

**VIRGINIA
POLYTECHNIC
INSTITUTE AND STATE
UNIVERSITY**

**TECHNOLOGY
CONTROL PLAN**

Updated April 11, 2009

Virginia Polytechnic Institute and State University
Technology Control Plan

I. Overview

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

The U.S. Department of Commerce regulates certain dual-use technologies, materials, items, software, and technology by the Export Administration Regulations (EAR) and the U.S. Department of State controls the export of defense articles performance of defense services, including the release of defense article-related technical data, through the International Traffic in Arms Regulations (ITAR). The Department of the Treasury regulates travel and business activities with sanctioned and embargoed countries through Office of Foreign Assets Control (OFAC) regulations.

Each employee is personally responsible for safeguarding export-controlled items, materials, software, technical data, or technology as required by the above federal agencies from disclosure or release to foreign nationals or foreign persons (“foreign nationals”) without export license or other government approval if required. An export license or other government approval from the U.S. government is required before a foreign national may be given access to many items, materials, software, or technology controlled by either the U.S. Department of Commerce or the U.S. Department of State. No release of classified information (i.e. confidential, secret, top secret) is permitted to any person without the proper security level clearance and a documented “need to know” for that specific information.

Each employee is personally responsible for complying with travel to and business with countries, entities, and individuals sanctioned by the United States in regulations, laws, and executive orders enforced by OFAC.

Persons presenting research findings or other technical information at open conferences may not divulge information subject to export control regulations without export license or other government approval. Sponsored project agreements containing export controlled items, materials, software, or technology may require that project personnel formally request and obtain prior government approval before the release of a publication or presentation. These requests shall be made in compliance with, and within the time frame stated in the sponsored project agreement. If no time frame is stated in the project agreement, three to six months may need to be anticipated for approval to be received from the contracting officer. Public release of information shall not occur until any required permission or other government approval is received by U.S. Department of State, Directorate of Defense Trade Controls, (DDTC), or U.S. Department of Commerce, Bureau of Industry and Security (BIS).

Virginia Polytechnic Institute and State University
Technology Control Plan

II. Purpose

The purpose of this Technology Control Plan (TCP) is to delineate the controls necessary to ensure that the transfer of export controlled items, software, or technology, classified information or other unclassified but restricted data (e.g., controlled but unclassified, NOFORN, Naval Nuclear Power Information) that is not to be conveyed in any manner to foreign national visitors, employees, and students beyond that which is approved for export by a license or other approval from the appropriate U.S. federal agency, or which is authorized to an individual possessing the required security classification and “need to know.”

III. Authority

The National Industry Security Program Operating Manual (NISPOM) 10-509 specifies the need for this Plan: “A Technology Control Plan is required to control access by foreign nationals assigned to, or employed by, cleared contractor facilities unless the CSA [Cognizant Security Agency] determines that procedures already in place at the contractor’s facility are adequate. The TCP shall contain procedures to control access for all export-controlled information.”
[Emphasis added]

International Traffic in Arms Regulations (ITAR) 22CFR §126.13 (c) also encourages use of a Technology Control Plan (TCP): “In cases when foreign nationals are employed at or assigned to security-cleared facilities, provision by the applicant of a Technology Control Plan (available from the Defense Investigative Service) will facilitate processing.”

IV. Existing Policies and Procedures

This TCP requires Virginia Tech adherence to the NISPOM. Regarding the handling of classified information reference is made to Virginia Tech’s agreement with the U.S. Department of Defense document dated October 16, 1970. These documents, including Virginia Tech’s Office of Sponsored Programs policy OSP-29-05 “Management of Export Controlled Sponsored Projects,” shall be considered a part of this TCP, by reference.

V. Definitions

A. Controlled Unclassified Technical Data

Controlled unclassified technical data, are defined as follows (22 CFR §120.10):

1. Information (i.e. technology), other than software as defined below, material and equipment which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles or included in the U.S. Munitions Lists (USML). Information may be in the form of

Virginia Polytechnic Institute and State University
Technology Control Plan

blueprints, drawings, photographs, plans, instructions, and documentation.

2. U.S. Government classified information relating to defense articles and defense services; classified information shall include all documents/information marked by any U.S. federal agency as NOFORN (Not Releasable To Foreign Nationals), Confidential, Secret, and Top Secret.
3. Information covered by an invention secrecy order;
4. Software, as defined below, directly related to defense articles or subject to the Commerce Control List.

