



Washington University in St. Louis

Export Management and Compliance Program

The purpose of this document is to provide overall guidance on export control regulations and Washington University export control internal policy and procedures. For additional information or assistance please contact the Export Control Manager, via email at ovcreportcompliance@wustl.edu or at 314-747-1378. Please note that although every attempt is made to keep this information up to date, regulations do change, so for the most up to date information consult primary sources cited in this manual.

Reviewed and Updated
January 5, 2022
May 15, 2019

Initial Approval Date: January 12, 2017

TABLE OF CONTENTS

	Frequently Used Abbreviations.....	5
I.	Introduction.....	6
II.	Overview of U.S. Export Control Regulations.....	7
	What is an “Export”?.....	7
	Who is a U.S. Person vs. a Foreign National?.....	7
	What are the Main Concerns of Export Control?.....	7
	Regulations.....	8
	Department of State International Traffic in Arms Regulations (ITAR).....	9
	Department of Commerce Export Administration Regulations (EAR).....	9
	Department of Treasury and Office of Foreign Assets Control (OFAC).....	10
	Penalties.....	10
III.	Export Controls at Washington University.....	11
	Institutional Commitment.....	11
	Washington University Export Control Policy.....	11
	Applicability.....	11
	Policy.....	11
	Roles and Responsibilities.....	12
	University Export Control Manager.....	12
	Principal Investigator.....	12
	Senior Official.....	13
	Empowered Officials.....	13
	Export Control Advisory Committee.....	13
	Cooperating Entities.....	13
	Office of Sponsored Research Services	13
	Joint Office of Research Contracts	13
	Environmental Health and Safety	13
	Office of International Students and Scholars.....	14
	Purchasing Services.....	14
	University Compliance Office.....	14
	Information Technology.....	14
	Office of Technology Management	14
	Human Resources.....	14
	Office of General Counsel.....	14
IV.	Exclusions from Export Controls Relevant to Universities.....	15
	Publicly Available Information.....	15
	Educational Information.....	17
	Fundamental Research.....	18
	Full-time University Employees.....	18

V.	Washington University Processes and Procedures.....	20
	Restricted Party Screening.....	20
	Export Control Review.....	20
	Sponsored Research.....	21
	Material Transfer and Licensing Agreements.....	22
	H-1B Visa Applicants.....	22
	Shipping.....	22
	Purchases.....	23
	Additional Reviews.....	23
	Protecting Export Controlled Technology from Unauthorized Access.....	23
	Technology Control Plans.....	23
	Licensing.....	24
	Records and Record Retention.....	24
	Training.....	24
	Audits.....	24
	Detecting and Reporting Violations.....	25
	Appendix I – International Traffic in Arms (ITAR) Regulations	26
	Regulatory Authority and Scope.....	26
	Items Controlled under the ITAR.....	26
	U.S. Munitions List Categories.....	26
	Exporting under the ITAR.....	27
	Important ITAR Definitions.....	27
	Appendix II – Export Administration (EAR) Regulations (EAR).....	29
	Regulatory Authority and Scope.....	29
	Items Controlled Under the EAR.....	29
	Commerce Control List Categories.....	29
	Exporting under the EAR.....	30
	Important EAR Definitions.....	30
	Determining License Requirements under the EAR.....	31
	License Exceptions.....	32
	Appendix III –Office of Foreign Assets Control (OFAC) and Other Regulations.....	33
	Restricted Persons.....	33
	Anti-boycott Regulations.....	34
	Other Export Regulations.....	34
	Appendix IV – Penalties.....	36
	Defense Articles & Technical Data.....	36
	EAR Controlled Technology.....	36
	Anti-Boycott.....	36
	OFAC.....	36
	Voluntary Self-Disclosure.....	36
	Appendix V – Washington University Export Control Compliance Organizational Chart.....	38

Appendix VI – H1-B Export Control Review Questionnaire.....	39
Appendix VII - ITAR Language in Washington University Purchase Terms and Conditions.....	46
Appendix VIII – Technology Control Plan and Briefing Template.....	47

List of Figures

Figure 1. Four Elements of U.S. Export Controls.....	8
Figure 2. Export Control Decision Tree.....	21

List of Tables

Table 1. Export Control Regulations.....	8
Table 2. Public Information Excluded from Export Controls by Agency.....	15
Table 3. Definition of “Educational Information” by Agency.....	17
Table 4. Restricted Party Screening Processes at Washington University.....	20

FREQUENTLY USED ABBREVIATIONS

BIS	Bureau of Industry and Security
CCL	Commerce Control List
CFR	Code of Federal Regulations
CJ	Commodity Jurisdiction
DDTC	Directorate of Defense Trade Controls
EAR	Export Administration Regulations
ECCN	Export Control Classification Number
ECM	Export Control Manager
ITAR	International Traffic in Arms Regulations
JROC	Joint Office for Research Contracts
OFAC	Office of Foreign Assets Control
OISS	Office of International Students and Scholars
OSRS	Office of Sponsored Research Services
OTM	Office of Technology Management
PI	Principal Investigator
RPS	Restricted Party Screening
TCP	Technology Control Plan
USML	United States Munitions List

I. INTRODUCTION

The United States (U.S.) has a complex set of regulations which govern the transfer of controlled technology and information to foreign countries and to foreign nationals within the U.S. These include the International Traffic in Arms Regulations (ITAR), the Export Administration Regulations (EAR), and the Office of Foreign Assets Control (OFAC) regulations, collectively called the “Export Control Laws”. The purpose of the Export Control Laws is to provide for the national security of the United States by promoting regional stability, preventing the proliferation of weapons of mass destruction, advancing U.S. foreign policy objectives abroad, and protecting U.S. economic interests at home. These complex laws are administered by multiple federal agencies and may apply to university activities.

The Washington University environment is open and collaborative by design, as evidenced by its Policy on [Open Research and Free Dissemination of Ideas and Information](#). Our campus hosts international students, postdocs, and scholars and our investigators participate in international collaborations and scholarly exchanges. At the same time, the University is committed to compliance with federal laws and regulations. The [University Code of Conduct](#) mandates that all University personnel abide by federal regulations in their pursuit of University activities. It is important that the campus community be aware of, understand, and comply with the Export Control Laws while continuing to advance our mission of discovering and disseminating knowledge and protecting freedom of inquiry.

The purpose of this Export Management and Compliance Program (EMCP) document is to promote awareness and understanding of the Export Control Laws, to describe the export control compliance program at Washington University, and to facilitate export control compliance by the University community including faculty, staff, administrators, students, postdoctoral fellows and other scholars. It is for internal use only. Any inconsistencies between this manual and the Export Control Laws are unintentional. In such cases the applicable export control law takes precedence.

The information in this document is available on the Washington University Office of the Vice Chancellor for Research website under “Topics”; [“Export Control”](#), including this document in its entirety in PDF form. It will be updated by the Export Control Manager as needed. For questions, feedback or suggestions related to this document please contact the Washington University Export Control Manager at OVCRExportCompliance@wustl.edu.

II. OVERVIEW OF U.S. EXPORT CONTROL REGULATIONS

In order to understand and apply export control regulations it is important to understand how the government defines an “export” and how it defines a “foreign national”.

WHAT IS AN “EXPORT”?

An “export” is the shipment or transfer of items out of the U.S., or the “release” of technology, software, or technical data to a foreign person within the U.S. If the transfer is made to a foreign national within the U.S. it is called a “deemed export”. “Release” is not limited to shipment or physical transfer but may occur through visual inspection, oral exchanges of information, email and electronic exchanges, or training that reveals technical data. For example, release of controlled technical data to a foreign graduate student working in a laboratory on campus would be considered a deemed export. Depending on the technology and the citizenship of the foreign national, it may be necessary to obtain an export license before this release could occur.

WHO IS A U.S. PERSON vs. A FOREIGN NATIONAL?

A U.S. person is a U.S. citizen, a lawful permanent resident, or a protected individual under the Immigration and Naturalization Act¹. A U.S. person can also be an entity, for example a business, university, or government body. All other persons and entities are considered foreign nationals.

WHAT ARE THE MAIN CONCERNS OF EXPORT CONTROL?

There are four main concerns of U.S. Export Controls; technology classification, destination, end-user, and end-use (Figure 1). The **technology classification** is determined by the technology that is being exported. Was it designed for military or civil use? If equipment, what are the technical specifications? What type of technical information or software is it? The classification will in large part determine whether a license is needed for export. The **destination** refers to where the technology is being exported to. Does technology with that classification require a license for export to that particular country? Is it destined for a sanctioned country? The **end-user** refers to the institution and/or the individual who will receive the export. Are they allowed to receive it without a license? Are they on any restricted party lists? **End-use** refers to what they will do with it. Some end-uses, such as weapons proliferation, are prohibited, regardless of what item is being exported.

¹ 8 U.S.C. §§ 1101-1178

Four Elements of U.S. Export Controls

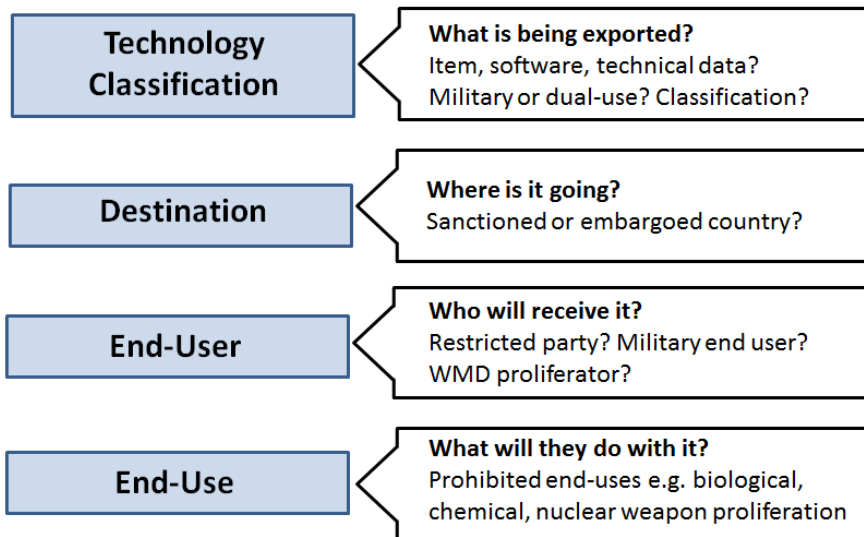


Figure 1. Four Elements of U.S. Export Controls

REGULATIONS

The most extensive export control regulations are associated with the export of technology, associated technical data, and technical assistance or defense services. Authority over those exports is primarily controlled by three agencies: the Directorate of Defense Trade Controls (DDTC) within the Department of State; the Bureau of Industry and Security (BIS) within the Department of Commerce; and the Office of Foreign Assets Control (OFAC) within the Department of the Treasury. Each agency maintains an independent set of regulations which are discussed briefly below. Detailed information for each set of regulations can be found in Appendices I, II and III.

