EXPORT CONTROLS PROGRAM MANUAL

OFFICE OF ETHICS AND COMPLIANCE

UNIVERSITY OF SOUTHERN CALIFORNIA
HTTPS://OEC.USC.EDU/COMPLIANCE-PROGRAMS/INTERNATIONAL-ACTIVITY/RESEARCH/ |
COMPLIANCE@USC.EDU

Table of Contents

I. Overview

Export controls are U.S. laws and regulations that regulate and restrict the release of certain technologies, information, and services to foreign nationals within and outside the United States, and to foreign countries for reasons of foreign policy and national security. These laws and regulations are complex and updated frequently.

USC engages in a variety of activities related to research, instruction, healthcare, student outreach, and other strategic partnerships and affiliations that may create obligations under United States export control regulations, the Foreign Corrupt Practices Act (FCPA), and economic and trade sanctions regulations. These include:

- Research and teaching
- International travel
- Doing business with international partners
- Restrictive trade practices and boycotts
- Sharing proprietary, confidential or otherwise controlled information, source code, or technology with foreign nationals located in the U.S. or abroad;
- Sending or taking tangible items or controlled technology or source code to another country;
- Collaborations with foreign entities;
- Interactions with embargoed or sanctioned countries, organizations, or individuals.

USC is fully committed to complying with all U.S. Government export control laws and regulations. This USC Export Control Manual (also referred to as the "Manual") provides an overview of USC's export control responsibilities under applicable laws, regulations, and university policy and explains the roles, responsibilities, and processes the university has implemented to meet its obligations. The Manual is not itself a policy document, and all export-related questions should be directed to the Office of Ethics and Compliance (OEC). Please visit https://oec.usc.edu or e-mail compliance@usc.edu for assistance when specific scenarios arise.

A. Key Terms

Deemed export: Releasing or otherwise transferring "technology" or source code (but not object code) to a foreign person in the United States. [15 CFR 734.13]

Defense article: Any item or technical data designated in the United States Munitions List (USML). This includes technical data recorded or stored in any physical form, models, and mock-ups, or other items that reveal technical data directly relating to the defense article listed in the USML. [22 CFR 120.6]

Defense service: Furnishing of assistance (including training), whether in the United States or abroad, to a foreign person in connection with the design, development, engineering, manufacture, production,

assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing, or use of Defense Articles; or the furnishing of any controlled Technical Data to a foreign national anywhere; or military training of foreign units and forces in the U.S. or abroad. [22 CFR 120.9]

Dual-use: Under US export control regulations, "dual-use" refers to items, software, or technology that have both commercial applications and potential military, defense, intelligence, or proliferation uses. [15 CFR 772.1]

Export: Any release of export-controlled items, information, or services outside the U.S. to anyone (including a U.S. citizen). "Release" includes shipment as well as oral, written, electronic (fax, e-mail, Internet, etc.), or visual disclosure as well as the export of encryption source code or object code software. Any release of export-controlled Items, information, or services to a foreign national or foreign person in the U.S. is a Deemed Export. [15 CFR 734.15; 22 CFR 120.17]

Export license: A written authorization provided by the appropriate governing regulatory authority (such as BIS, OFAC, or DDTC) detailing the specific terms and conditions under which the export, deemed export, reexport, or deemed reexport of export-controlled items, information, technology, services, or other regulated activities are allowed. [15 CFR 772.1; 22 CFR 120.20 and 123]

Foreign Person: Any natural person who is not a lawful permanent resident as defined by 8 U.S.C. 1101(a)(20) or who is not a protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any foreign corporation, business association, partnership, trust, society, or any other entity or group that is not incorporated or organized to do business in the U.S., as well as international organizations, foreign governments, and any agency or subdivision of foreign governments. [22 CFR 120.16]

Fundamental research: Under the EAR, Fundamental Research is defined as research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons [15 CFR 734.8]. Under the ITAR, Fundamental Research is similarly defined, with the added requirement that it be conducted at accredited institutions of higher learning in the U.S. in order to be exempt from the controls. [22 CFR 120.11(8)]

Item: A commodity, software, or technology. [15 CFR 772.1]

Technical data: For purpose of ITAR control, this means information regarded as required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles. Technical Data includes information in the form of blueprints, drawings, photographs, plans, instructions, or documentation. [22 CFR 120.10(a)]

Technology: Information necessary for the "development," "production," "use," operation, installation, maintenance, repair, overhaul, or refurbishing of an Item. 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. [15 CFR 772.1]

U.S. Person: Any individual who is a citizen of the United States, an individual who is a lawful permanent resident as defined by 8 U.S.C. 1101(a)(20), or an individual who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any corporation, business association, partnership, society, trust, or any other entity, organization or group that is incorporated to do business in the United States. [22 CFR 120.15].