Controlled Technical Data does not include information or software concerning general scientific, mathematical or engineering principles currently in the public domain. It does not include basic marketing information on function or purpose or general system descriptions of defense articles. ITAR (22CFR § 120-130) (reference c). It also does not include information that advances the state of the art of articles on the U.S. Munitions List.¹ Export of ITAR-controlled technical data to a foreign person requires the following criteria be met:

“In accordance with *U.S. v. Edler Industries*, 579 F.2d at 521, the [State] Department’s practice is to regulate technical data if it is “significantly and directly related to specific articles on the Munitions List,” and is to be exported in connection with “the provision of technical assistance for the foreign manufacture of articles that, if manufactured domestically, would be on the Munitions List,” i.e., “the conduct of assisting foreign enterprises to obtain military equipment and related technical expertise.” *Edler*, 579 F.2d at 521.”² [emphasis added]

Disclosure of unclassified technical data controlled by the International Traffic in Arms Regulations (ITAR) to foreign persons, or unclassified technology or source code controlled by the Export Administration Regulations (EAR) to foreign nationals in the course of employment with U.S. institutions of higher learning is considered an export disclosure. Such disclosure is subject to and requires a U.S. government export license or other government approval prior to disclosure. Administration of the ITAR is conducted by the Directorate of Defense Trade Controls, Department of State. Administration of the EAR is conducted by the BIS, Department of Commerce

¹ In 1993, DDTC removed from its definition of ITAR-restricted technical data “information that advances the state of the art of articles on the U.S. Munitions List.” (58 FR 39285 and 57 FR 19671 compare the definitions of “technical data”).

² Declaration of William Lowell, Case No. 96 CV 1723 *Junger v U.S. Department of State* August 20, 1996, p. 8.

Virginia Polytechnic Institute and State University
Technology Control Plan

Individuals must be careful that an unauthorized “release” or transfer action does not inadvertently occur during meetings, telephone conversations, facilities, visits, or other circumstances.

NOTE: For security assistance and government contracting purposes, the Security Assistance Management Manual (SAMM para 140104.B) and the Department of Energy Acquisition Regulations ((DEARS) Section 227.401(18)) define “technical data” differently.

B. Controlled Technology

Controlled Technology (“Technology”) is defined as:

Information, i.e. technology, including scientific information that relates to research, development, engineering, test, evaluation, production, operation, use, and maintenance of munitions and other military supplies and equipment. (DoD Directive 5200.21).

“Technology” is also defined under the EAR as specific information necessary for the development, production, or use of a product. The information takes the form of “technical data” or “technical assistance.”

“Technical assistance” may take forms such as instruction, skills training, working knowledge, consulting services.

“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, and read-only memories. (EAR 15 CFR § 772)

In accordance with *Edler*, the threshold of what constitutes ITAR-restricted technical data is quite high- it must be “significantly and directly related to specific articles on the Munitions List.” It does not include basic marketing information on function or purpose or general system descriptions of defense articles, nor “information that advances the state of the art of articles on the U.S. Munitions List.”

Similarly, the threshold for what constitutes EAR-restricted “technology” is very high, it must be “specific information necessary for the “development”, “production”, or “use” of a product listed on the Commerce Control List. “Use” is defined as “Operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing” [emphasis added]

In practice, it is often difficult to determine whether or not vendor-supplied technical data is ITAR- or EAR-restricted. In the cases of vendor supplied data, Virginia Tech will err on the side of caution with unmarked technical data or technology. With

Department of Defense (DoD) supplied technical data that may be ITAR-restricted, Virginia Tech relies on DoD having followed DoD Directives 5230.24 & 25 and provided export restricted technical data with the required Export Control Warning distribution statement.

C. Defense Service (22CFR § 120.9)

A defense service is defined as:

1. “The furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles;” or
2. “The furnishing to foreign persons of any technical data controlled under this subchapter (see § 120.10), whether in the United States or abroad.”³

Virginia Tech interprets “assistance” in accordance with *U.S. v Edler Industries*, meaning “technical assistance” with or without providing technical data, and the definition of “defense service” in accordance with 38 USC § 2794. Virginia Tech interprets “design” to refer to design information relating to “detailed” design and manufacture of a defense article that if manufactured domestically, would be on the Munitions List and not concept design, which is basic or applied research.⁴ The conduct of fundamental research using only public domain information does not constitute a defense service.⁵

D. Foreign Persons and Foreign Nationals

ITAR defines a “foreign person” as any person who is not a citizen or national of the U.S. unless that person has been lawfully admitted for permanent residence, (i.e., a U. S. national

³ “Assistance is not defined in ITAR, however, it was originally “technical assistance” in the 1980 issuance of the original ITAR, but was amended in 1984 to “assistance” to reflect the State Department’s concern that: “technical assistance” could be provided to a foreign person or country without technical data having been disclosed (see 45 FR 83975 and 49 FR 47685 definitions of “defense services”). The term “technical assistance” first appeared under “foreign assistance” in the Foreign Assistance Act (substantially 22 USC §2051), and in an earlier (1984) version of the arms export regulations definition of “defense articles and defense services” in 22 CFR §121.32. However, In accordance with *Edler*, DDTC’s practice is to regulate technical data only if it is “significantly and directly related to specific articles on the Munitions List,” and is to be exported in connection with “the provision of technical assistance for the foreign manufacture of articles that, if manufactured domestically, would be on the Munitions List,” i.e., “the conduct of assisting foreign enterprises to obtain military equipment and related technical expertise.” *Edler*, 579 F.2d at 521