Table 1. Export Control Regulations

Governing Agency	Mechanism	Covers
Department of State	International Traffic in Arms Regulations ((ITAR)	Items designed for military use, defense services
Department of Commerce	Export Administration Regulations (EAR)	Dual use items
Department of the Treasury	Office of Foreign Assets Control (OFAC)	Sanctioned countries and restricted entities

Department of State International Traffic in Arms Regulations (ITAR)

The Department of State Directorate of Defense Trade Controls (DDTC) administers export controls through the International Traffic in Arms Regulations (ITAR)². The ITAR regulations are the first regulations to consult when conducting **technology classification** (Fig. 1). ITAR controlled technologies are described on the [United States Munitions List](#) (USML).³

The USML includes defense articles and associated technical data. It is important to note that although these items were designed for military purposes, they are controlled for export *regardless of how they are being used on campus*. ITAR controlled items require licenses from the DDTC for physical export or for technology release to foreign nationals (deemed export). The license requirement applies to foreign nationals from all countries (licenses are not available for nationals of the People's Republic of China). There are no exceptions for students, postdocs, or short term visitors.

Performing a defense service for the benefit of a foreign person within the U.S. or abroad requires a license under the ITAR. ITAR regulations also contain country based sanctions that relate to the **destination** (Fig. 1) of an export. Exports of defense items to countries under U.S. arms embargos are prohibited <https://www.law.cornell.edu/cfr/text/22/126.1> (e.g. China). .

For more information on ITAR regulations including important definitions and USML categories please see Appendix I.

Department of Commerce Export Administration Regulations (EAR)

The U.S. Department of Commerce Bureau of Industry and Security (BIS) administers the Export Administration Regulations (EAR)⁴. The EAR controls “dual use” items, software, and technology. These are items that have civilian uses (as well as possible military uses in some cases) and may be controlled for reasons other than national security. **Technology classification** (Fig. 1) under the EAR is done through the [Commerce Control List](#)⁵.

Similar to the ITAR, the EAR defines an export as shipment or transfer of controlled items out of the U.S. or the release of controlled technology, technical data or software to a foreign national within the U.S.⁶ The EAR classification of a technology in combination with the destination will determine whether a license is required for export (unless an exception or exemption is available). The Bureau of Industry and Security also maintains an [Entity List](#)⁷, one of the restricted party lists that should be consulted when screening the **end-user** (Fig. 1) for an export. For additional information on the EAR please see Appendix II.

² 22 CFR §§ 120-130

³ 22 CFR §121

⁴ 15 CFR § 730-774

⁵ 15 CFR § 774 Supplement No. 1

⁶ 15 CFR § 734.13

⁷ 15 CFR § 744 Supplement No. 4

Department of Treasury Office of Foreign Assets Control (OFAC)

The Office of Foreign Asset Control (OFAC) administers economic and trade sanctions based on U.S. national security and policy interests and United Nations and international mandates⁸. These programs may be country-based or list-based (weapons of mass destruction proliferation, global terrorism, narcotic trafficking). There are also prohibitions against transactions with specific entities or individuals ([Specially Designated Nationals](#) (SDN)). OFAC licenses are generally required for transactions between a U.S. person or entity and a person or entity on the SDN list, as well as for interactions involving sanctioned countries. Licensable transactions can include financial transactions or the exchange of goods or services. Some transactions may be permitted under a general license and do not need permission from OFAC. In other cases a specific license from OFAC may be required.

OFAC sanctions and restricted party lists are relevant to the **destination** and **end-user** (Fig. 1) aspects of export control. [Sanctions programs](#) should be consulted to determine what types of transactions are prohibited and what are allowed. For more details on OFAC, restricted party screenings, and information on other export control regulations not included here, please see Appendix III.

Penalties

Export of a controlled item without proper authorization (license or license exception) or exports violating the terms of an export license may result in criminal and/or civil penalties of up to 1 million dollars per violation depending on the agency. Penalties may also include seizure of items, loss of export privileges, debarment from participating in future federal contracts, or imprisonment. Penalties may be assessed on the University *and/ or on the individual responsible for the violation (e.g. PI or staff member)*. In some cases multiple violations of related restrictions may apply to a single export, resulting in extremely large fines. Investigation of possible violations may result in disruption of research, especially in cases of possible deemed exports involving foreign nationals on campus. It is important to note that deemed export violations are subject to the same federal penalties as physical exports.

Voluntary self-disclosure of a violation can be a mitigating factor in penalty assessment, reducing penalties up to 50%. In most cases conditions will apply, such as implementing or improving a comprehensive compliance program. For more information on specific penalties by agency and on voluntary self-disclosure, please see Appendix IV.

⁸ 31 CFR §§ 500-599

III. EXPORT CONTROLS AT WASHINGTON UNIVERSITY

INSTITUTIONAL COMMITMENT

As part of its mission to create and transmit knowledge through research, education and patient care, Washington University strives to maintain a diverse and vibrant academic community that welcomes foreign researchers, educators and clinicians and encourages international collaborations for the general advancement of human knowledge. In its Policy on [Open Research And Free Dissemination of Ideas and Information](#), the University affirms its belief that this mission is best served by fostering a culture of academic freedom that promotes the free exchange of ideas and encourages the broadest possible dissemination of knowledge and information through a wide array of research, teaching and clinical activities both within the United States and abroad.

The University also recognizes that the United States government has a legitimate interest in limiting the proliferation of certain technologies and the dissemination of technical data relating to those technologies. The Export Control Laws are a means of protecting this interest. In the university setting, the Export Control Laws apply not only to the physical export of technology and technical data overseas, but also to the deemed export of technical data to foreign nationals within the United States.

The University recognizes the importance of maintaining an effective and comprehensive export control compliance program that can readily adapt to an evolving regulatory environment. The purpose of this Export Management Compliance Program is to affirm the University's commitment to compliance with the Export Control Laws; to promote faculty and staff awareness and understanding of the Export Control Laws as they relate to University activities; and to provide resources to assist faculty and staff with export control issues and compliance.

WASHINGTON UNIVERSITY EXPORT CONTROL POLICY

Applicability

This policy applies to all Washington University investigators, faculty, staff, clinicians, visiting scientists, postdoctoral fellows, students, scholars and any other person working at or for Washington University. The policy sets forth the basic responsibilities that all such persons must meet in conducting their research, teaching, clinical or other activities at or on behalf of the University.

Policy

The [Washington University Export Control Policy](#) prohibits the transfer of any controlled technology, technical data, or services, in violation of the Export Control Laws, whether the transfer occurs inside or outside of the U.S.

ROLES AND RESPONSIBILITIES

The University export control compliance program is administered by the Office of the Vice Chancellor for Research. For an overview of export control administration at Washington University please see the Export Control Compliance Organizational Chart in Appendix V.

The primary individuals and entities and their responsibilities are described here.

University Export Control Manager (ECM)

The University's Export Control Manager (ECM) is responsible for export control oversight, including the development and implementation of procedures to promote the University's ongoing compliance with export control laws and the development of training and education for faculty and staff. The ECM is an Empowered Official and Chair of the Export Control Advisory Committee. Duties include:

- Provide education and guidance to faculty and staff
- Promote a culture of export control awareness and compliance
- Conduct export control reviews
- Oversee restricted party screening processes
- Implement Technology Control Plans
- Submit license applications, classification requests, advisory opinions and act as main point of contact for official communications
- Review H1-B Visa applications for I-129 export control certifications
- Coordinate with other University entities to facilitate export control compliance

Faculty/ Principal Investigator

Faculty and Principal Investigators (PI) will have primary responsibility for assuring that their research and other activities comply with export control regulations. Faculty/PI responsibilities include:

- Understand how the Export Control Laws may affect their activities and when to call the University Export Control Manager (ECM) for Assistance.
- Assure that they and their staff are informed about export controls and the resources available to enable compliance.
- Establish and maintain standards of export control compliance for locations and personnel under their direction.
- Cooperate with the ECM to evaluate and manage potential export control issues such as shipping, travel, and deemed exports.
- Manage access by unlicensed foreign persons to any identified controlled technology or technical data in areas under their supervision that does not qualify for an exclusion to export control regulations. This may require compliance with a Technology Control Plan and/or working with the ECM to obtain an export control license.
- Coordinate and cooperate with the ECM to obtain necessary export control licenses from the appropriate federal agency. If that license is granted with provisos, the PI must ensure that the conditions of the license are met and maintained.
- Contact the ECM for restricted party screening of shipping destinations, foreign travel destinations, and potential collaborators and visitors as necessary.

Senior Official

The Washington University Provost is the senior official representing Washington University to Federal Agencies with export control authority.

Empowered Officials

Empowered officials represent Washington University in official export control matters such as registrations, licensing, commodity jurisdiction and classification requests, and voluntary self-disclosures. They have the authority to sign paperwork binding the university in proceedings with any agency with export control oversight. Washington University has three empowered officials; the Export Control Manager, the Assistant Vice Chancellor and Associate General Counsel, and the Director of the Office of Biological and Chemical Safety (). The primary empowered official is the Export Control Manager.

Export Control Advisory Committee (ECAC)

The Export Control Advisory Committee (ECAC) provides guidance and makes recommendations to University Officials and to the Export Control Manager on export control policies and procedures at Washington University. Members of the ECAC provide input on education and training, compliance programs and policy, technology and tool needs, and provide subject matter expertise in their areas of responsibility. They assist with development of export control compliance action plans and periodic program reviews, and facilitate communication throughout the University community about the importance of export control compliance. The ECAC is chaired by the Export Control Manager. Membership of the ECAC includes representatives of the cooperating entities listed below and includes all three empowered officials.