B. List of Abbreviations

BIS	Department of Commerce Bureau of Industry and Security
CCL	Commerce Control List
CJ	Commodity Jurisdiction
DCG	Department of Contracts and Grants, University of Southern California
DDTC	Department of State Directorate of Defense Trade Controls
DFAR	Defense Federal Acquisition Regulation
EAR	Export Administration Regulations
FAR	Federal Acquisition Regulation
FCPA	Foreign Corrupt Practices Act
FRE	Fundamental Research Exclusion
ECCN	Export Control Classification Number
FSVS	Faculty and Staff Visa Services, University of Southern California
ICT	Institute for Creative Technologies, University of Southern California
ISI	Information Sciences Institute, University of Southern California
ITAR	International Traffic in Arms Regulations
MTA	Material Transfer Agreement
NDA	Non-Disclosure Agreement
OEC	Office of Ethics and Compliance, University of Southern California
OFAC	Department of the Treasury Office of Foreign Assets Control
OIS	Office of International Services, University of Southern California
RPS	Restricted Party Screening
SDN	Specially Designated Nationals and Blocked Persons List
TAA	Technical Assistance Agreement
TCP	Technology Control Plan
USML	United States Munitions List
SVPRI	Senior Vice President for Research and Innovation, University of Southern California

C. Roles and Responsibilities

In order to designate compliance responsibility to appropriate stakeholders, USC has assigned the following roles and responsibilities within the university:

Associate Vice President of Research Compliance

The Associate Vice President (Associate VP) of Research Compliance is responsible for the implementation of USC's export control compliance program. In this capacity, the Associate VP directs the implementation of the export compliance program, which includes:

- Ongoing risk assessment to identify activities at USC that are impacted by export control regulations
- Education of faculty and staff
- Development and revision of policy as appropriate
- Assisting investigators, researchers, and schools/units at USC when research involves export-controlled equipment or information
- Assisting principal investigators (PIs) in developing technology control plans for research involving export-controlled items or information.
- Supporting applications for export licenses, commodity jurisdiction and commodity classification requests when applicable
- Monitoring and interpreting export control legislation
- Ensuring appropriate record keeping for export-controlled activities
- Supporting USC's standing faculty committee charged with the review of restricted research proposal exception requests, in accordance with USC's International Collaborations and Export Controls policy

Assistant Director, Export Control Compliance

The Assistant Director of Export Control Compliance supports the implementation of the export control compliance program in each of the areas of the Associate VP's oversight.

Office of Research and Innovation

The Senior Vice President of Research and Innovation (SVPRI) chairs the International Research Committee (IRC), which is USC's standing committee charged with oversight of restricted research.

Department of Contracts and Grants

The Department of Contracts and Grants assists in identifying sponsored agreements with provisions that may carry export control ramifications, and negotiating these provisions out of the applicable

agreement whenever possible. When these provisions exist, DCG coordinates with OEC to ensure the principal investigator submits a proposal exception request for committee review, in accordance with USC's International Collaborations and Export Controls policy. See Section VII.A for additional detail.

Principal Investigators (PIs)

Because PIs have a unique understanding of the information and technology involved in their research activities, they play an important role in ensuring compliance with export control requirements. This understanding is critical to appropriately characterizing items and information that may be subject to export control obligations and ensuring all export requirements are met. The PI's roles and responsibilities include:

- Assisting OEC in correctly classifying technology and items that are subject to export control laws
- Assisting in developing and maintaining the conditions of a technology control plan (TCP) for any activity, technology, data, or equipment where the need for such a plan is identified
- Ensuring that research staff and students have been trained on the technology control plan and on the export control regulations, should any apply
- Notifying OEC prior to or immediately upon the receipt of any information or technology that is either identified as or suspected to be export controlled
- Ensuring that information that has been designated as export controlled is not disclosed to a foreign national or exported to a foreign country prior to engaging with OEC for guidance.

II. U.S. Export Laws and Regulations

Export controls aim to advance U.S. economic interests at home and abroad, prevent the proliferation of weapons of mass destruction, aid regional stability, implement anti-terrorism and crime controls, and protect human rights. Additionally, the United States maintains economic embargoes against a number of countries whose governments consistently violate human rights or support global terrorism. Export control laws and regulations have grown in scope and complexity over the years, particularly since September 11, 2001. Export regulations change frequently, are lengthy, and can be challenging to interpret.