⁴ “Detailed design and manufacture” is regulated, but “concept design” is not. On May 14, 2008, the Director, OESRC confirmed this interpretation with two DDTC representatives (LtCol Richard Baily, Defense Trade Agreements Analyst, Licensing, and LtCol Daniel Buzby, Deputy Director, Compliance)

⁵ Office of Defense Trade Controls Advisory Opinion, University of Michigan, April 8, 2004, Deputy Undersecretary of Acquisition and Logistics Memorandum on Contracted Fundamental Research, 26 June 2006, and DFAR 204.7301..

Virginia Polytechnic Institute and State University
Technology Control Plan

is under immigrant-visa status, or is an individual referred to as “immigrant aliens” under previous laws), in the U.S. under the Immigration and Naturalization Act (8 U.S. C1101, section 101(a) 20, 60 State. 163) and “Protected Individuals” under the INA (8 USC 1324b(a)(3)) designated an asylee or refugee or a temporary resident under amnesty provisions. The definition includes foreign corporations, i.e., corporations that are not incorporated in the U.S., international organizations, foreign governments and any agency or subdivision of foreign governments (e.g. diplomatic missions).

The EAR defines a “foreign national” as “any person who is not a citizen or national of the United States.” (Note: same as “alien” pursuant to 8 U.S.C. 1101).

The National Industrial Security Program Manual (1995 version) distinguishes between a “foreign national” and an “immigrant alien,” the latter defined as “any person lawfully admitted into the U.S. under an immigration visa for permanent residence” (i.e. one who possesses permanent resident, or immigrant-visa status).

Foreign students that are in the United States on non-permanent resident status are considered foreign persons or foreign nationals.

E. Export and Deemed Export

ITAR (22CFR § 120.17) (reference c) defines “export” as:

1. Sending or taking a defense article out of the U.S. in any manner, except by mere travel outside the U.S. by a person whose personal knowledge includes technical data; or
2. Transferring registration or control to a foreign person of any aircraft, vessel, or satellite covered by the U.S. Munitions List, whether in the U.S. or abroad; or
3. Disclosing (including oral or visual disclosure) or transferring in the U.S. any defense article to an embassy, any agency or subdivision of a foreign government (e.g. diplomatic mission); or
4. Disclosing (including oral or visual disclosure) or transferring controlled technical data to a foreign person, whether in the U.S. or abroad; or
5. Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the U.S. or abroad.

ITAR does not expressly define “deemed export”, however, ITAR 22 CFR § 120.17(4) & (5) are roughly analogous to EAR definitions of “deemed export”, in that exports can occur in the United States.

Virginia Polytechnic Institute and State University
Technology Control Plan

EAR (15 CFR § 734.2(b)) (reference e) defines “export” as:

1. Sending or taking an article out of the U.S. except by mere personal knowledge, or transferring registration, control, or ownership in the U.S.;
2. Disclosing (including oral or visual disclosure) controlled information to a Non-U.S. Person, in the U.S. or abroad;
3. Performing technical assistance, training, or other defense services for, or on behalf of a Non-U.S. Person, whether in the United States or abroad; and
4. Re-exporting from foreign countries items or technology of U.S. origin (including some foreign-made items that incorporate U.S.-origin components or technology).

EAR defines “deemed export” as: “any release of technology or source code subject to the EAR to a foreign national. Such release shall be deemed to be an export to the home country or countries of the foreign national.” (15 CFR § 734.2(b)(ii)). Technology or software is “released” for export through:

1. Visual inspection by foreign nationals of U.S.-origin equipment and facilities;
2. Oral exchanges of information in the United States or abroad; or
3. The application to situations abroad of personal knowledge or technical experience acquired in the United States.

In summary, an ITAR export of technical data occurs whenever ITAR-controlled technical data, or source code is released to a foreign person, or a defense service is performed for a foreign person, in the U.S or abroad. If an export of EAR-controlled technology or source code occurs within the U.S., that action is termed an EAR “deemed” export to the foreign national or foreign person’s country of origin.

F. Defense Articles and Equipment

In general, export of materials, items, or software occur only when they are physically exported outside of the United States, or transferred to a foreign national or foreign person in the United States for the purpose of subsequent export outside of the United States. Access to a material, item, or software in the United States, accompanied by attendant technology or technical data may be considered a deemed export, even in fundamental research. The term defense article does not include any items fabricated and used solely for fundamental research purposes.