Cooperating Entities

Many units of the University coordinate with the Export Control Manager (ECM) including the following offices which are represented on the Export Controls Advisory Committee:

Office of Sponsored Research Services (OSRS)

The Office of Sponsored Research Services (OSRS) supports Washington University faculty and administrative personnel in all aspects of their work associated with the proposal and acceptance of research projects with federal, industry and private sources. The OSRS grant team works with the ECM to identify proposed and funded projects with potential export control issues.

Joint Research Office of Contracts (JROC)

The Joint Research Office of Contracts (JROC) facilitates the timely execution of federal contracts, industry supported research agreements, industry supported clinical trials, and other research related agreements. The office works closely with the ECM to identify and resolve potential export control concerns in University research agreements.

Environmental Health and Safety (EH&S)

Environmental Health and Safety (EH&S) provides oversight and consulting in all areas of safety, health and environmental compliance. It includes the Institutional Biological and Chemical Safety Committee (IBC). The IBC oversees research involving recombinant DNA, infectious or potentially infectious agents,

and/or hazardous chemicals. It works closely with the ECM to identify potential biological and chemical export control concerns.

Office of International Students and Scholars (OISS)

The Office of International Students and Scholars (OISS) provides resources and support services to international students and scholars including integration into the U.S., language assistance, and expertise on immigration and visa matters. The OISS conducts restricted party screenings of foreign students and scholars, works closely with the ECM on the I-129 certification process for H-1B Visas, and alerts the ECM to matters of export control concern regarding foreign students, postdoctoral fellows, and visiting scholars.

Accounting Services

Accounting services conducts restricted party screening on new vendors and many foreign transactions.

University Compliance Office (UCO)

The University Compliance Office (UCO) monitors and coordinates the university's many existing compliance efforts, assesses university-wide performance and provides senior leadership and the Audit Committee with an independent, comprehensive view of the university's compliance activities. The Compliance office provides expertise on the development and administration of university compliance programs.

Information Technology (IT)

The Washington University Information Technology offices oversee information technology services and security and work with the ECM on export control issues related to information technology.

Office of Technology Management (OTM)

The mission of the Office of Technology Management (OTM) is to extend the value of Washington University research to the wider community. The objective is to license the university's intellectual property to private entities so the science uncovered in University laboratories may benefit society through direct impact on health and quality of life. OTM coordinates with the ECM for export control guidance when licensing or exporting technology to foreign entities.

Human Resources (HR)

Human Resources (HR) manages recruitment, training and development, compensation and benefits and employee relations for employees of the university. HR works with the ECM when export control issues arise regarding foreign national employees.

Office of General Counsel (OGC)

The Office of General Counsel (OGC) provides ad hoc representation and counsel on a broad range of legal issues affecting the University. The OGC works with the ECM on legal aspects of export control matters. The OGC does not have an official representative on the Export Control Advisory Committee but gives counsel upon request.

IV. EXCLUSIONS FROM EXPORT CONTROL RELEVANT TO UNIVERSITIES

Both the EAR and the ITAR have specific exclusions or exemptions that are applicable to university activities. Most university research and instructional activities fall within these exclusions, however there may be instances when exclusions do NOT apply and export authorization is needed. Exclusions are often similar across agencies but may have subtle differences which must be carefully considered.

PUBLICLY AVAILABLE INFORMATION

The EAR, the ITAR, and OFAC each generally exclude publicly available or published information from export controls. Although similar, there are slight differences in the definition of publicly available information for each agency (see Table 2).

Table 2. Public Information Excluded from Export Controls by Agency.

EAR
<p>§ 734.7 Published information and software.</p> <p>(a) Except as set forth in paragraph (b) of this section, unclassified “technology” or “software” is “published” and is thus not “technology” or “software” subject to the EAR, when it has been made available to the public without restrictions upon its further dissemination such as through any of the following:</p> <ul style="list-style-type: none">(1) Subscriptions available without restriction to any individual who desires to obtain or purchase the published information;(2) Libraries or other public collections that are open and available to the public, and from which the public can obtain tangible or intangible documents;(3) Unlimited distribution at a conference, meeting, seminar, trade show, or exhibition, generally accessible to the interested public;(4) Public dissemination (i.e. unlimited distribution) in any form (e.g. not necessarily in published form), including posting on the Internet on sites available to the public; or(5) Submission of a written composition, manuscript, presentation, computer-readable dataset, formula, imagery, algorithms, or some other representation of knowledge with the intention that such information will be made publicly available if accepted for publication or presentation:<ul style="list-style-type: none">(i) To domestic or foreign co-authors, editors, or reviewers of journals, magazines, newspapers or trade publications;(ii) To organizers of open conferences or other open gatherings. <p>(b) Published encryption software classified under ECCN 5D002 remains subject to the EAR unless it is publicly available encryption object code software classified under ECCN 5D002 and the corresponding source code meets the criteria specified in 15 CFR § 742.15(b) of the EAR.</p>

(c) The following remains subject to the EAR: “software” or “technology” for the production of a firearm, or firearm frame or receiver, controlled under ECCN 0A501, that is made available by posting on the internet in an electronic format, such as AMF or G-code, and is ready for insertion into a computer numerically controlled machine tool, additive manufacturing equipment, or any other equipment that makes use of the “software” or “technology” to produce the firearm frame or receiver or complete firearm

Note: Technology contained in a patent or patent application is also generally excluded from the EAR, see 15 CFR § 734.3(b)(iv).

ITAR

[22 CFR § 120.11 Public Domain](#)

(a) Public Domain means information which is published and which is generally accessible to the public through:

- (1) Sales at newsstands and bookstores;
- (2) Subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information;
- (3) Second class mailing privileges granted by the U.S. government;
- (4) Libraries open to the public or from which the public can obtain documents;
- (5) Patents available at any patent office;
- (6) Unlimited distribution at a conference, meeting, seminar, trade show, or exhibition which is generally accessible to the public, in the United States;
- (7) Public release (unlimited distribution) in any form (e.g. not necessarily in published form) after approval by the cognizant U.S. government department or agency;
- (8) **Fundamental research** in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community. Fundamental research is defined to mean basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. University research will not be considered fundamental research if:
 - (i) The University or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity, or
 - (ii) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable.

OFAC

31 CFR § 560.315 Information and Informational Materials

- (a) The term Information and Informational Materials includes but is not limited to
- Publications
 - Films
 - Posters
 - Phonograph records
 - Photographs
 - Microfilms
 - Microfiche
 - Tapes
 - Compact disks
 - CD ROMS
 - Artworks (*must be classified under chapter subheading 9701, 9702, or 9703 of the Harmonized Tariff Schedule of the United States.*)
 - News wire feeds

EDUCATIONAL INFORMATION

Both the EAR and the ITAR contain provisions which exclude information generally taught in university courses from export control regulations.

Table 3. Definition of “Educational Information” by Agency.

EAR	ITAR
<p>15 CFR § 734.3(b)</p> <p>The following are not subject to the EAR:</p> <p>(3) Information and software that</p> <p>(iii) Are released by instruction in a catalog course or associated teaching laboratory of an academic institution;</p>	<p>22 CFR § 120.10 (b)</p> <p>The ITAR provision regarding educational information is within the definition of technical data and states that technical data</p> <p><i>“does not include</i> information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities or information in the public domain as defined in §120.11 of this subchapter or telemetry data as defined in note 3 to Category XV(f) of part 121 of this subchapter . It also does not include basic marketing information on function or purpose or general system descriptions of defense articles.”</p>

FUNDAMENTAL RESEARCH

The [National Security Decision Directive 189 \(NSDD189\)](#), [National Policy on Transfer of Scientific, Technical and Engineering Information](#) addresses the flow of information produced by federally funded fundamental research at colleges, universities, and laboratories. NSDD 189 defines fundamental research in the following way:

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

Following this definition, if the University or its researchers accept publication, dissemination, or participation restrictions as part of a grant or contract award, or if the sponsoring government agency applies specific access and dissemination controls, the government will not consider the research to be fundamental. The EAR and the ITAR both contain definitions of fundamental research that essentially align with NSDD 189⁹. The ITAR considers fundamental research to fall under “public domain” (see Table 2. ITAR 22 CFR § 120.11 (8)). In addition if research is being provided as a defense service, it is not considered fundamental research under the ITAR.

Grants funded by the National Science Foundation, the National Institutes for Health, and many foundations are typically fundamental research. The results of fundamental research under both the ITAR and the EAR are excluded from export control regulations¹⁰.

The Fundamental Research Exclusion

The results of fundamental research under both the ITAR and the EAR are excluded from export control regulations¹¹.

Washington University is primarily a fundamental research institution. Restrictions on publication or participation which would prevent applicability of the Fundamental Research Exclusion are only accepted with written permission from the Vice Chancellor for Research and the Dean of the relevant school. In such cases, once all sponsor restrictions are lifted and the results can be freely disseminated, the Fundamental Research Exclusion can be applied.

FULL-TIME UNIVERSITY EMPLOYEES

The ITAR provides that unclassified technical data in the U.S. can be disclosed by U.S. institutions of higher learning to a foreign person who is the university’s bona fide and full-time regular employee if:

- The employee’s permanent abode throughout their period of employment is in the U.S.
- The employee is not a national of a prohibited country under [22 CFR § 126.1](#)
- The University informs the individual in writing that they are prohibited to transfer the technical data to other foreign persons without prior written approval of DDTC¹²

⁹ EAR 15 § CFR 734.8; ITAR 22 CFR § 120.11 (8)

¹⁰ EAR 15 § CFR 734.3(b)(3)(ii); ITAR 22 CFR § 120.11 (8)

¹² 22 CFR § 125.4(b)10

¹² 22 CFR § 125.4(b)10

This provision only applies to information disclosed by the University to the employee. This exemption does NOT apply in cases where a third party, for example an industry sponsor, wishes to disclose export controlled information to the employee. In this case an export license may be needed. The provision also does not apply to students.

V. WASHINGTON UNIVERISTY PROCESSES AND PROCEDURES

Restricted Party Screening

“Restricted Party Screening” (RPS) refers to the screening of individuals and entities against a set of restricted party lists and country sanctions. Restricted party screening is conducted using University provided commercial software or by consulting the government [Consolidated Screening List](#). Authorized personnel from several university offices conduct RPS after training by the Export Control Manager (ECM.) The ECM administers the screening program.

Table 4. Restricted Party Screening Processes at Washington University.

