• Administering and monitoring of existing TCP of their faculty/researchers;</td>
</tr>
<tr>
<td></td>
<td>• Notifying the ECO of any issues that arise regarding the implementation of, or compliance with, any TCP; and</td>
</tr>
<tr>
<td></td>
<td>• Notifying the ECO when non-externally funded research in their unit may involve export controlled technology.</td>
</tr>
<tr>
<td><strong>Office of Technology Transfer (OTT)</strong></td>
<td>The OTT is responsible for</td>
</tr>
<tr>
<td></td>
<td>• Notifying the ECO of potential export control issues arising in conjunction with material transfer agreements, non-disclosure agreements, license agreements, or other agreement where foreign entities are parties to the agreements and</td>
</tr>
<tr>
<td></td>
<td>• Notifying the ECO when non-student foreign nationals are co-inventors on patent applications assigned to the University.</td>
</tr>
<tr>
<td><strong>Office of Legal Affairs and General Counsel</strong></td>
<td>The Office of Legal Affairs and General Counsel serves in an advisory role to the ECO.</td>
</tr>
<tr>
<td><strong>International Traveler</strong></td>
<td>The International Traveler from WVU is responsible for</td>
</tr>
<tr>
<td></td>
<td>• Notifying the ECO at least two weeks prior to departure when traveling internationally on University business or on personal travel if University-owned property is accompanying the traveler or if University e-mail or electronic files on WVU servers will be accessed from outside the U.S.</td>
</tr>
<tr>
<td></td>
<td>• Contacting the ECO at least three months in advance of travel in case a license is required, if WVU Personnel are traveling to an embargoed or sanctioned country or if the travel may involve export controlled subject matter or equipment.</td>
</tr>
<tr>
<td><strong>Office of International Students and Scholars (OISS)</strong></td>
<td>The OISS is responsible for</td>
</tr>
<tr>
<td></td>
<td>• Notifying the ECO when visa applications requiring export control certification is required.</td>
</tr>
<tr>
<td><strong>Unit Hiring a Foreign National</strong></td>
<td>The Unit Hiring a Foreign National is responsible for</td>
</tr>
<tr>
<td></td>
<td>• Contacting OISS and the ECO and</td>
</tr>
<tr>
<td></td>
<td>• Providing completed Visa Attestation Forms to the Export Control Office for processing.</td>
</tr>
</tbody>
</table>
IX. Glossary of Terms


**Defense Article** – Any item or technical data designated in the USML. Examples include specified chemical agents, cameras designated for military purposes, specified lasers, and GPS equipment. 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 a defense article listed in the USML. International Traffic in Arms Regulations, 22 C.F.R. 120.6 (2015).

**Defense Service** – “Defense service means:

1. The furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles;
2. The furnishing to foreign persons of any technical data controlled under this subchapter (see § 120.10), whether in the United States or abroad; or
3. Military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice. (See also § 124.1.)”


**Denied Persons List** – A list, defined in Part 744, Supplement 4 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. Export Administration Regulations, 15 C.F.R. pt. 744, Supp. 4, (2015).

**Directorate of Defense Trade Controls (DDTC)** – The office in the Department of State that promulgates and implements the International Traffic in Arms Regulations (ITAR) and is responsible for reviewing applications to export and re-export items on the U.S. Munitions List.

**Dual-use** – Items that have both commercial and military applications. “A ‘dual-use’ item is one that has civil applications as well as terrorism and military or weapons of mass destruction (WMD)-related 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. Export Administration Regulations, 15 C.F.R. § 730.3 (2015).
**Empowered Official** – A U.S. Person who:

(1) Is directly employed by the applicant or a subsidiary in a position having authority for policy or management within the applicant organization; and

(2) Is legally empowered in writing by the applicant to sign license applications or other requests for approval on behalf of the applicant; and

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

(4) Has the independent authority to:

   (i) Enquire into any aspect of a proposed export or temporary import by the applicant; and

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

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


**End-use** – A detailed description of how the ultimate consignee intends to use the items or commodities being exported.