There are two primary sets of export control regulations: the Export Administration Regulations, or EAR, and the International Traffic in Arms Regulations, or ITAR. The EAR regulates "dual use" items – physical items, software and technology that have both commercial and military uses – while the ITAR regulates physical items, technical data, software, and services controlled for military purposes.

In the research context, EAR and ITAR considerations frequently arise in the following areas and disciplines:

- Military or Defense Articles and Services
- High Performance Computing
- Dual Use Technologies (technologies with both a military and commercial application)
- Encryption Technology
- Missiles & Missile Technology
- Chemical/Biological Weapons
- Nuclear Technology
- Select Agents & Toxins
- Space Technology & Satellites
- Medical Lasers

A. Export Administration Regulations (EAR)

The EAR regulates exports (including re-exports and "deemed exports") of commercial and "dual-use" goods, software and technology (i.e., items intended for non-military applications that nonetheless may be useful for military purposes). These regulations are administered by the Commerce Department's Bureau of Industry and Security ("BIS").

Exports of items identified on the CCL may require a specific license from the Commerce Department, depending upon the reasons for control, the country of destination, and the purpose for which the items will be used.

Additional information and guidance regarding the EAR (15 C.F.R. Parts 730 to 774) is available on the BIS website at http://www.bis.doc.gov. In addition, the full text of the EAR, including the CCL, is available at http://www.access.gpo.gov/bis/ear/ear_data.html.

B. International Traffic in Arms Regulations (ITAR)

The ITAR regulates items and services that are considered to be "defense articles" or "defense services," as well as certain temporary imports of foreign-made defense articles and "brokering" activities that have been identified by the U.S. government as being inherently or predominantly suited for military applications.

The defense articles and defense services subject to the ITAR include those goods, software and "technical data" that appear on the United States Munitions List ("USML") ("technical data" is information related to the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of a defense article). Examples include firearms, ammunition, explosives, propellants, and military training equipment and any hardware, software, or related technical data. Even if a specific item does not appear on the USML, it is controlled under the ITAR if it has been specifically designed, developed, configured, adapted or modified for a military purpose and does not have "predominant civil applications."

With very few exceptions, the ITAR requires exporters to obtain prior written authorization from DDTC before exporting or re-exporting defense articles or defense services or engaging in "deemed exports" of ITAR-controlled technical data.

Finally, the ITAR includes a list of countries that are subject to U.S. arms embargoes. The State Department maintains a general policy of denying license applications for exports of ITAR-controlled items to the embargoed countries. The list of ITAR embargoed countries is available at http://www.pmddtc.state.gov/embargoed_countries/.

Additional information and guidance regarding the ITAR is available on DDTC's website at http://www.pmddtc.state.gov/. In addition, the full text of the ITAR (22 C.F.R. Parts 120 to 130), including the USML, is available at http://www.pmddtc.state.gov/regulations_laws/itar.html.

C. Trade Sanctions Regulations (OFAC)

The Treasury Department's Office of Foreign Assets Control ("OFAC") administers and enforces economic and trade sanctions against targeted countries on the basis of foreign policy and national security reasons.

Under these laws, certain entities and individuals (both foreign and domestic) may be subject to trade sanctions, embargoes, and other restrictions on exports, re-exports, or transfers of U.S.-origin items. In

addition, certain countries may be subject to either comprehensive or targeted sanctions or export restrictions.

- Comprehensive sanctions prohibit nearly all exports and other business transactions without specific government authorization. (e.g., Cuba, Iran, North Korea).
- Targeted sanctions prohibit transactions related to specific goods, technologies, and services with specific sanctioned entities or individuals, or apply to certain industries or sectors of a country's economy (e.g., the financial services, energy, mining, and defense and related material sectors of the Russian economy).