Who is screened?	What office performs the screening?
Visa applicants sponsored by the university	Export Control (H-1B), Office of International Students and Scholars (other)
New vendors; foreign financial transactions	Accounting Services
Foreign parties to research contracts and service agreements, foreign subawards	Joint Research Office of Contracts, Office of Sponsored Research Services, Export Control
Foreign parties to Material Transfer and Licensing Agreements	Environmental Health and Safety (biological and chemical), Export Control Manager
Foreign recipients of tangible exports*	Environmental Health and Safety (biological and chemical), Export Control(other)
Personnel authorized in a Technology Control Plan	Export Control

*Principal Investigators are responsible to contact the ECM for restricted party screening of international shipping destinations, travel destinations, and foreign visitors (if visitors are not being otherwise processed through the Office of International Students and Scholars).

Export Control Review

Principal Investigators (PI) and department personnel may contact the Export Control Manager (ECM) and request an export control review at any time. Laboratories and departments may also be selected by the ECM for review based on the type of research conducted or technology being used. Export control reviews are conducted by the ECM. The ECM will, in consultation with the Principal Investigator or staff member, evaluate the following questions:

1. Does the research fall under the Fundamental Research Exclusion?
2. Is the technology or technical data subject to export control regulations?
3. If yes, what is the classification of the technology or technical data under the EAR or ITAR?
4. Do individuals who will access the technology or technical data, or the destination of said technology if a physical export, require an export license under the EAR or the ITAR?
5. Is a management plan (Technology Control Plan; TCP) necessary to protect access to the technology or technical information? If so the ECM will develop and implement the TCP in consultation with the PI.
6. Are any individuals or entities that will receive or have access to the items restricted parties? The ECM will conduct restricted party screening.
7. Are any of the countries involved sanctioned or embargoed?

Faculty and staff are encouraged to use the [decision tree](#) in figure 2. If any questions are answered “Yes” or “I don’t know”, the Export Control Manager should be consulted.

EXPORT CONTROL DECISION TREE

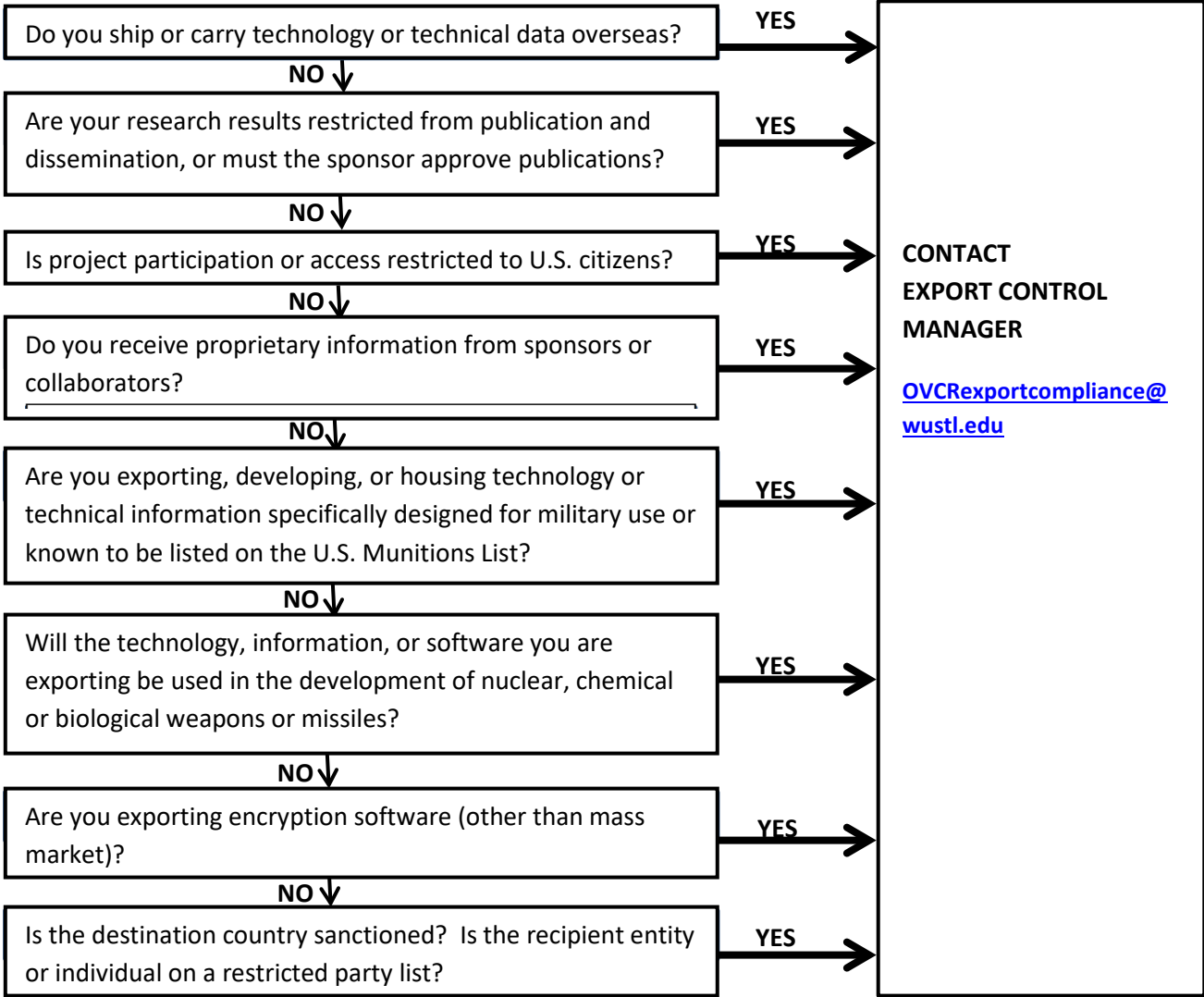


Figure 2. Export Control Decision Tree

Export control reviews may also be triggered by the following circumstances:

Sponsored Research

Export control review may be triggered when the institution submits a proposal, receives an award, or is negotiating a contract. Staff in the Office of Sponsored Research Services (OSRS) and the Joint Office of Research Contracts (JROC) watch for the following red flags which indicate possible export control issues

- Restrictions on publication or dissemination of research results
- References to U.S. export control regulations (beyond a statement of general compliance)
- Restrictions on participation or access

- Assertions that proprietary information will be provided by sponsor
- Military application of results with no “civil” or “dual” use
- Involvement of foreign military
- Involvement of foreign sponsors

Projects which are flagged are referred to the Export Control Manager (ECM) for review. The ECM reviews the project for specific export control issues and works with the contract manager and the Principal Investigator (PI) to negotiate acceptable export control terms and conditions with the sponsor. If the export control issues cannot be eliminated the ECM will work with the PI to implement a Technology Control Plan or apply for a license to ensure compliance with export control regulations.

The vast majority of research conducted at Washington University is fundamental research. Fundamental research projects will be reviewed if one of the following occurs:

- There is an identified need to export technology or technical data overseas.
- Instruments and individuals involved in the conduct of the research meet criteria which trigger the need for a deemed export license (e.g. ITAR).
- Sponsor indicates that information being provided to the university is proprietary and export controlled.

Material Transfer Agreements and Licensing Agreements

Material transfer agreements (MTA) and licensing agreements are handled by personnel in the Office of Technology Management (OTM). MTAs and Licensing agreements involving foreign entities are sent to the ECM for review and restricted party screening.

H-1B Visa Applicants

Export control reviews will be triggered when the University sponsors a foreign student or scholar on an H1-B visa. A preliminary export control questionnaire (see Appendix VII) is filled out by the scholar’s supervisor and is reviewed by the Export Control Manager (ECM). The ECM follows up with the supervisor if necessary and makes a recommendation to the Office of International Students and Scholars (OISS) of whether an export control license is anticipated to be needed for the foreign national’s activities on campus. This recommendation is then used by the OISS to complete the I-129 form. OISS may also request export control reviews be done for individuals applying for other classes of visas, for example a visiting J-1 scholar from a sanctioned country. OISS conducts restricted party screening on applicants for all Visa categories. Potential matches go to the ECM for verification. The ECM conducts the restricted party screening on H-1B visa applicants and other visa applicants for which an export control review is conducted.

Shipping

University personnel are responsible for contacting the ECM prior to shipping items overseas. The ECM will conduct a review to determine the export status of the item, whether a license is needed, or whether a license exception is available. The ECM also conducts restricted party screening on the shipping destination and recipient. In cases of biological and chemical exports, export control review and restricted party screening are conducted by an authorized individual from the Office of Environmental Health and Safety and/ or the ECM. Potential restricted party matches are reviewed by the ECM.

Purchases

Purchasing personnel alert the ECM if indications that an item is export controlled are identified. Export control education programs provided to faculty and staff by the ECM emphasize red flags to look for when purchasing technology that indicate an item is export controlled. The University's standard vendor contract requires vendors to notify the ECM and receive written authorization of acceptance before delivering any ITAR controlled items to campus (see Appendix VIII). If the ECM is notified of an ITAR purchase, a review will be conducted in order to assure that access controls are in place before delivery of the item to campus.

Additional Reviews

The Export Control Manager (ECM) may choose to review selected laboratories or Departments at any time based on their activities or their technology. In general the ECM will meet with an appropriate staff member who is knowledgeable about the technology in use in that area. Potential export control issues will be evaluated by the ECM and if indicated a plan will be developed for either license submission or implementation of a Technology Control Plan.

Protecting Export Controlled Technology from Unauthorized Access

Technology Control Plans (TCP)

In cases where it is determined that export controlled technology or technical information must be protected from unauthorized foreign national access, a Technology Control Plan (TCP) is developed by the Export Control Manager (ECM) in consultation with the Principal Investigator (PI). A TCP is a formal document that outlines the procedures that will be used to protect access to controlled technology or technical information. The TCP typically includes

- A statement of commitment to export control compliance by the University;
- Identification of the primary responsible parties;
- Identification and description of the project;
- Identification of the items or technologies and the applicable classification and controls;
- A physical security plan;
- An information security plan; and
- Names and nationalities of all personnel granted access to the item/information

TCPs must be read and signed by all personnel with authorized access to the controlled technology or technical data. An additional briefing on export controls including a statement of understanding and commitment must be read and signed by authorized personnel. Restricted party screening is conducted by the ECM on all personnel included on the TCP before implementation. It is the responsibility of the Principal Investigator (PI) and the personnel listed on the TCP to ensure that the conditions of the TCP are followed and to notify the ECM of any changes (locations, protocols, personnel, materials). Protocol changes must be approved by the ECM. Periodic reviews (approximately yearly) are conducted of all TCPs by the ECM. Records related to TCPs will be maintained by the ECM for five years after the TCP is closed out. A TCP and briefing template may be found in Appendix IX of this manual.