**End-user** – The person abroad that receives and ultimately uses the exported or re-exported items. The end-user cannot be a forwarding agent or intermediary, but may be the purchaser or ultimate consignee.

**Export** – U.S. export control laws broadly define the term “export.” Due to this, the scope of these laws is not intuitive. Any item that is transferred from a U.S. Person to a foreign person is an export. Exports can happen by mail, facsimile, uploading/downloading via the web, e-mail, by face-to-face conversation, or by phone.

**Export Administration Regulations** – These are the regulations promulgated and implemented by the Department of Commerce that regulate the export of goods and related technology identified on the Commodity Control List (CCL), 15 CFR 774, Supplement 1. Goods and technology on the CCL are not inherently military in nature; they are primarily commercial in nature. Export Administration Regulation, 15 C.F.R. pts. 730–774 (2015).

**Export controls** – The set of laws, policies, and regulations that govern the export of sensitive items for a country or company. This refers to the EAR and ITAR as well as other regulations.

**Export Control Classification Number (ECCN)** – Identifies items on the Commerce Control List that are subject to the export licensing authority of the Bureau of Industry and Security.

**Exporter** – The person who has authority of a principal party in interest to determine and control the sending of items out of the U.S.
**Export license** – 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.

**Foreign Person** – Any natural person who is not a lawful permanent resident or who is not a protected individual as defined by 8 USC 1324(a) (3). It also includes any foreign corporation, business association, partnership, trust, society or any other entity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments and any agency or subdivision of foreign governments (e.g., diplomatic missions). International Traffic in Arms Regulations, 22 C.F.R. 120.16 (2015).

The EAR uses the definition “non-U.S. Person” instead of “foreign person.”

**Fundamental Research** – Basic or applied research in science and engineering performed or conducted at an accredited institution of higher learning in the United States where the resulting information is ordinarily published and shared broadly in the scientific community. Fundamental research is distinguished from research that results in information that is restricted for proprietary reasons or national security reasons or pursuant to specific U.S. government access and dissemination controls. Export Administration Regulation, 15 C.F.R. § 734.8 (2015); International Traffic in Arms Regulations, 22 C.F.R. § 120.11 (2015).

**Good** – Any article, natural or man-made substance, material, supply, or manufactured product, including inspection and test equipment, and excluding technology.

**International Trafficking in Arms Regulations (ITAR)** – The regulations promulgated and implemented by the DDTC that control the export and temporary import of articles, services, and related technical data that are inherently military in nature, as determined by the Arms Export Control Act (AECA). These “defense articles,” “defense services,” and related “technical data” are listed on the United States Munitions List (USML), 22 CFR 121. International Traffic in Arms Regulations, 22 C.F.R. pts. 120–130 (2015).

**Public Domain** – Information that is published and that is generally accessible or available to the public: (1) through sales at newsstands and bookstores; (2) through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information; (3) through second class mailing privileges granted by the U.S. government; (4) at libraries open to the public or from which the public can obtain documents; (5) through patents available at any patent office; (6) through unlimited distribution at a conference, meeting, seminar, trade show, or exhibition, generally accessible to the public, in the United States; (7) through public release (i.e., unlimited distribution) in any form (e.g., not necessarily in published form) after approval by the cognizant U.S. government department or agency; and (8) through fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community. International Traffic in Arms Regulations, 22 C.F.R. § 120.11 (2015).

The EAR uses the term “publically available” rather than “public domain.” Export Administration Regulations, 15 C.F.R. 734.3(b)(3).
**Purchaser** – The person abroad who has entered into a transaction to purchase an item for delivery to the ultimate consignee. In most cases, the purchaser is not a bank, forwarding agent, or intermediary. The purchaser and ultimate consignee may be the same entity.

**Re-export/Retransfer** – “Re-export” means an actual shipment or transmission of items subject to export control regulations from one foreign country to another foreign country. For the purposes of the EAR, the export or re-export of items subject to the EAR that will transit through a country or countries to a third country, or are intended for re-export to the third country, are exports to the new country.