Virginia Polytechnic Institute and State University
Technology Control Plan

In proprietary research, access to an export controlled item (including software), material, or defense article, when it includes its access to technology or technical data, or is provided with training on the defense article (a defense service) is a deemed export.

However, in fundamental research, there are significant differences in the two technology-based export control regimes (ITAR/EAR) governing access to export controlled items, materials, or defense articles and their associated technology or technical data. Under ITAR, access to a defense article with or without its associated technical data, or when a defense service is performed, is an export subject to ITAR regulation.⁶ Even if the university can meet all other criteria for conducting its research as fundamental, such access to the defense article and/or its associated technical data is still subject to ITAR regulation. The portion of the research involving access to the defense article and its associated technical data must be dealt with as ITAR-restricted technical data.

Under the EAR, equipment with criteria of items listed on the Commerce Control List (CCL) and some of its “use” technology may be used in fundamental research, not subject to export controls unless the item is furnished with technology enabling the foreign national to “develop, produce, or “use” the equipment, “use” as defined in 15 CFR §772.1: “Operation, installation (including on-site installation) maintenance (checking), repair, overhaul, and refurbishing.” Access to technology that enables the foreign national to perform only a few of these functions is not “use” and is not subject to export control regulation in fundamental research, but access to technology that enables the foreign national to perform all of the functions is a deemed export subject to export control regulation.

Access to ITAR-regulated defense articles by foreign persons in the United States is problematic for Virginia Tech, because defense services can occur even though no technical data is transferred to the foreign person in the United States. Further, DDTC guidance requires a foreign person employment authorization (Export license DSP-5) must be obtained for all foreign person employees who require access to ITAR-controlled defense articles and/or technical data in the performance of their job responsibilities.⁷

G. Software (15 CFR §772.1, 22 CFR §§120.10, 121.8(f))

Software includes, but is not limited to, the system functional design, logic flow, algorithms, application programs, operating systems and support software for design, implementation,

⁶ See Licensing of Foreign Persons by a U.S. Person—UPDATED 2/27/2009

⁷ See Licensing of Foreign Persons by a U.S. Person-- UPDATED 2/27/2009. IAW 22 CFR § 120.17, the only licensable exports for transfers of defense articles in the United States that are statutorily required include: transferring registration, control or ownership to a foreign person of any aircraft, vessel, or satellite covered by the U.S. Munitions List or transferring in the United States any defense article to an embassy, any agency or subdivision of a foreign government (e.g., diplomatic missions). However, the Guidelines require export license for export of defense articles and or technical data and associated defense articles to foreign national employees, in the United States or abroad.

Virginia Polytechnic Institute and State University
Technology Control Plan

test, operation, diagnosis, and repair. Under ITAR software is classified as technical data, and may be subject to export license requirements if it is software defined in 121.8(f) as directly related to defense articles; including but not limited to the system functional design, logic flow, algorithms, application programs, operating systems and support software for design, implementation, test, operation, diagnosis and repair. A person who intends to export software only should, unless it is specifically enumerated in §121.1 (e.g., XIII(b)), apply for a technical data license pursuant to part 125. Under EAR software is a category of export controlled items regulated separately from technology.

H. Published Information and Information in the Public Domain (15 CFR § 734.7 and 22 CFR § 120.11) is:

All information that is currently published, generally accessible, or available to the public. For example:

1. Through sales at news stands and bookstores;
2. Through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information; or
3. At libraries open to the public or from which the public can obtain documents;
4. Through issued patents;
5. Through fundamental research: ITAR: (22 CFR § 120.11(a)(8)) Basic and applied research in science and engineering at accredited institutions of higher learning, in the United States, in which the resulting information can be published and shared broadly within the scientific community. Such research is termed “fundamental research” and is not subject to security classification or export control procedures. However, sponsored research conducted by a university is not considered “fundamental research” if:
 - i. The University or its researchers accept sponsor’s restrictions on publication of scientific and technical information resulting from the project ; 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
6. Fundamental Research: EAR: (15 CFR § 734.8) Research conducted by scientists, engineers, or students at a university normally will be considered fundamental research. (“University” means any accredited institution of higher education located in the United States.) Prepublication review by a sponsor of university research solely to insure that the publication would not inadvertently divulge proprietary information that the sponsor has furnished to the researchers does not change the status of the research as fundamental research. However, release of information from a corporate sponsor to university researchers where the research results are subject to prepublication review is subject to the EAR. Prepublication review by a sponsor of

Virginia Polytechnic Institute and State University
Technology Control Plan

university research solely to ensure that publication would not compromise patent rights does not change the status of fundamental research, so long as the review causes no more than a temporary delay in publication of the research results.