Licensing

Export licenses may be required for physical exports, deemed exports, or transactions with restricted entities or embargoed countries. In the case of deemed exports, licenses are specific to foreign nationals, and each individual foreign national requires a separate license. For example if there is one ITAR controlled item in a laboratory and there are four foreign national graduate students in that laboratory who need access to that item, four separate export control licenses will be necessary, one for each foreign national.

1. In order to determine if a license is required, the following information must be provided by the requestor to the Export Control Manager (ECM):
 - Technology description (Manufacturer, make, model, and purpose in layman's terms). This will facilitate classification of the technology by the ECM.
 - Destination
 - Country
 - Institution
 - End User (full name)
 - End use
2. License applications are submitted on behalf of the University by the Export Control Manager or other empowered official.
3. Licenses are granted by the government agency to the University; however the Principal Investigator (PI) is responsible for ensuring that any provisos of the license are followed.
4. Documentation (e.g. shipping records) must be maintained by the PI and a copy submitted to the ECM.

Records and Record Retention

Records will be maintained in accordance in a manner consistent with applicable law, and in accordance with plans developed by the schools, departments, and other units that maintain University Records.

Training

Presentations on the basics of export controls are conducted by the ECM at faculty and staff meetings across the university on a periodic basis. The ECM will conduct training sessions with any group upon request, and often meets one-on-one with investigators. Extensive information on export controls can be found on the university Office of the Vice Chancellor for Research website and is accessible to all University personnel. <http://research.wustl.edu/ComplianceAreas/ExportControl/Pages/default.aspx>.

Audits

The University Compliance Office verifies that effective compliance is occurring in all university activities governed by federal laws and regulations or by University policy. University audits of internal compliance programs are generally conducted every three to five years.

Detecting and Reporting Violations

Any individual who suspects that an export control violation has occurred should notify the University through one of several channels:

- Contact the Export Control Manager directly at OVCRExportCompliance@wustl.edu
- Call the University Compliance hotline at 314-362-4998
- Submit the online reporting form
<http://universitycompliance.wustl.edu/code-of-conduct/online-reporting-form/>.

Individuals may report anonymously. The Export Control Manager will investigate the suspected violation by gathering information and will review the case in conjunction with the Office of General Counsel and the University Compliance Office to determine if a violation has occurred and if subsequent self-disclosure to a government agency is needed. If it is determined that a self-disclosure is needed the disclosure will be handled and submitted by the Export Control Manager, senior official and other empowered officials.

APPENDIX I

Department of State International Traffic in Arms Regulations

Regulatory Authority and Scope

The Arms Export Control Act (AECA)¹³ grants authority to the president of the U.S. to regulate the export and import of defense articles and services. The President has delegated this responsibility to the Secretary of State.¹⁴ The Department of State Directorate of Defense Trade Controls (DDTC) administers these controls through the International Traffic in Arms Regulations (ITAR)¹⁵ and lists the designated articles on the United States Munitions List (USML).¹⁶

Items Controlled under the ITAR

The USML includes defense articles and associated technical data. It is important to note that these items were designed for military purposes and that they are controlled for export regardless of how they are being used on campus. ITAR controlled items require licenses from the DDTC for physical export or for technology release to foreign nationals within the U.S. (deemed export). The license requirement applies to foreign nationals from all countries, and includes students and postdoctoral fellows. No licenses are available for nationals from the People's Republic of China.

USML Categories

The USML defines twenty one classes of defense articles¹⁷. Below is a list of category headings. The full regulations including the USML can be accessed at

<https://www.govinfo.gov/content/pkg/CFR-2016-title22-vol1/xml/CFR-2016-title22-vol1-chap1-subchapM.xml>

[or for a slightly more user friendly version, see](#)

<https://www.law.cornell.edu/cfr/text/22/chapter-1/subchapter-M>

Category I-Firearms, Close Assault Weapons and Combat Shotguns

Category II-Guns and Armament

Category III-Ammunition/Ordnance

Category IV-Launch Vehicles, Guided & Ballistic Missiles, Rockets, Torpedoes, Bombs and Mines

Category V-Explosives and Energetic Materials, Propellants, Incendiary Agents and Constituents

Category VI-Surface Vessels of War and Special Naval Equipment

Category VII-Ground Vehicles

Category VIII-Aircraft and Related Articles

Category IX-Military Training Equipment and Training

Category X-Protective Personnel Equipment and Shelters

Category XI-Military Electronics

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

Category XIII-Materials and Miscellaneous Articles

¹³ 22 USC 2778, Chapter 39

¹⁴ Executive order 11958

¹⁵ 22 CFR §§ 120-130

¹⁶ ITAR §121

¹⁷ 22 CFR §121

Category XIV-Toxicological Agents, including Chemical and Biological Agents, Associated Equipment
Category XV-Spacecraft Systems and Associated Equipment
Category XVI-Nuclear Weapons Design and Testing Related Items
Category XVII-Classified Articles, Technical Data and Defense Services Not Otherwise Enumerated
Category XVIII-Directed Energy Weapons
Category XIX-Gas Turbine Engines and Associated Equipment
Category XX-Submersible Vessels and Related Articles
Category XXI-Articles, Technical Data, and Defense Services Not Otherwise Enumerated

Exporting Under the ITAR

Transferring defense articles outside of the U.S., disclosing or transferring technical data to foreign nationals within the U.S., or performing a defense service for the benefit of a foreign person within the U.S. or abroad constitute an export under the ITAR¹⁸. In cases where technology is released to a foreign national within the U.S., the export is deemed to occur to *all* countries that foreign national has held or holds citizenship or permanent residency.

If there is doubt as to whether an item is controlled under the ITAR, an empowered official can submit a written “Commodity Jurisdiction” request to the DDTC, which will determine which regulations apply (EAR or ITAR). U.S. entities wishing to export ITAR controlled articles must be registered with the DDTC¹⁹. Registration is required in order to apply for ITAR export licenses.

The ITAR also contains country-based prohibitions²⁰, prohibiting exports to countries under embargos. For example China is under a U.S. arms embargo with a current policy of denial for license requests. It is not possible to obtain a license for an ITAR export or deemed export to China. These embargoes are subject to change and can be checked at https://www.pmdotc.state.gov/embargoed_countries/?id=ddtc_public_portal_country_landing/. Also see [ITAR §126.1](#).

Important ITAR Definitions

Defense Article²¹ refers to anything listed on the U.S. Munitions List and related technical data. It may also include articles that provide the equivalent performance capabilities of a defense article on the USML. It does not include basic marketing information on function or purpose or general system descriptions.

Defense Service²² means the furnishing of assistance (including training) to foreign persons, whether in the U.S. or abroad, in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles. It also includes the furnishing to foreign persons of ITAR controlled technical data and military training of foreign units and forces, regular and irregular, including formal or informal instruction in the U.S. or abroad or by correspondence courses, technical, educational or information publications and media of all kinds, training aid, orientation, training exercise, and military advice.

¹⁸ 22 CFR §120.17

¹⁹ 22 CFR §122.1

²⁰ 22 CFR §126.1

²¹ 22 CFR §120.3

²² 22 CFR §120.9

Release²³ (a) Visual or other inspection by foreign persons of a defense article that reveals technical data to a foreign person or (b) oral or written exchanges with foreign persons of technical data in the U.S. or abroad.

Technical Data²⁴ refers to information other than software²⁵ which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation. Technical data also includes classified information relating to defense articles or services or to 600 series items on the Commerce Control List, information covered by an invention secrecy order, or software directly related to defense articles.

²³ 22 CFR §120.50

²⁴ 22 CFR §120.10

²⁵ as defined in CFR § 120.10(a)(4)

APPENDIX II

Department of Commerce Export Administration Regulations (EAR)

Regulatory Authority and Scope

The U.S. Department of Commerce Bureau of Industry and Security administers the EAR under the Export Administration Act (EAA) of 1979²⁶, as amended. This act has lapsed but its authority has been extended by Presidential Executive Orders under the International Emergency Economic Powers Act (IEEPA)²⁷. The EAR controls “dual use” items, software, and technology. These are items that have civilian uses (as well as possible military uses in some cases) and may be controlled for reasons other than national security.

Items Controlled under the EAR

The EAR is traditionally described as controlling “dual use” items which have both military or strategic and civilian uses. However, the EAR also controls items with strictly civilian uses, and some military items which have been transferred from the ITAR as part of export control reforms. Generally all items of U.S. origin or located in the U.S. are controlled by the EAR unless under the jurisdiction of another regulatory agency. Items specifically controlled by the Departments of State (ITAR), Treasury, Energy, Nuclear Regulatory commission and the Patent and Trademark Office are excluded from the scope of the EAR²⁸.

The [Commerce Control List \(CCL\)](#)²⁹ identifies items subject to specific EAR control and license requirements. It is divided into 9 categories. Items are given an Export Control Classification Number (ECCN) composed of the category number, a letter, and three additional numbers (for example 1C350).

Commerce Control List Categories

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

The second character, a letter, indicates the type of item controlled (A-E). Each CCL Category is subdivided into five (5) Groups:

- (A) Equipment, assemblies, and components
- (B) Test, inspection and production equipment

²⁶ 15 CFR Chapter VII, Subchapter C

²⁷ PL 95-223; 50 USC 1701 *et seq.*

²⁸ 15 CFR §734.3(b)(1)

²⁹ 15 CFR §774 Supplement 1

- (C) Materials
- (D) Software
- (E) Technology

For example, ECCN 1C350 indicates that it is in Category 1, “Materials, Chemicals, Microorganisms, and Toxins”, and the item type is C, “Materials”.

Each ECCN has unique licensing requirements. Items that are subject to the EAR but that do not have specific licensing requirements are categorized as EAR99. EAR99 items have very few controls and are mainly of concern when dealing with sanctioned or embargoed countries, restricted entities, or a prohibited end-use. In the event of an incorrect classification, the exporter is liable for resulting violations.