**Specially Designated Nationals (SDNs)** – Individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. The list also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called “Specially Designated Nationals” or “SDNs.” Their assets are blocked and U.S. Persons are generally prohibited from dealing with them.

**Technical assistance** – Technical assistance may take forms such as instruction, skills training, working knowledge, consulting services, and may also involve the transfer of technical data. Export Administration Regulations, 15 C.F.R. 772 (2015).

**Technical data** – Information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of controlled articles. 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, or read-only memories. This definition specifically excludes information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities, or information in the public domain. International Traffic in Arms Regulations, 22 C.F.R. § 120.10 (2015).

**Technology** – Any specific information and know-how (whether in tangible form, such as models, prototypes, drawings, sketches, diagrams, blueprints, manuals, software, or in intangible form, such as training or technical services) that is required for the development, production, or use of a good, but not the good itself.

**U.S. Person** – A U.S. Person is a (1) U.S. Citizen, including U.S. university, such as WVU; (2) Permanent Resident Alien; or (3) Political Refugee protected under the Immigration and Naturalization Act.

**United States Munitions List (USML)** – Articles, services and related technical data designated as defense articles and defense services pursuant to the Arms Export Control Act (AECA). International Traffic in Arms Regulations, 22 C.F.R. § 121.1 (2015).

**X. Forms and Additional Information**

A. Appendix 1 – Additional Information
   • Anti-Boycott Protections
• Anti-Bribery Protections

B. Appendix 2 – Additional Information
• International Travel Screening Form
• Export Administration Regulations TMP Exception Form
• Best Practices to Maintain Security of Controlled Technology of Technical Data during International Travel
• WVU Deemed Export Verification for Non-Immigrant Visas Form
• Electronic Devices Lost/Stolen on International Travel Form
Appendix 1

A. Anti-Boycott Protections

Avoiding and Reporting Illegal Boycotts

The “anti-boycott” provisions of the EAR prohibit U.S. Persons, including U.S. companies and institutions like WVU, from participating in any non-U.S. sanctioned foreign government boycott.

Participation in this context includes refusing to engage in business transactions with the boycotted country, agreeing not to use “blacklisted” suppliers from the boycotted country, or providing information related to business relationships with the boycotted country. Also prohibited are agreements to discriminate against others based on race, religion, sex, national origin, or nationality.

While the EAR’s anti-boycott provisions apply to any foreign country’s boycott, in practice the primary anti-boycott focus involves the Arab League’s boycott of Israel. This long-standing boycott is aimed at Israel, with people who do business with Israel, or those who do business with parties the Arab League places on its “black list.”

Therefore, if any project or activity involves countries in or aligned with the Arab League, WVU Personnel must be on the alert for inquiries about whether WVU does business with Israel or with companies who do business with Israel. Such questions are invitations to participate in the boycott and must be reported. More information on the reporting requirement is in the section below, under “Positive Obligations.”

Negative and Positive Obligations

Under U.S. Anti-Boycott law, there are both negative and positive obligations. The negative obligations are things U.S. Persons cannot do, and the positive obligations are things U.S. Persons must do. While the boycott most likely to be encountered remains the Arab League Boycott of Israel, any minimal request for information might be part of an illegal boycott.

Negative Obligations – What U.S. Persons Cannot Do

- Agree to refuse or refuse to do business with companies located in boycotted countries, businesses organized in boycotted countries, or blacklisted companies.
- Agree to furnish, or furnish information about business with boycotted countries, businesses organized in boycotted countries or blacklisted companies.
- Agree to discriminate against others based on race, religion, sex, national origin, or nationality.
- Agree to furnish, or furnish information about race, religion, sex, national origin, or nationality.
- Pay with, or accept letters of credit that include requirements that violate any of these negative obligations.
• Agree to follow the laws of countries participating in a prohibited boycott, which may include requirements to comply with the Arab League Boycott of Israel.

Positive Obligations – What U.S. Persons Must Do

• Report any invitation to participate in a boycott. An invitation includes
  ▪ Being asked to comply with the boycott; or
  ▪ Being asked to furnish information that helps the country carry out the boycott.