If research is funded by the U.S. Government (15 CFR § 734.11), and specific national security controls are agreed on to protect information resulting from the research, 15 CFR §734.3(b)(3) will not apply to any export or reexport of such information in violation of such controls. However, any export or reexport of information resulting from the research that is consistent with the specific controls may nonetheless be made under this provision.

Fundamental research is not subject to export control regulation by license or other government approval, and there are no restrictions on participation in fundamental research by foreign nationals/ persons. Procedures for conducting Sponsored Projects that are subject to export controls are established in OSP 29-05 Management of Export Controlled Sponsored Projects.

ITAR and EAR fundamental research excluded research do not have entirely similar criteria. For ITAR-defined fundamental research, DDTC interprets the regulations to require that the fundamental research be performed at an accredited institution of higher learning (physically) in the United States. For EAR-defined fundamental research, the Commerce Department interprets its regulations as being performed at a U.S. institution of higher education, regardless of geographic location.

- I. U.S. Government Classified Technical Data, Material, Items (e.g., contracts that incorporate Federal Acquisition Regulations (FAR) Clause “Security Requirements,” 52.204-2, or DEARS 952.204-2).

Classified Information is releasable only to those individuals (e.g. employees, graduate students, visitors, etc.) with the appropriate U.S. security clearance (confidential, secret, top secret, etc.) and the appropriate need-to-know, as determined by the possessor of the classified information. The handling of classified information is discussed in detail with the Principal Investigator and the University’s Facility Security Officer. Classified information is not authorized for release or disclosure to any foreign national. No classified access will be provided to the foreign national, thereby prohibiting access to facilities, documentation, and records, as well as prohibiting foreign nationals’ access to design, development, and test areas where classified work is in process.

Foreign nationals and permanent resident aliens will not be authorized access to classified contracts without proper authority under NISPOM.

1. Unclassified Controlled Technical Data

Virginia Polytechnic Institute and State University
Technology Control Plan

- a. Foreign persons/foreign nationals can not be granted access to controlled technical data or technology without appropriate export license or other government approval (i.e., a license exemption or license exception) from ODTC or BIS as appropriate. Prior to acceptance of a sponsored project with export control restrictions, the Principal Investigator and Office of Export and Secure Research Compliance (OESRC) shall prepare a project specific TCP prior to their participation in the project, unless this requirement is waived by the OESRC Director.
- b. If the publication or any disclosure of the project's findings is subject to approval by the contracting officer, once that approval is received, the information contained in that disclosure can therefore be placed in the "public domain" and, consequently, is no longer considered export controlled.

2. Proprietary Information

- a. Virginia Tech Proprietary Information is protected internally by confidential invention disclosures and internal nondisclosure agreements as may be necessary. Release of Virginia Tech proprietary information externally occurs only after a nondisclosure agreement is executed between the party receiving the information.
- b. Proprietary Information received by Virginia Tech is protected under the terms of each individual nondisclosure agreement as may be negotiated and executed by the parties involved unless the information is required to be released by a court of competent jurisdiction or as otherwise required under legal proceedings.

Proprietary information is subject to ITAR and EAR export regulations.

VI. Education

Academic departments will be responsible for appropriate orientation of all new employees, graduate, and undergraduate students, including foreign nationals employed by their departments for projects that fall within this Technology Control Plan. When appropriate, foreign nationals will be briefed and/or informed concerning those areas of export control and export licensing actions that are pertinent to their activities. OESRC will make available export awareness training to university personnel.

VII. Export Controlled Research and International Collaborations

Acceptance of an export control restricted research project or international collaboration places Virginia Tech at risk of inadvertent violation of export and sanctions laws. Principal

Virginia Polytechnic Institute and State University
Technology Control Plan

Investigators shall coordinate with OESRC to determine if a proposed research project or international collaboration is subject to export restrictions. The OESRC will assist each Principal Investigator in determining the appropriate export regime and if subject to export regulation, the project-specific security measures needed to prevent unauthorized export of restricted defense articles, items, technical data, technology, and software. Principal Investigators for any identified export controlled projects shall submit to the OESRC a Project-specific Technology Control Plan prior to the initiation of the project.

In addition to ITAR and EAR export restrictions, OFAC regulates the following transactions with sanctioned countries, entities, and individuals (31 CFR §§ 500-599)

- i. Transactions involving designated foreign countries or their nationals;
- ii. Transactions with respect to securities registered or inscribed in the name of a designated national;
- iii. Importation of and dealings in certain merchandise; and
- iv. Holding certain types of blocked property in interest-bearing accounts.
- v. Transactions with specific entities or individuals known as “specially designated nationals,” found in the Specially Designated Nationals List (“SDNL”),

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

OESRC provides periodic and special export and trade sanctions training to all Principal Investigators for any international collaboration that meets the criteria of fundamental research, or does not involve technology transfer.