Exporting under the EAR

Similar to the ITAR, the EAR defines an export as shipment or transfer of items out of the U.S. or the release of technology or source code to a foreign national within the U.S.³⁰ Release of technical data or source code to a foreign national within the U.S. is considered a deemed export. In contrast to the ITAR, under the EAR a deemed export is considered to be an export to only the *most recent* country of citizenship or permanent residency of the foreign national.

Important EAR Definitions³¹

Development

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

Production

All production stages, such as: product engineering, manufacture, integration, assembly (mounting), inspection, testing, quality assurance.

Re-export

Shipment or transmission of an item subject to the EAR from one foreign country to another foreign country, including the sending or taking of an item to or from such countries in any manner. For full definition see 15 CFR § 734.14.

Release³²

Visual or other inspection by a foreign person of items that reveals “technology” or source code subject to the EAR to a foreign person: or oral or written exchanges with a foreign person of “technology” or source code in the U.S. or abroad. Any act causing the “release” of “technology” or software through use of “access information” or to yourself or another person requires an authorization to the same extent an authorization would be required to export or re-export such “technology” or software to that person.

Required

As applied to “technology” or “software”, refers to only that portion of “technology” or “software” which is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or

³⁰ 15 CFR § 734.2

³¹ 15 CFR § 772.1

³² 15 CFR § 734.15

functions.

Technical assistance

May take forms such as instruction, skills, training, working knowledge, consulting services. 'Technical assistance' may involve transfer of 'technical data'.

Technical data

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

Technology

Information necessary for the "development," "production," "use," (operation, installation, maintenance, repair, overhaul, or refurbishing or other terms specified in ECCNs on the CCL that control "technology" of an item). "Technology" not elsewhere specified on the CCL is designated as EAR99, unless the "technology" is subject to the exclusive jurisdiction of another U.S. Government agency or is otherwise not subject to the EAR. "Technology" may be in any tangible or intangible form, such as written or oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, electronic media or information revealed through visual inspection.

Use

Operation, installation, maintenance , repair, overhaul and refurbishing.

Determining License Requirements under the EAR

Once the ECCN has been determined the license requirements can be determined. The reasons for control affect which country destinations will need licenses. More than one reason may apply. These reasons include:

- Anti-Terrorism (AT)
- Chemical & Biological Weapons (CB)
- Crime Control (CC)
- Chemical Weapons Convention (CWC)
- Encryption Items (EI)
- Firearms Convention (FC)
- Missile Technology (MT)
- National Security (NS)
- Nuclear Nonproliferation (NP)
- Regional Security (RS)
- Short Supply (SS)
- Computers (XP)
- Significant Items (SI)

For details and the complete list see [15 CFR §742](#). The most common reasons for controls are AT, NP and NS. After the controls are determined (for example AT1), the user must refer to the [Country Control Chart](#)³³. If the country in question has an "X" in the appropriate column (e.g. AT1) then an export to that country will require a license from the Department of Commerce Bureau of Industry and Security (BIS).

³³ 15 CFR §738 Supp 1

The ECCN listing will give detailed information on reasons for control and possible license exceptions that are available. University personnel wishing to determine technology classification and license requirements should contact the Export Control Manager for an export control review.

License Exceptions

The EAR contains a number of exceptions that may be used in some cases. The details of each case as well as the notes on applicable license exceptions listed in the ECCN must be reviewed to ensure correct interpretation and use of license exceptions. Descriptions of all license exceptions can be found at [15 CFR § 740](#).

Two exceptions which can at times be used for temporary exports are “BAG” and “TMP”. U.S. persons or authorized foreign persons may take personal devices out of the U.S. under the “BAG”³⁴ exception and University owned devices under the “TMP”³⁵ exception, *if*:

- The device will be returned to the U.S. within 12 months
- The device and technology will remain in the traveler’s effective control throughout the trip (in physical possession or in a secured space e.g., hotel safe)
- Controlled technology is not released or shared while overseas
- Traveler takes responsibility for preventing inadvertent releases. Use secure connections, a password to protect technical data, and firewalls.
- The device does not contain non-mass-market encryption applications or software
- The device does not contain defense related items and will not be used to support or assist foreign military or space programs
- The device, technology, or software will not be directly or indirectly used for nuclear activity

Additional restrictions may apply and these exceptions cannot be used in all circumstances. There may be recordkeeping and notification requirements. University personnel should contact the Export Control Manager regarding license exceptions.

³⁴ 15 CFR §740.14

³⁵ 15 CFR §740.9

APPENDIX III
Department of Treasury
Office of Foreign Assets Control (OFAC)
And Other Regulations

The Office of Foreign Asset Control (OFAC) administers economic and trade sanctions based on U.S. national security and policy interests and United Nations and international mandates³⁶. These programs may be country-based or list-based (weapons of mass destruction proliferation, global terrorism, narcotic trafficking). Transactions are generally prohibited between a U.S. person or entity and a person or entity in a sanctioned country (e.g. Iran, Syria, Sudan, North Korea) without a license from OFAC.

There are also prohibitions against transactions with specific entities or individuals (Specially Designated Nationals (SDN)). An OFAC license is generally required for transactions between a U.S. person or entity and a person or entity on the SDN list. Transactions can include financial transactions or the exchange of goods or services.

Both country based sanctions and the [SDN list](#) are subject to change. Specific OFAC [sanctions programs](#) determine what types of transactions are prohibited and what are allowed. Some transactions may be permitted under a general license which does not need permission from OFAC. In other cases a specific license from OFAC may be required. University personnel should contact the Export Control Manager for assistance in determining sanction and restriction applicability.

Restricted Persons

Several agencies in addition to OFAC maintain lists of individuals or entities that are barred from certain transactions with U.S. persons or entities. A U.S. Government "[Consolidated Screening List](#)" search engine is available. The Consolidated Screening list includes, but is not limited to the following lists:

- Specially Designated Nationals and Blocked Persons List (OFAC)
- Persons Named in General Orders
- AECA Debarred List (Department of State)
- Denied Persons List (BIS)
- Entity List (BIS)
- Unverified List (BIS)
- Nonproliferation Sanctions (Department of State)

Third party subscription services are also available for screening of restricted party lists ("restricted party screening" or "RPS").

Anti-Boycott Regulations

Anti-Boycott regulations are administered by the BIS (EAR) and can be found at 15 CFR 760. The "antiboycott" laws are the 1977 amendments to the Export Administration Act (EAA)³⁷ and the Ribicoff Amendment to the 1976 Tax Reform Act (TRA)³⁸. Both of these provisions are designed to prevent any U.S. person or entity, whether in the U.S. or abroad, from participating directly or indirectly in a foreign boycott that is not sanctioned by the U.S. This prevents U.S. entities from inadvertently supporting

³⁶ 31 CFR §§ 500-599

³⁷ PL 96-72

³⁸ PL 94-455

foreign policies of other nations which may run counter to U.S. foreign policy. The regulations were implemented in response to the Arab League's boycott of Israel; however they apply to all boycotts imposed by foreign countries that are not sanctioned by the U.S.

Conduct that may be penalized under the TRA and/or prohibited under the EAR includes:

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

The TRA does not "prohibit" conduct, but denies tax benefits ("penalizes") for certain types of boycott-related agreements.

Exceptions

There is a provision which does allow exporters to comply with the import restrictions of a boycotting country under certain circumstances. Details of exceptions can be found at 15 CFR § 760.3.

Reporting Requirements and Penalties

Both the EAR and TRA require reporting of requests received to support unsanctioned foreign boycotts³⁹. Even if the request is refused or the language in the contract is changed, the initial request must be reported. Reporting procedures and additional information on anti-boycott regulations can be found on the BIS website: <https://www.bis.doc.gov/index.php/enforcement/oac> .

Other Export Regulations

Other agencies with regulations affecting export include but are not limited to:

- Nuclear Regulatory Commission, Office of International Programs
 - Nuclear materials and equipment
 - Regulations: 10 CFR § 110
 - Website: <http://www.nrc.gov/>
- Department of Energy, Office of Export Control Policy & Cooperation
 - Nuclear technologies and service which contribute to the production of special nuclear material
 - Regulations: 10 CFR § 810
- Department of Justice, Drug Enforcement Administration
 - Drugs of abuse, chemicals, precursors
 - Regulations: 21 CFR § 1311-1313
- Website: <https://www.dea.gov/Food and Drug Administration>
 - Drugs, biologics, medical devices

³⁹ 15 CFR § 760.5

- Regulations: 21 CFR § 301 et seq. 21 CFR § 312.1106
 - Website: <http://www.fda.gov/>
- Department of the Interior
 - Endangered species
 - Regulations: 50 CFR § 17.21-22, § 17.31-32
 - Website: <https://www.doi.gov/>

APPENDIX IV Penalties

Export of a controlled item without proper authorization (license or license exception) or exports violating the terms of an export license may result in criminal and/or civil penalties for the university *and/or the responsible individual (e.g. the PI)*. In some cases multiple violations of related restrictions may apply to a single export, resulting in extremely large fines. Penalties may include seizure of items, loss of export privileges, debarment from participating in future federal contracts, or jail time. It is important to note that deemed export violations are subject to the same federal penalties as physical exports. Penalties are subject to change. Details listed below were current as of 2017. For updated penalties please follow footnotes or consult the relevant agency.

Defense Articles & Technical Data

Under the ITAR and the AECA willful violations of defense controls can incur criminal penalties of up to \$1,000,000 per violation and/or up to 20 years of imprisonment for the person committing the violation⁴⁰. Civil penalties of up to \$500,000 per violation may also be assessed by the Secretary of State⁴¹.

EAR Controlled Technology

Under the EAR criminal penalties can reach \$1,000,000 per violation and civil penalties can reach \$250,000⁴². Imprisonment of responsible individuals can be up to 20 years.

Anti-Boycott

The Export Administration Act (EAA) provides for criminal penalties for Anti-Boycott regulations to include fines of up to \$50,000 and imprisonment of up to 10 years. When the EAA is in lapse, the International Emergency Economic Powers Act (IEEPA) provides for penalties of up to the greater of \$250,000 per violation or twice the value of the transaction for administrative violations, and up to \$1 million and 20 years in prison for criminal violations⁴³.

OFAC

Criminal violations may be fined up to \$1,000,000 per violation and up to 20 years imprisonment. Civil violations have a maximum penalty of \$250,000 per violation³⁰.