If any WVU Personnel receive a request to participate in an illegal boycott, do not furnish any information. Stop the transaction and immediately contact the ECO.

B. Anti-Bribery Protections

Under U.S. anti-bribery laws, U.S. citizens, nationals, residents, and businesses are prohibited from giving a corrupt payment to a foreign government official for the purpose of influencing a decision of the official in his official capacity.

Prohibited Payments

A “corrupt payment” is the payment of money or an offer or promise to give anything of value to influence the official in his official capacity, to influence the official to violate his/her lawful duty, or to seek an improper advantage. For example, making a contribution to the private school the official’s children attend or making charitable contributions to the official’s favored charity could be a corrupt payment, if made with the intent to obtain an improper advantage or to secure the official’s action in his/her official capacity.

Under the law, even making an offer of payment, as long as it is made with the intent to influence, obtain improper advantage, or induce improper influence, is all that is required for a violation. Even if the official refuses to accept the benefit, or accepts the benefit but does not take the desired action, it is still a violation.

Limited Exceptions for Common Business Practices and Payments

Certain common business practices, such as paying the costs of a foreign official to travel to campus for a site visit may be legal. In addition, certain payments as part of routine government action may be allowed. Since the exceptions are extremely limited, WVU Personnel must contact the ECO for pre-authorization for any payment to a foreign official and instructions for reimbursement for these limited, pre-approved transactions.

Third Party Payments Can Create Liability

If a third party, such as a WVU project partner, makes an illegal payment, WVU can still be liable, even if WVU Personnel have no knowledge of the payment. Therefore, it is extremely important to let WVU’s partners know that they must abide by U.S. law. Applicable contract terms must provide that WVU may unilaterally terminate the contract in the event of non-
compliance with anti-bribery laws. If WVU Personnel ever suspect that a partner may violate or has violated anti-bribery law, he or she must report this immediately to the ECO.

**High Risk Projects**

Although WVU Personnel are strictly prohibited from making an illegal payment or offer, they may receive a request for corrupt payment from a foreign official. Certain WVU projects and activities may be at higher risk than others for violations of anti-bribery laws. When a foreign government has regulatory control or approval authority over aspects of a large contract or key aspects of a program, this may create an incentive for officials to request bribes or “payoffs” in exchange for favorable treatment on the project. Some countries are considered to present a higher risk for bribery requests or inadvertent violations.

If WVU Personnel are notified that the project is at increased risk because of the specific countries involved, proceed with caution. Any questions or concerns during the project must be directed to the ECO.
Appendix B

WVU Export Control Form for International Travel

This form is to be completed ELECTRONICALLY by WVU international travelers and forwarded via e-mail to the WVU Export Control Office (ECO) when complete and electronically signed where indicated. The international traveler is responsible for export control compliance. Please send completed forms or questions to Nancy.Draper@mail.wvu.edu (304)293-3084.

Part 1: Traveler’s Information
Traveler’s Name: 
Traveler’s U.S. Telephone No.: 
Preferred Email Address: 
Country of Citizenship (current & prior, including dual): 
Country of Permanent Residence (current & prior, including dual): 
Country of Birth: 
WVU Title: 
Department/Unit Name: 
Site of Employment: 
Supervisor’s Name and Telephone No.: 
Travel Dates: from: to: 
List all countries traveling to (including layovers):