OFAC administers sanctions against designated entities and individuals found by the U.S. government to be agents of the sanctioned countries, terrorism sponsoring organizations, international narcotics traffickers, weapons proliferators or otherwise engaged in activities that threaten the security of the United States. These entities and individuals generally are identified on the List of Specially Designated Nationals (the "SDN List"). Virtually all transactions with these entities and individuals are prohibited. Countries currently subject to these sanctions may be found on the Department of the Treasury Office of Foreign Assets Control website. As of March 2026, OFAC currently administers sanctions against the following countries, among others, but the list is subject to change at any time:

Category	Jurisdictions currently in this category (as of March 2026)	Practical compliance posture
Comprehensive / embargo-style	**Cuba; Iran; North Korea; Crimea region of Ukraine; Donetsk and Luhansk "Covered Regions" of Ukraine**	These are the closest things to jurisdiction-wide OFAC embargoes. For the Ukraine Covered Regions, E.O. 14065 prohibits new investment and most import, export, sale, supply, financing, or facilitation involving the covered areas. OFAC also clarifies that these Covered Regions are **not** the entirety of the Donetsk and Luhansk oblasts.
Partial / targeted / sectoral	**Afghanistan; Belarus; Burma/Myanmar; Central African Republic; China** *(via Chinese Military Companies sanctions)*; **Democratic Republic of the Congo; Ethiopia; Hong Kong; Iraq; Lebanon; Libya; Mali; Nicaragua; Russia; Somalia; South Sudan; Sudan/Darfur; Venezuela; Yemen**	These are **not** full country embargoes. Restrictions are program-specific and typically involve SDN blocking, government-related restrictions, sectoral measures, or other defined transactional prohibitions. OFAC expressly states that **Afghanistan** is **not** subject to comprehensive sanctions, and that the **Venezuelan people** are **not** subject to comprehensive U.S. sanctions.

There are certain circumstances in which distance education implicates sanctions considerations, particularly for OFAC-sanctioned countries like Iran. Iranian students are eligible to participate in both undergraduate and graduate-level study and research while physically in the United States as long as appropriate visas are in place. With respect to online education, however, the regulations impose

limitations on Iranian students participating while in Iran. Please consult with OEC prior to allowing participation in an online course by a student who is or will be located in Iran. More information can also be found in OEC's Guidance on Iran and OFAC.

D. Foreign Corrupt Practices Act (FCPA)

The Foreign Corrupt Practices Act's (FCPA) anti-bribery provisions generally prohibit U.S. organizations and employees from offering payments or anything of value to foreign officials to secure an improper advantage or obtain or retain business, and impose due diligence requirements on US entities in the selection of foreign business partners.

The types of payments covered by the FCPA are broad and cover anything that may confer a benefit on someone in a position to provide a commercial or other advantage to USC. Some examples include, but are not limited to:

- Any gift of cash or a cash substitute
- Anything that is offered as a "quid pro quo" (a payment in exchange for favor or advantage)
- Any gift or entertainment that is illegal under the foreign country's laws, or known to be prohibited by the foreign official's department, agency, or organization
- Anything that may influence, or may be perceived as influencing, the decision of anyone considered to be a foreign official
- Anything given to a foreign official associated with a tender or competitive bidding process where USC is involved
- Any inappropriate entertainment (such as entertainment that is illegal under local law or U.S. law)
- Any travel, entertainment, or gifts to a family member of, or person otherwise closely associated with, a foreign official

USC faculty, staff, and student employees are expected to exercise care and take all necessary precautions to ensure that they are conducting business with reputable and qualified business collaborators (e.g., partners, representatives, recruiters, distributors, and any other representatives collaborating with or on behalf of USC). The Office of the Vice President for Strategic and Global Initiatives must approve all initiatives that involve establishment of an overseas presence or international partnership with any overseas university, institution, or governmental entity, excluding sponsored research agreements and technology licenses.

To avoid making improper payments to foreign officials when conducting university business overseas, USC faculty, staff, and student employees are also expected to perform due diligence on overseas business partners and collaborators and to be alert to "red flags" with regard to these business partners. For guidance on the kinds of factors that may constitute red flags, please visit OEC's International Business page.

E. Anti-Boycott Restrictions

Participation in certain restrictive trade practices is prohibited under anti-boycott provisions found in the EAR. Specifically, the "anti-boycott" provisions of the EAR prohibit U.S. persons or businesses from participating in any non-U.S.-sanctioned foreign government boycott. As such, USC is not permitted to enter into any contract or other business relationship that requires it to participate in any non-U.S.-sanctioned foreign government boycott. An example of this would be the Arab League's boycott of Israel that manifests through provisions in contractual agreements between the Arab League and business partners that attempt to require that the business partner not conduct business with Israel as a condition to the contractual arrangement. Please consult with OEC for additional information.