Voluntary Self-disclosure

Voluntary self-disclosure of a violation can be a mitigating factor in penalty assessment, reducing penalties up to 50%. In most cases certain conditions apply, such as implementing or improving a comprehensive compliance program. Other factors which potentially affect penalty assessment include:

- If this was a first offense
- If there was a compliance program in place
- If steps were taken after discovery of the violation to correct gaps in the compliance program
- Cause of the violation; e.g. misapplication of laws, mistake of fact
- Was the violation willful or intentional
- Were steps taken to hide the violation

⁴⁰ 22 CFR § 127, 22 USC§ 2778(c), 2780(j)

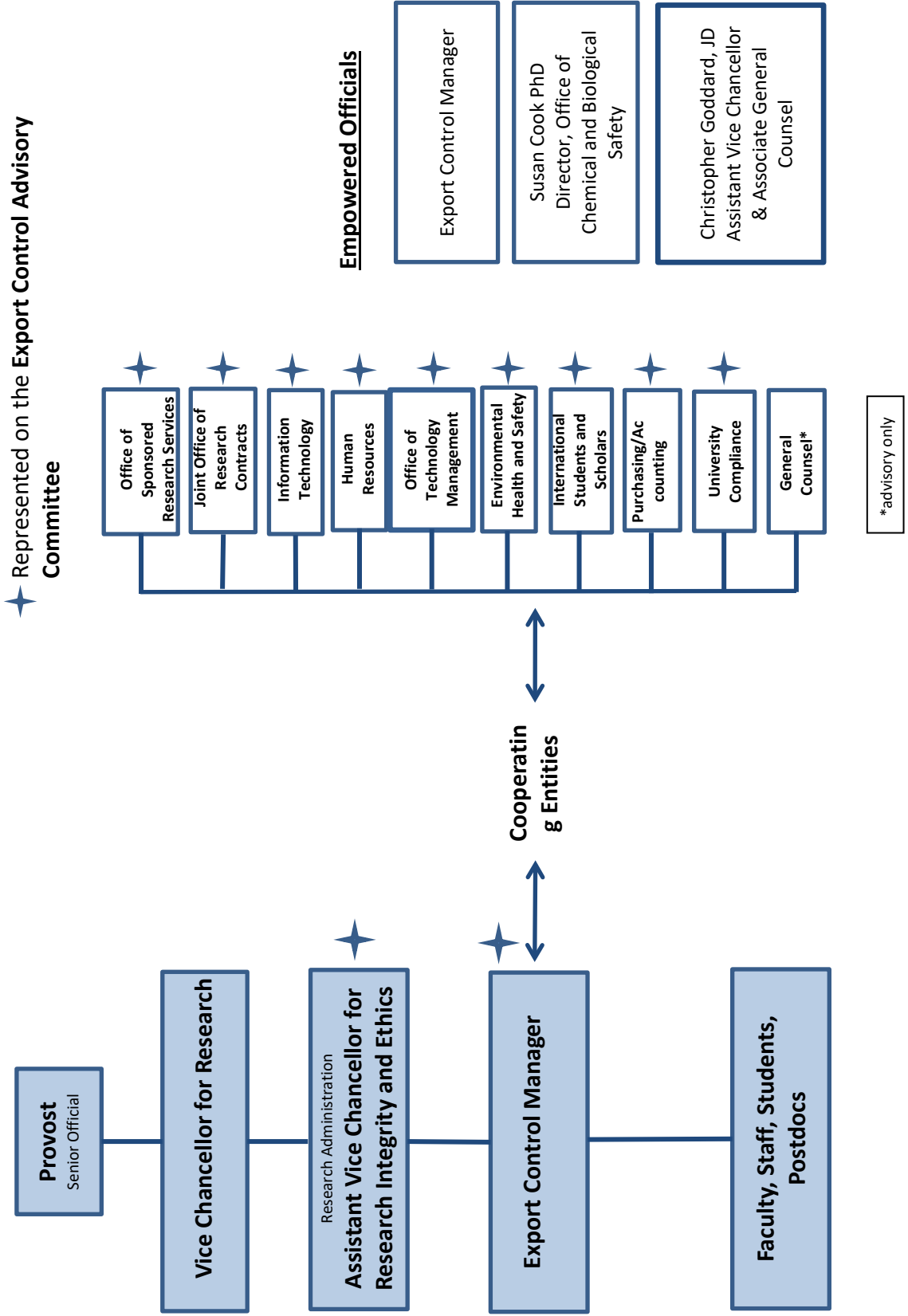
⁴¹ 22 USC § 2778(e)

⁴² PL 110-96

⁴³ PL 95-223; 50 USC 1701 *et seq*

Information on the process of voluntary self-disclosure can be found at 15 CFR § 764.5 of the EAR and 22 CFR § 127.12.

APPENDIX V EXPORT CONTROL COMPLIANCE ORGANIZATIONAL CHART Washington University in St. Louis



APPENDIX VI
Export Control Questionnaire

Name of Foreign National (FN): _____

Is this a renewal of a current H-1B Visa for employment at Washington University in the same position and job title? Yes No

IF YES, ANSWER QUESTIONS IN SECTION A ONLY. IF NO, PLEASE BEGIN AT SECTION B.

A. Renewal of Current Visa

A.1. Has there been any change in role or duties of the foreign national (FN) since the last Visa approval?

Yes No

If yes, please describe what has changed.

A.2. Are there any new or alternate funding sponsors for the work this FN will be doing since the last Visa approval? If yes, please list (e.g. NIH, NSF, Foundation...)

Yes No

A.3. Are there any changes in foreign collaborations since the last Visa approval? If yes, please describe and list the countries involved.

Yes No

A.4. Will the FN have access to any significant new equipment, materials, software, or technology since the last Visa approval? If yes, please describe.

Yes No

A.5. Are there any new publication restrictions on the work the FN will be doing?

Yes No

A.6. Are there any new citizenship requirements or restrictions on participation by foreign nationals for the work this FN will participate in since the last Visa approval?

Yes No

****IF YOU HAVE ANSWERED SECTION A, YOU MAY SKIP SECTIONS B, C, and D and PROCEED TO THE SIGNATURE SECTION ON THE LAST PAGE.****

B. General Information – Please answer to the best of your ability based on your current knowledge of the anticipated activities of the foreign national.

B.1 The Foreign National's work will include **(mark all that apply)**:

- Clinical Research
- Patient Care
- Basic Research
- Technician/Technical Support
- Teaching/Educational Activities
- Other (please describe)

B.2 Who is the funding sponsor for the project/employment of the foreign national (FN)?
Please identify specific sponsors (e.g. NIH, NSF, foundation, industry).

B.3 Will the FN participate in activities which involve the receipt of proprietary information from a sponsor?

Yes No

If yes, what type? (e.g. drug information from a pharmaceutical company)

To your knowledge is this proprietary information export controlled?

Yes No

B.4 Does the FN's work involve the design or development of encryption?

Yes No

B.5 Will the FN participate in any projects known to be export controlled?

Yes No

B.6 Will the FN participate in any projects involving Controlled Unclassified Information (CUI)?

Yes No

If yes please give a project identifier (e.g. grant or contract number).

B.7 Will the FN be working in or near a space where there is a Technology Control Plan in place?

Yes No

B.8 Will the FN's work involve collaborations outside the US?

Yes No

If yes, with what countries?

B.9 Will the FN participate in projects funded by the U.S. Military (e.g DOD) or which have direct military applications?

Yes No

If yes please give a project identifier (e.g. grant or contract number) and attach documentation that briefly describes the aims of the project, for example the abstract or scope of work.

B.10 To your knowledge is the FN a member of or connected to a foreign military?

Yes No

B.11 Does the FN still maintain an official connection to a foreign institution (e.g. has an official position, is enrolled as a student, or receives funding support from)

Yes No

If yes, please name the institution and country and describe the connection.

C. Access to Possible Controlled Items

C.1. Are you aware of any equipment, materials, software, technical data, or encrypted software or hardware that would be export licensable under the **International Traffic in**

Arms (ITAR) Regulations or the **Export Administration Regulations (EAR)** that the FN would have access to (including in an open/shared lab or office environment)?

Yes No

If yes, please indicate the type(s) of item that is (are) export controlled.

C.2. Will the FN have access to any equipment, material, software, or technical data (directly or through unrelated projects occurring in an open lab or office environment) which have been or are currently being specifically designed, developed, configured, adapted, or modified for a military, satellite, or space application?

Yes No

If yes, please explain:

C.3. Please indicate the types of significant equipment the FN will be utilizing or developing in connection with his/her/their position. (e.g., examples include high speed, underwater or infra-red cameras, high-technology electronic sensors, unmanned aerial vehicles (UAVs) spectrographic instruments, chromatography instruments).

C.4. For any of the items described in question C.3., will the FN have access to technical information which would enable them to do **all six** of the following tasks: installation; operation; maintenance; repair; refurbishing; overhaul. (**Note: if they are only operating and maintaining the instrument, the answer is "No"**).

Yes No

If yes, for which instruments will they have access to this information?

D. Determination of Fundamental Research Status **If you checked ONLY Clinical Research Patient Care, and/or Teaching/Educational Activities, you may skip section D and proceed to signature.**

D.1. Please read the U.S. Government's definition of Fundamental Research: *“Fundamental Research means basic and applied research in science and engineering the results of which ordinarily are published and shared broadly within the scientific community as distinguished from proprietary research and industrial development, design, production and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons”*

Do you consider the work this FN will be doing to be “Fundamental Research?”

Yes No

D.2. Will the FN participate in any activities or projects that contain restrictions (formal or informal) on publication or presentation of results in any way beyond a brief review by an industry sponsor for elimination of proprietary information?

Yes No

If yes, please give a project identifier (e.g. grant or contract number).

D.3. Will the FN participate in any projects or activities that require approval or security clearance for foreign nationals, or that stipulate limitations on participation based on citizenship?

Yes No

If yes, please give a project identifier (e.g. grant or contract number).

D.4. Will the FN participate in activities that involve non-disclosure agreements or confidentiality agreements with an external sponsor (i.e. the U.S government or an industry sponsor), collaborator, or third party?

Yes No

If yes, please give the nature of the confidential subject matter (e.g. proprietary drug information from a pharmaceutical company).