Part 2: International Travel Questionnaire
1) Are you traveling to Cuba, Iran, North Korea, Syria, or Sudan? □ YES □ NO
2) What is the purpose of this trip? Select one:
☐ Conference or meeting; Are You Presenting? □ YES □ NO
☐ Research project
☐ Other (Please specify: )
If you are attending a conference or meeting, please provide the full name of the event, sponsor, and the website in your email when submitting this form, if applicable. If you are presenting, please attach a copy of your abstract and/or presentation. Please list the names of people you plan to meet to do business.
3) Will you carry a WVU-owned laptop computer, tablet/smart phone, or other equipment while traveling? □ YES* □ NO
4) Will you travel with hazardous material or scientific instruments containing licensed or hazardous materials? □ YES □ NO
5) Have you cleared electronic storage media (laptop computers, flash drives, tablets, smartphones, etc.) of sensitive (either export controlled or proprietary) information? □ YES □ NO □ N/A Please contact the ECO if you have questions.
6) Do any of the items with which you are traveling contain encryption software source or object code? □ YES □ NO
7) Will you carry items, documents, information, or data related to previously identified export controlled research? □ YES □ NO
8) Do you have any reason to believe that the items, documents, information, or data you will carry have a military use (e.g., the design, development, production, or stockpiling or use of nuclear explosive devices, chemical or biological weapons, or missiles) □ YES □ NO □ N/A
9) Is your software (if any), technology, or information considered to be in the PUBLIC DOMAIN or considered to be FUNDAMENTAL RESEARCH because:
   a. The information has already been published in open literature and is available worldwide? □ YES □ NO □ N/A
      If yes, please cite such a source where the information can be found:
   b. The information is free to be published without restriction? □ YES □ NO
   c. The software does not contain source code for encryption software or marketed encryption? □ YES □ NO □ N/A

*List in the table below any WVU owned equipment which you are taking on your trip including laptop computer, tablet, smart-phone, scientific instruments, etc. Use an extra page, if necessary.

<table>
<thead>
<tr>
<th>Common Name of Item</th>
<th>Model No. if Applicable</th>
<th>Manufacturer if Applicable</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: If the Export Control Office determines your equipment may include export controlled material, you will be contacted for more information.

Traveler’s Electronic Signature: ____________________________ Date: ____________

(Please use the format “/John Q. Doe/” for the electronic signature, no hand signature is required.)
Export Administration Regulations TMP Exclusion

The TMP Exclusion must be filed with WVU’s Export Control Office prior to shipping or hand-carrying export controlled item(s) or software to Iran, Syria, Cuba, North Korea, or Sudan. If you have any questions about this, please contact the WVU Export Control Office at 304-293-3084 or nancy.draper@mail.wvu.edu.

The export of tangible items, software, and encryption software/technology is subject to export control regulations. The 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 exclusion does not apply to any satellite or space related equipment, components or software, or to any technology associated with high level encryption products. In addition, this exclusion does not apply to items, technology, data or software regulated by the Department of State’s International Traffic in Arms Regulations (ITAR).

In the table below, please provide a description of the items, technology, or software, to which this certification applies. Common items to be listed include laptop computers, smart phones, tablets, scientific equipment, etc.

**TMP Exclusion Table**

**Description of Items, Equipment, Technology, or Software Accompanying Traveler***

<table>
<thead>
<tr>
<th>Common Name of Item</th>
<th>Model No. if Applicable</th>
<th>Manufacturer if Applicable</th>
<th>Comments (please WVU or personal)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*If you have potentially sensitive software installed on a device you are taking along on international travel, please attach a screenshot of the program file list from the device. If you require more space, please attach additional sheets.

**By my signature below, I certify that:**

1. Any WVU owned item(s) and software I take abroad will ONLY be used as a “Tool of the Trade” to conduct WVU business or research.
2. None of the items I am taking are defense articles or technical data controlled under the ITAR.
3. None of the personally owned items I am taking contain WVU related files in electronic memory.
4. I will return the item(s) and any related software to the U.S. no later than 12 months from the date of export unless the item(s) and software are certified in writing by me to have been consumed or destroyed abroad during this 12 month period.
5. I will maintain any WVU owned item, technology, or software under “Effective Control” while abroad. (Effective Control is defined as retaining physical possession of an item at all times or maintaining it in a secure environment such as a hotel safe).
6. I will take security precautions to protect against unauthorized release of WVU technology while the technology is being shipped or transmitted and used abroad such as:
a. Use of secure connections when accessing email 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.

7. I will not ship or hand-carry items or software not listed above to Iran, Syria, Sudan, Cuba, or North Korea without a license and written approval from the WVU Export Control Officer.