VIII. Administration

Administration of this TCP is the responsibility of the University’s Technical Control Plan Officer, who is also the Export and Secure Research Program Manager (ESRPM), assigned to the Office of Export and Secure Research Compliance, as it applies to the release of controlled technical data of U.S. origin in a foreign country or to a foreign person/national or entity.

Principal Investigators and/or department heads are responsible for ensuring that employees in their activities are properly instructed in the handling of classified, export-controlled, or controlled but unclassified information, and restrictions relating to traveling abroad; and that they have signed or submitted the required briefing document:

1. Technology Control Plan Briefing (Attachment A) *Applicable to Classified Projects.*

Virginia Polytechnic Institute and State University
Technology Control Plan

2. Foreign National's Nondisclosure Statement (Attachment B) *Applicable to Foreign Nationals/Foreign Person employees with a license for access to export controlled defense articles and/or technical data and defense services.*
3. Bona Fide Employee Letter (Attachment C) *Applicable to Virginia Tech employees who are exempt from ITAR export control license requirements as a Bona Fide Employee of the University.*
4. Project Specific Technology Control Plan (Attachment D) Example Only *Applicable when the University accepts an export controlled or similarly restricted Sponsored Project.*
5. Employee Annual Temporary Export (TMP/ENC) Certification-. https://secure.research.vt.edu/oesrc_forms/ *Applicable when a Virginia Tech employee travels outside of the United States and Canada, taking a university owned laptop computer, cell phone, personal data assistance, and or digital storage devices.*
6. Faculty Certification-Export controlled nondisclosure agreement (nda)- https://secure.research.vt.edu/oesrc_forms/ *Applicable when Virginia Tech accepts an nda from an entity or individual who refuses to accept Virginia Tech's standard export compliance terms for the nda.*

The Technology Control Plan Officer (TCPO) shall prepare and maintain the University's Technology Control Plan.

The TCPO shall prepare and maintain Office of Sponsored Programs policy OSP-29-05 "Management of Export Controlled Sponsored Projects," Other University management personnel supporting the TCPO's implementation and administration include:

Vice President for Research
Director, Office of Export and Secure Research Compliance
Special Assistant Research Contract Affairs, VP for Research Office
Assistant Vice President for Administration, Sponsored Programs

Freedom of Information

As a public educational institution of the State of Virginia, Virginia Tech has certain obligations to respond to requests for "public" information. However, not all information of the University is subject to state statutes and each request for information is reviewed by appropriate administrators/University Counsel for our legal obligations for release or protection of the information. Virginia Tech believes sufficient control and supervision will exist in regard to all employees, undergraduate and graduate students, including those with foreign national status, as regards technology transfer or release of technical know-how. It is the intention of Virginia Tech to protect all its information not in the public domain unless appropriately authorized by a court of competent jurisdiction, applicable state statute, or the U.S. Government as may be required in each individual case.

In order for Virginia Tech to assume responsibility to meet federal regulations previously cited, no employee, graduate/undergraduate student or other person acting on behalf of Virginia Tech shall disclose

Virginia Polytechnic Institute and State University
Technology Control Plan

or release controlled technical data, technology or source code, as herein defined, without full compliance to this policy document.

Virginia Polytechnic Institute and State University
Technology Control Plan

ATTACHMENT A

TECHNOLOGY CONTROL PLAN BRIEFING
Applicable to Classified Projects

Project Account:

Sponsor Name & Project Title:

This is to acknowledge that I, _____, have read the Virginia Tech University Technology Control Plan and have discussed the plan with the Virginia Tech Facility Security Officer, or his designee, and that I understand the plan and agree to comply with its requirements.

(Signature) Date

(Printed Name)

Acknowledgement of Immediate Supervisor:

(Signature) Date

(Printed Name)

**Non-Disclosure Agreement – Access to ITAR-Controlled Defense Articles by
Foreign Person Employees**

I, [name of foreign person], acknowledge and understand that any technical data related to a defense article covered by the U.S. Munitions List to which I have access per authorization by the U.S. Department of State, Directorate of Defense Trade Controls (DDTC) under [state relevant export license/authorization number**] and disclosed to me in my employment by [name of U.S. person] is subject to the export controls of the International Traffic in Arms Regulations (ITAR) (Title 22, Code of Federal Regulations, Parts 120-130), particularly the 22 CFR 124.8 clauses.

1. This authorization shall not enter into force, and shall not be amended or extended, without the prior written approval of the Department of State of the U.S. Government.

2. This authorization is subject to all United States laws and regulations relating to exports and to all administrative acts of the U.S. Government pursuant to such laws and regulations.

3. The parties to this authorization agree that the obligations contained in this authorization shall not affect the performance of any obligations created by prior contracts or subcontracts which the parties may have individually or collectively with the U.S. Government.

4. No liability will be incurred by or attributed to the U.S. Government in connection with any possible infringement or privately owned patent or proprietary rights, either domestic or foreign, by reason of the U.S. Government's approval of this authorization.