Certification by Principal Investigator (PI) or Supervisor

I certify that the answers provided are based on knowledge of the foreign national's anticipated activities while at Washington University. The responses on this questionnaire are accurate and complete to the best of my knowledge.

Signature

Date

Name (Please Print)

Title

THANK YOU FOR COMPLETING THIS QUESTIONNAIRE

PLEASE RETURN TO THE OFFICE OF INTERNATIONAL STUDENTS AND SCHOLARS

APPENDIX VII
ITAR Language in Washington University Purchase Terms and Conditions

Before fulfilling this order, vendor must notify the University via e-mail (ovcreportcompliance@wusm.wustl.edu and Gary_maus@wustl.edu) to obtain authorization from University's Export Control Manager if any products, technical information, service, software, or source code (collectively referred to herein as "Articles") to be provided by vendor are controlled by the Department of State, Directorate of Defense Trade Controls, International Traffic in Arms Regulations (ITAR). This vendor notification shall include the name of the Washington University point of contact for the transaction, identify each ITAR controlled commodity, provide the associated U.S. Munitions List (USML) category number(s), and indicate whether or not the determination was reached as a result of a commodity jurisdiction or self-classification process. The vendor agrees that the University shall have the unilateral and unfettered right to terminate this Purchase Order, without penalty, based on such notification. The vendor agrees that if it fails to notify the University's Export Control Manager that it is providing ITAR-controlled Articles, it shall reimburse the University for any fines, legal costs or other fees imposed by the above-named regulatory agency for any violation of export controls regarding the provided Articles.

APPENDIX VIII
Technology Control Plan and Briefing

WASHINGTON UNIVERSITY TECHNOLOGY CONTROL PLAN

The purpose of this Technology Control Plan (TCP) is to prevent unauthorized access by foreign nationals to technology controlled for export under the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR). This TCP sets forth the security measures the department, principle investigator, and project personnel agree to implement in the performance of this project to prevent unauthorized foreign persons from gaining access to controlled technologies.

COMMITMENT:

It is the policy of Washington University to comply fully with all United States laws and regulations, including the laws and regulations governing the export of controlled technologies. These laws and regulations include without limitation the Export Administration Regulations (“EAR”), the International Traffic in Arms Regulations (“ITAR”), and regulations and orders administered by the Treasury Department’s Office of Foreign Assets Control (“OFAC”) (collectively, the “Export Control Laws”).

1. Primary Responsible Party (Principal Investigator):

Name:

Department:

Primary Phone:

Primary Email:

Administrative Contact:

Name:

Department:

Primary Phone:

Primary Email:

2. Identifying information for project

Contract number, parties, brief description

3. Description of the Item, Technology or Technical Data:

The nature of the controlled item, technology or technical data. Include export classification (USML or ECCN number) and if possible who classified it.

3. Physical Security Plan

Location

Project data and/or materials must be physically protected from access and observation by unauthorized individuals.

[Describe the physical location of each sensitive technology/item, to include building and room numbers.]

Physical Security

[Provide a detailed description of the physical safeguards that will be put in place to prevent unauthorized persons from accessing the technology/information. Physical safeguards may include locked doors, locked cabinets/drawers, key card or badge access, escorts and similar physical restrictions.]

In addition to the foregoing, the following measures will be observed to prevent inadvertent access by unauthorized foreign nationals to the export-controlled technology/information:

- Hard copy documents containing export-controlled information will be clearly labelled as “Export Controlled” and secured from unauthorized access, for example stored in a locked drawer when not in use.
- Technical data will not be printed unless necessary, and if printed will be promptly retrieved, and will not be left in the open where unauthorized persons can access it.
- Documents containing export-controlled information will be shredded prior to disposal.
- Unauthorized individuals will be prevented from visually accessing export controlled information, for example by viewing it on a computer monitor when it is in use.

4. Information Security

Controlled electronic information must be secured by appropriate measures, such as User IDs, password control, SSL etc. An example would be database access managed via Virtual Private Network (VPN) for authorized persons using 128-bit Secure Sockets Layer (SSL) or other advanced federally approved encryption technology.

[Describe the structure of your IT security set up at each item/technology location and how you will prevent access by unauthorized persons.]

Information security procedures may include the following:

- Export-controlled technical data shared within the research team must be distributed via secure media. Cloud services such as Gmail are not secure and therefore should not be used to communicate controlled information.

- Export-controlled technical data will not be stored on computers unless the computers are locked and password-protected when unattended. An exception may occur only if the files themselves are protected, for example with passwords or a means such as <https://www.newsoftwares.net/folderlock/>.
- Discussions about the project or work product are limited to authorized personnel and are held only in areas where unauthorized personnel are not present.
- Removable memory storage devices may be used for data back-up only within the designated secure area. When not in use, back-up drives must be clearly marked ("Export Controlled") and stored in a designated secured location (e.g. locked drawer or cabinet).
- All electronic storage media must be secured or destroyed upon completion of the project.

5. Personnel Screening

[Identify all personnel who will have access to export-controlled technology/information related to this project.]

Person	Citizenship

This TCP will be amended if personnel changes occur. All personnel assigned to this project and all visitors afforded access to controlled information or technology must be screened against the U.S. Government's denied parties lists prior to being afforded such access. Documentation of screening results will be provided by the Export Control Manager.

6. Training and Awareness

All personnel with access to export-controlled technology or information will be briefed on this Technology Control Plan and must certify their understanding of the TCP by signing the attached "Briefing and Certification on the Handling of Export-Controlled Information." Additional export control training may be required by the Export Control Manager on a case-by-case basis.

7. Ongoing Compliance Assessments

The Export Control Manager may conduct periodic reviews and/or training to assess or improve compliance with the TCP. Any changes to procedures or personnel identified in this TCP must be approved in advance by the Export Control Manager. Contact the Export Control Manager with questions or concerns at OVCRExportCompliance@wustl.edu.

8. Project Termination

The obligations of this TCP continue as long as the technology/information remains in the University's possession. Disposition of export-controlled items, equipment or information should be coordinated

with the Export Control Manager. All records pertaining to the export-controlled technologies/information will be retained in accordance with University policy and all applicable federal regulations.

9. TCP Periodical Review

All TCPs must be reviewed by the PI on a periodic basis, approximately annually. This review includes ensuring that all sections of the TCP are up-to-date. Any changes to personnel or control measures must be reported to the Export Control Manager so the TCP can be revised accordingly.

CERTIFICATION:

I hereby certify that I have read and understand the terms of this Technology Control Plan. I agree to follow the procedures set forth herein and to take other actions as necessary to prevent unauthorized access by foreign persons to the controlled technologies. I understand that I may be held personally liable for civil and criminal penalties, up to and including incarceration, if I disclose any export-controlled information to unauthorized foreign persons.

PRINTED NAME	SIGNATURE	DATE

Approved:
[Must be approved by the Export Control Manager]

Date:

BRIEFING AND CERTIFICATION ON THE HANDLING AND PROTECTION OF EXPORT CONTROLLELD INFORMATION

Briefing

This research project involves the receipt and/or use of information controlled for export under the International Traffic in Arms Regulations (ITAR) or the Export Administration regulations (EAR).

Controlled Information

In general, “Controlled Information” means any information relating to the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, operation, modification, demilitarization, destruction, processing, or use of items with a capacity for military application. Technology or information may be export-controlled even if the intended end use is civilian in nature. The term does not include basic marketing information, general system descriptions, information already in the public domain, or information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges and universities.

International Traffic in Arms Regulations (ITAR)

The International Traffic in Arms Regulations (ITAR) control the export-and re-export of equipment, software and technical data designed primarily for military, space or satellite applications. The ITAR also control the provision of certain defense-related services. Under the ITAR, it is unlawful to transfer controlled information outside the U.S. or (whether in oral, visual or hard copy form) to any foreign person inside the U.S. (“deemed” exports). A foreign person is someone who is not a U.S. citizen or permanent resident alien (green card holder) of the United States. The law recognizes no exceptions for students.

Export Administration Regulations (EAR)

The Export Administration Regulations (EAR) control the export and re-export of equipment, software and technical data having both civilian and military applications (“dual use” technologies). Unlike the ITAR, the EAR’s prohibitions can vary depending upon a foreign person’s home country. Under the EAR, transfer of controlled information to certain countries or foreign nationals from those countries who are within the U.S. may require a license.

Penalties

Researchers may be held personally liable for violations of the ITAR and EAR. Both the ITAR and EAR authorize criminal and civil sanctions. Criminal sanctions under the ITAR include fines of up to \$1,000,000 and 10 years’ incarceration per violation. Criminal sanctions under the EAR include fines of up to \$1,000,000 and incarceration up to 20 years per violation.

Reasonable Care

You must exercise care in using, sharing and safeguarding export-controlled materials or technical data with others. Unless authorized by the appropriate government agency and notified to that effect by Washington University’s Export Control Manager, you may not export controlled materials or technical data to which you have been granted access. If you foresee the

need to export such information to a foreign country or foreign person (including, but not limited to, any University employees or students) as a part of your research at Washington University, please inform the Export Control Manager (ovcreportcompliance@wustl.edu) immediately to determine if an exemption is applicable or if a license or written assurance is needed.

CERTIFICATION

I understand that my participation on the research project(s) listed may involve the receipt or use of export-controlled technology, items, software or technical data, and that it is unlawful to transfer, send or take export-controlled materials or technology out of the United States. I understand that I may not disclose, orally or visually, or transfer by any means, export-controlled technology or technical data to a non-U.S. person located inside or outside the U.S. without a license or applicable exemption as determined by WU’s Export Control Manager. I understand the law makes no specific exceptions for non-US students, visitors, staff, postdocs or any other person not pre-authorized under a TCP to access export controlled materials or data.

I have read and understand the conditions of this certification. I am electing to participate in the research cited, and I agree to follow the procedures outlined in the Technology Control plan. I understand I could be held personally liable if I unlawfully disclose export controlled technology, technical data, materials or software to unauthorized persons. I will address any questions I have regarding the designation, protection or use of export-controlled information with the Export Control Manager at ovcreportcompliance@wustl.edu.

Person	Signature	Date

Approved by:

Date:

Original signed forms for all project personnel ((including the PI) must be retained in the Department along with the Technology Control Plan (also signed by all project personnel.) Please also send a copy of all signed forms to the Export Control Manager at ovcreportcompliance@wustl.edu.