8. I am not using the items in relation to any nuclear research.

Traveler’s Name:  Date:

Traveler’s Signature:

Gary J. Morris, Export Control Officer

Signature of Export Control Officer  Date

**Keep a signed copy of this document with you when traveling abroad**
Best Practices to Maintain Security of Controlled Technology or Technical Data during International Travel

Introduction
Academic personnel including faculty investigators, graduate students or research fellows, and undergraduates travel internationally to attend or present at conferences and meetings, to collaborate with colleagues at other research institutions, and to perform field research. It is important to note that the academic traveler’s failure to comply with U.S. export control laws can have grave consequences for the traveler and WVU. The traveler is ultimately responsible for compliance.

The Department of Commerce (Export Administration Regulations - EAR), the Department of State (International Traffic and Arms Control Regulations - ITAR), and the Department of Treasury (Office of Foreign Asset Controls - OFAC) have regulations that govern items which a traveler may take on international travel such as:

- Laptop computers, smart phones, tablets, etc.
- Encryption products on your laptop computer
- Data/Technology
- Blueprints, drawings, schematics etc.

Academic personnel must consider the potential effect of each set of U.S. export control regulations on the proposed international travel to assure that both the institution and the individual traveler are in compliance. The Department of Commerce and the Department of State are principally concerned with whether the academic traveler will take and then disclose (intentionally or unintentionally) any controlled technology or other controlled information to non-U.S. persons (e.g. in papers, in personal conversations, on their laptop computers, or other electronic storage devices) or will export any controlled items (e.g., sensors, test instrumentation, reagents, biological materials or other similar tangible goods) to non-U.S. persons. The Department of Treasury is most concerned with the specific entities (institutions, companies, and persons) which the traveler may interact with or do business with while traveling abroad. A U.S. person is defined as a U.S. citizen, a U.S. permanent resident, or a person having protected status in the U.S.

Traveling with Electronic Devices or Data
A U.S. person travelling abroad may take an institution-owned laptop computer, smart phone, tablet, etc. to most countries without a license or license exemption or exclusion. While visiting some embargoed countries, a laptop computer, smart phone, tablet, etc. may be carried by a US person provided the laptop computer is kept under the traveler’s effective control* and is returned to the United States not more than one year after the original departure date. It may be necessary to complete the TMP/BAG exclusion form prior to traveling to embargoed countries if the traveler is taking a laptop computer, smart phone, tablet, etc. The Export Control Office will inform the traveler if their trip requires a TMP/BAG exclusion based on information provided by the traveler.

*Effective control: The traveler maintains effective control over an item when they either retain physical possession of the item, or secure the item whereby no other person may gain access to the item without engaging in criminal activity.

Vacation or Personal Travel
Vacation travel or other personal travel abroad to destinations other than embargoed countries does not need to be reported to the Export Control Office, however, such travelers MUST read and sign the most recent Best Practices document once per fiscal year and submit same to the Export Control Office if any WVU owned devices or information is accompanying the traveler or if the traveler will access WVU email. Any person traveling to an embargoed country for any reason, needs to consult with the Export Control Office as soon as the trip is planned.

Guidelines to Remain Compliant
To ensure that the traveler does not run the risk of releasing sensitive information or technology when traveling abroad, or dealing with sanctioned countries, entities, or individuals, keep the following guidelines in mind:
• Presentations and discussions must be limited to topics that are not related to controlled items or technologies unless that information is already published or otherwise already in the public domain.

• Verify that your technology or information falls into one or more of the following categories prior to travelling to non-embargoed countries:
  o Research which qualifies for the fundamental research exclusion
  o Openly published information
  o Publically available information
  o Unrestricted academic information
  o Publically available software
  o Issued patents and published patent applications

• DO NOT allow any person to connect a USB flash drive or other external storage device to your laptop computer or other electronic devices.

• DO NOT access WVU file servers or remote desktop computers.

• DO NOT access WVU email or personal email involving WVU related information from an unsecured network or WiFi connection. Do not transmit export controlled information even over a secured connection even if the information is encrypted. Encrypted information is still controlled by export control laws.