5. The technical data or defense services exported from the United States in furtherance of this authorization and any defense article which may be produced or manufactured from such technical data or defense service may not be transferred to a person in a third country or to a national of a third country except as specifically authorized in this authorization unless the prior written approval of the Department of State has been obtained.

6. All provisions in this authorization which refer to the United States Government and the Department of State will remain binding on the parties after the termination of the authorization.

During my employment with [name of U.S. person], I will be considered and treated as a U.S. person for the purposes of the ITAR. As such, I am authorized to interact and participate in discussions with other U.S. and foreign persons, and disclose technical data as necessary, while performing my job duties covered under DDTC [case number]. It will be the responsibility of my employer, [name of U.S. person], to notify other U.S. and foreign persons of my status as a foreign national employee prior to my interaction.

I also acknowledge and understand that should I inadvertently receive technical data or defense articles for which I have not been granted access authorization by DDTC, or if I inadvertently export technical data or defense articles received during my employment to an unauthorized recipient, I will report such unauthorized transfer and acknowledge the transfer to be a violation of U.S. Government regulations.

In furtherance of the above, I hereby certify that all defense articles, including related technical data, to which I have access will not be used for any purpose other than that authorized by DDTC and will not be further exported, transferred, disclosed via any means (e.g., oral disclosure, electronic, visual access, facsimile message, telephone) whether in its original form, modified, or incorporated in any other form, to any other foreign person or any foreign country without the prior written approval of DDTC.

Signature – Foreign Person (Employee)

Date

Signature – U.S Person (Employer)

Date

Bona Fide Employee Letter

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

VIRGINIA POLYTECHNIC INSTITUTE
AND STATE UNIVERSITY

Office of Export and Secure Research Compliance

2000 Kraft Drive, Suite 2000
Blacksburg, Virginia 24060
Phone (540) 231-3801 Fax: (540) 231-0959

Dear :

You are hereby notified that as _____ (*participant/principal investigator*) in the Sponsored Project for

_____ (*name of project*) you will be producing International Traffic in Arms (ITAR) export control restricted experimental or developmental electronic equipment specifically designed or modified for military application or specifically designed or modified for use with a military system and associated technical data.

In accordance with ITAR 22 CFR § 125.4(b)(10), the ITAR-restricted defense articles or technical data may not be transferred to foreign persons without the prior written approval of the Office of Defense Trade Controls. Prohibited technical transfer includes oral, visual, written or electronic disclosure, as well as transfer of physical custody. Violations of International Traffic in Arms Regulations can result in criminal penalties of up to 10 years in prison and \$1 Million in fines, and civil penalties of up to \$500,000 in fines and forfeiture (22 CFR §§ 127-1 through 127-12).

If you have questions about this export control restriction, please contact David Brady (540-231-3801) from our office.

Sincerely,

David A. Brady
Director and FSO, Office of Export and Secure
Research Compliance

University File

**Technology Control Plan
Virginia Polytechnic Institute and State University
Office of Export and Secure Research Compliance**

Principal Investigator:

Department:

Title of Sponsored Program:

Sponsor:

Government Prime Sponsor:

Institutional Commitment

Virginia Polytechnic Institute and State University (“Virginia Tech”) is committed to complying with applicable export control laws. To ensure compliance with these laws in sponsored programs, this project will be managed in accordance with OSP Policy 29-05 Management of Export Controlled Sponsored Projects.

Commodity Jurisdiction and Classification

There are contractual **publication and foreign person** restrictions on this research project voiding the universities ability to conduct this as fundamental research excluded from export regulations. In addition, the sponsor has determined that this project will be export controlled under the International Traffic in Arms Regulations (ITAR). The applicable category from the United States Munitions List is:

Detail of ITAR Category

As a result of this determination, the Principal Investigator has adopted a technology control plan to ensure that controlled defense services, articles, and technical data, hereafter referred to as “controlled items”, are adequately protected from disclosure to foreign persons who do not have an approved license, valid license exception from the government or other written government approval. Any data and/or research results generated from the controlled items will also be treated as controlled items.

Security Overview

“One Lock” is the principal of securing controlled items by using at least one mechanism to prevent disclosure to unauthorized persons. This is the minimum requirement for safeguarding the controlled items. Methods for obtaining at least “one lock” are described in the physical and information security sections. It is the responsibility of the project personnel to safeguard the controlled items at all times by having “one lock” in place.

Physical Security

Work Area. The minimum security requirement for a controlled item work area is set forth in the National Industrial Security Program Operating Manual (NISPOM); section 5-305 “Restricted Areas”. The restricted area shall have a clearly defined perimeter, which is adequate to protect against oral and visual disclosure of the controlled items. Physical barriers are strongly recommended but are not required as long as oral and visual disclosure can be prevented. Project personnel within the Restricted Area shall be responsible for challenging all persons who may lack appropriate access authority.