• When accessing WVU email while abroad, use ONLY the web-based Office 365 client NOT the desktop client or a mobile application on a smart phone or tablet. The desktop client and mobile applications download all email and attachments to the local device which makes accessing email much more risky while traveling abroad. Use only a web-based client for accessing any email when using your smart phone or tablet if there is any chance that you will be receiving export controlled emails while you are traveling abroad so that such email and related attachments will not be downloaded to your local device.

• DO NOT open any email attachments you suspect contain may export controlled information.

• Change your MyID password immediately upon return from international travel if you have used this password to access WVU email or for any other purpose during your travel.

• If at all possible, take a clean, department laptop computer configured specifically for international travel rather than your work or personal laptop computer. A clean laptop computer is one which has been screened by OIT personnel to be clean of all malware, viruses, etc. and contains only standard the Microsoft Suite and Adobe Suite of software. The clean laptop computer is to be re-screened by OIT personnel upon your return before it is connected to any University systems including wireless or wired networks.

• The FBI warns that in some countries, the simple act of turning on your laptop computer while WiFi is enabled (or if you connect to wired network) will result in ALL files and information on your computer being copied. Therefore, you should assume that everything stored on your computer or connected to your computer will be viewed by others when you are traveling abroad.

• Be aware that keyboard logger devices or malware may be recording your keystrokes on your electronic device while you are in airports, hotels, restaurants etc.

• Don’t use telephones, computers, and fax equipment at foreign hotels or business centers for anything not currently in the public domain.

• If any electronic devices are stolen, file a police report and notify the ECO as well as OIT as soon as possible. Also notify the ECO and OIT immediately if any electronic devices are lost.
• Other precautions may be necessary depending on the traveler’s destination. The ECO will notify the traveler of these prior to departure.

**Preparing your electronic devices before leaving the U.S.:**

• Remove anything from any electronic device that constitutes a trade secret, proprietary information, export-controlled technical data/information or anything you wish to keep confidential prior to leaving the United States.

• *Deleting a file is NOT enough.* Use a “Shredder” program to erase the information you do not want to share so that it cannot be recovered.

• Keep your work files on an encrypted flash drive or an encrypted external hard drive.

• Delete any saved passwords.

• Keep all electronic devices in your carry-on luggage.

  **Remember: If you don't need it - don't take it with you!!**

I certify that I have read the above best practices information and understand it. I will contact the WVU Export Control Office (ECO) if any questions arise regarding best practices for protecting export controlled technology and information. I agree to comply with any additional instructions the ECO may need to convey to me in accordance with my specific travel plans. I understand that the traveler is responsible for export control compliance.

Traveler’s Name:
Traveler’s Hand Written Signature:
Date:

*This document must be read and signed by international travelers once per fiscal year as part of the Export Control Office review of international travel. Please send the Export Control Office an electronic copy of the signed document. The Export Control Office will maintain records of the signed documents and will request that a newly signed document be submitted for an international traveler if the latest signed document on file has expired.*
WVU Deemed Export Verification for Non-immigrant Visas

To be completed by Foreign National’s supervisor or a designee with knowledge of the Foreign National’s intended work and forwarded electronically to the Export Control Office (ECO) at nancy.draper@mail.wvu.edu:

Name of Foreign National:
Country of Citizenship (current & prior including dual):
Country of Permanent Residence (current & prior including dual):
Country of Birth:
Title at WVU:
Visa Type: □H-1B □J-1 □TN □O-1 □F-1 □OPT □J-2 □B-1/B-2
Renewal: □ YES □ NO
Department Name hosting Foreign National:
Site of Employment:
Supervisor’s Name, Telephone No., and Email:
PI’s Name, Telephone No., and Email:
Employment Date: From __________ To __________

Is the Foreign National currently assigned a project and/or equipment?
□ Yes
□ No

If yes, a detailed project description and/or list of equipment MUST BE attached. Or, if no projects are assigned to the Foreign National at this time, please complete the following statement:

Dr./Mr./Ms. ________ has no projects assigned to him/her at this time. The department/unit has the obligation of providing the ECO, a detailed project description and equipment description prior to the initiation of research project by Dr./Mr./Ms.