Storage. All controlled items will be secured in a locked storage container when not in the personal possession of the approved project personnel.

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

WARNING - This contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979, as amended, Title 50, U.S.C., App. 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.

Information Security

Computer. All computers run Microsoft Windows XP, Vista, Mac OS X, or Linux with the latest security service pack and patches. Approved project personnel are the only designated users of the computers and a valid account and password must be provided to gain access. Only approved project personnel retain this login information and no other login accounts are created. Both failed and successful logins are logged internally. Firewalls are installed on all computers to secure and monitor network access to/from the computer. If the firewall must be disabled to allow proper data collection, wired and wireless internet connections must be disabled.

Data Storage and Transmission. External portable hard drives or flash drives are strongly recommended for data storage. These storage devices can easily be locked in a storage container when not in use. It is suggested that these drives are password protected or encrypted. For data storage on drives with network access or backup servers, the controlled technical data files must be secured by encryption or password protection. Emails shall not contain controlled technical data files unless both send and receive email locations are encrypted.

Supercomputing. Supercomputing using controlled technical data files can be achieved in a secure manner. Separate login head-nodes will be provided for both System X and SGI systems. The controlled data users can transfer the files via SSH/SCP/SFTP file transfers. This transmission method is secure and encrypted. The controlled data users can also make arrangements to connect a portable hard drive directly to the server to enable large transfers. The controlled data server will be located in a locked rack within a locked room. A webcam will monitor the door and the rack and surveillance will be archived. Access to the controlled data server room and rack will be limited to U.S. Persons only. Multiple simultaneous controlled data users can use the system. UNIX security models are sufficient. Data access from System X nodes and SGI systems will use NFS over a secure communication channel. NFS can be run over open-VPN, IP-SEC, or using AES encrypted files. Once the project is complete, the controlled data user will arrange to transfer the data into their custody. Controlled data on the controlled data server will be erased by approved VT Advanced Research Computing personnel.

Project Personnel Screening Procedures

Clearly identify all project personnel and their national citizenship on Attachment A: Acknowledgement of a Technology Control Plan. All project personnel are responsible for reviewing and signing this document. All project personnel have attended or will attend export control training provided by OESRC. Personnel who have not had training before having access to controlled items will be signed up for the next available training session. All project personnel are made aware of their responsibilities to prevent either active or inadvertent disclosure of controlled items and of the criminal and civil penalties (including prison sentences of up to 10 years and fines of up to \$1M) for failure to comply with U.S. export control rules. All project personnel will be screened against the applicable restricted parties' access lists and will have their nationality screened by the OESRC. The PI will notify OESRC before adding additional personnel to a project having access to export controlled items.

Publication Risks

In most cases restricted research will contractually require that project personnel shall not release or disseminate any information pertaining to the project without the prior written approval of the sponsor, excluding information already in the public domain. In the rare case there is not a contractual publication restriction and the project involves

controlled items, research results and publications generated from the controlled items are still subject to the approval of the sponsor. Therefore, publications of projects that involve controlled items are subject to the approval of the sponsor and should be considered prior to employing graduate students and tenure track faculty. Publications (including but not limited to theses, dissertations and journal publications) may be delayed or denied based on the approval of the sponsor.

Project Completion Requirements

Upon completion of a restricted research project, all controlled items will be disposed of or stored properly. The secure storage requirements set forth in the previous sections remain the same after completion of the project. Hard copies will be disposed of by shredding. Electronic files will be disposed of by using current “wiping” software. Contact OESRC or your department IS administrator for information on effective solutions for wiping. Hardware and equipment can be disposed of properly by contacting OESRC.

Special Notes

This section is reserved for any special notes or information pertaining to the specific project.

Self Assessment

The PI and department shall notify OESRC (1) each time an additional person is added to the project so that they can be screened and trained, and (2) when the scope of the project changes. The PI will annually certify, by 31 December, and the *[Insert Department]* shall approve that the project is being carried out in compliance with this TCP.

Submitted:

PI *[Insert Department]*

By: _____ By: _____

Name: _____ **Name:** _____
Title: Principal Investigator Title: Department Head

Date: _____ Date: _____

**Attachment: Acknowledgement of Technology Control Plan
for Virginia Polytechnic Institute and State University
for the [Insert Project Name}
for the [Insert Government or flow through and Government sponsor]**

I hereby certify that I have read and understand the provisions of the above Technology Control Plan, as well as understand that I could be held personally liable if I unlawfully disclose, regardless of form or format, export controlled information to unauthorized persons.

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____

Print name: _____ School/Dept _____
US Citizen ___ Green Card ___ Foreign National/ Country of Origin _____
Signature: _____