________________________

Questionnaire: Please answer all questions below

1. Foreign National's work will be supported by:
   □ Grant
   □ Contract
   □ State Funds
   □ F&A Funds
   □ Faculty Start-up Funds
   □ Other (Please specify: ________ )

2. Foreign National's duties will be (mark all that apply):
   □ Administrative
3. Will the Foreign National be working with high-tech or experimental equipment (examples include, but are not limited to, high speed computers, high speed cameras, sensors, materials, electronics, lasers, biometrics, telecommunication devices, or other cutting edge equipment)?
   - Yes
   - No

4. Will the Foreign National have access to equipment that was specifically designed or developed for military or space applications (e.g., night vision cameras, satellite technology, controlled imaging equipment, or Y-code GPS) or that has been previously identified as export controlled?
   - Yes
   - No

5. Please list the names & contact details of the personnel who would be responsible for training the Foreign National. If there are none, please answer “none.”

6. Will the Foreign National have access to any WVU owned technical data or technology that is considered proprietary or confidential to WVU?
   - Yes
   - No

   If the answer to Question 6 is “yes,” describe briefly. If “no,” please skip to Question 7.

   Has the technical data or technology been disclosed to the WVU Export Control Office?
   - Yes
   - No

7. If the Foreign National will be involved in any research projects sponsored, in whole or in part, by either WVU or an external sponsor, including the federal government, are there any restrictions in the award grant or contract terms on publication of results or participation of foreign nationals?
   - Yes
   - No

8. Will the Foreign National travel outside of the United States for research related purpose?
   - Yes
   - No

   If “yes,” please list any WVU owned equipment they will take (i.e., laptop computer, tablet, cell phone or similar equipment).
Certification - WVU Deemed Export Verification

I work, or will work, in a capacity that enables me to anticipate the particulars of the employment of (henceforth, “Foreign National”), a citizen of , should he/she be granted permission from the U.S. Government to work within WVU.

I affirm that the contents of the foregoing Verification are true, to the best of my knowledge, information, and belief.

If at any time during Foreign National’s employment I become aware that technology or technical data have/are/or will be released to Foreign National in ways that were not anticipated by my answers to the Questionnaire, I will immediately notify the Office of International Students and Scholars and the WVU Export Control Office.

I will notify the Office of International Students and Scholars before the Foreign National moves to a new office or lab, or begins work activity outside my control or knowledge.

Certifier (Chair or other Supervisor)  Additional Certifier (e.g. Principal Investigator)
Printed Name  Printed Name
Certifier’s Title  Additional Certifier’s Title
Certifier’s Signature  Additional Certifier’s Signature
Date  Date
For Internal Purposes – to be completed by the ECO

☐ A license is not required from either the U.S. Department of Commerce or the U.S. Department of State to release such technology or technical data to the Foreign National; or

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

How and when was the beneficiary screened?  
☐ eCustoms Visual Compliance
☐ Other
Date: ______________________

Gary J. Morris, Export Control Officer

Signature: ______________________

Date: ______________________
Electronic Devices Lost/Stolen on International Travel

Traveler’s Name:
Traveler’s Department/Unit:
International Destination(s):
Dates of Travel: From to
Date of Loss of Device(s):
In what country was the device lost?
How was the device lost?
☐ Traveler misplaced device
☐ Device was stolen
If the device was stolen, was a police report filed?  ☐ Yes ☐ No
(if yes, please attach a copy of the police report)
☐ Device was destroyed

Description of the Lost Device (if multiple devices were lost or stolen, please include the information below for the additional devices on an attached sheet)

Type of Device:
Brand:
Model:
Serial Number (if known):
Ownership: ☐ WVU ☐ personal ☐ other (please specify):

Please attach a detailed description of the contents of the lost electronic device(s).

Certification
I certify that to the best of my knowledge, no export controlled information or confidential information was stored on the lost electronic device(s) described in this document and attached sheets.

___________________________
Printed Name

___________________________
Signature

___________________________
Date