F. Licensing

If an activity is controlled under the export regulations, then a license or other approval may be needed, unless an exemption or exception applies. Examples of situations where a license may be required include, but are not limited to:

- Access to export-restricted hardware, software, or information;
- Shipping or taking export-controlled hardware, software, or information outside of the U.S.;
- Attending a conference where registration is limited to U.S. citizens;
- Travel to a sanctioned country;
- Transfer of controlled technical data to a foreign person in or outside of the U.S.;
- Providing anything of value, controlled items or controlled technology to someone from a sanctioned country, on the entity list, denied persons list, debarred (or excluded) parties list or any other restricted list.

For other types of activities that may raise export control considerations, please review Research That Requires a License.

III. Exclusions and Exemptions from the Export Control Regulations

Generally speaking, the following items, activities, and categories of information are not subject to the export control regulations:

- Fundamental research: Fundamental research is defined to mean "basic and applied research" in science and engineering, where the resulting information is ordinarily shared broadly within the scientific community.

- Published (publicly available) Information and Software: Information that is published and is generally accessible to the public through publication in books or periodicals available in a public library or in bookstores, or information that is presented at a conference, meeting, seminar, trade show, or other open gathering is considered to be in the public domain. An open gathering is one in which members of the general public are eligible to attend and attendees are permitted to take notes.

- Published Educational Information: Most of the course material taught in U.S. universities that is published in the course catalog and is considered publicly available and not subject to the export control regulations.

- Laptops and other mobile devices: A laptop may be taken abroad as long as it does not contain any export-controlled documents or non-commercial, special purpose encryption software. If the laptop contains only the commercial encryption software that is standard for the computer, the encryption technology is not export-controlled (unless travel is to an OFAC-sanctioned country). If the laptop contains something other than standard commercial encryption software or if the foreign travel is to an OFAC-sanctioned country, the laptop should not be taken abroad before consulting with OEC.

- University bona fide Full Time Employee exemption

Under the EAR and ITAR, the release in the United States of controlled technical data, technology, or source code to a bona fide, full-time regular university employee may not require a license in limited circumstances. The ITAR provides relief from licensing requirements at 22 C.F.R. § 125.4(b)(10), and the EAR provides authorization under License Exception TSU at 15 C.F.R. § 740.13(f). These provisions have distinct requirements and must be evaluated separately before use.

This exemption/authorization is not available for all foreign national employees. Under the ITAR, the employee must not be a national of a country to which exports are prohibited under 22 C.F.R. § 126.1. Under the EAR, the employee must not be a national of a destination listed in Country Group D:5. Nationals of proscribed or arms-embargoed countries are ineligible for this exemption/authorization. This includes, but is not limited to, nationals of **Iran**, **China/PRC**, **Venezuela**, and **Russia**. Because the

ITAR § 126.1 and EAR Country Group D:5 lists may change, OEC must confirm eligibility against the current lists before the exemption/authorization is used.

At universities, typically only H-1B visa holders meet the bona fide, full-time regular employee criteria. Student employees, including graduate students, generally do not qualify regardless of the number of hours worked. The employee must maintain a permanent residence/abode in the United States throughout the period of employment.

Both the ITAR and EAR require the university to inform the employee in writing that the controlled technical data, technology, or source code may not be transferred or exported to other foreign persons/foreign nationals without prior U.S. Government authorization. The EAR also requires that the employee be informed in writing that this obligation extends beyond the end of employment. As a best practice, employees should also be instructed not to take controlled technical data, technology, or source code abroad or remotely access it from outside the United States without prior OEC review and authorization.

For questions about the bona fide full-time employee exemption/authorization, including whether it applies in a specific scenario, contact OEC at compliance@usc.edu.

IV. USC-Related Activities That May Be Subject to Export Control Regulations

Notwithstanding the exemptions and exclusions discussed above, there are a range of university activities and transactions that may raise export control considerations, including but not limited to:

i. The results of research conducted at USC or by USC employees are intended for military, nuclear, or space purposes or for other restricted End-Uses or Users;
ii. Foreign Persons will have access to Controlled Physical Items on campus;
iii. Software including encryption features will be developed or purchased;
iv. USC faculty or staff will export or travel abroad with research equipment, chemicals, biological materials, encrypted software, or Controlled Physical Items; or travel abroad with laptops, cell phones, tablets, portable drives, or other electronic devices containing Controlled Information;
v. A proposed activity/transaction will involve embargoed countries or entities, individuals/entities located in embargoed countries, or who are on prohibited or restricted End-User lists, as determined by Restricted Party Screening;
vi. Receipt of proprietary information from a third party
vii. Receipt of export-controlled information from a third party
viii. MTAs, DTAs, DUAs, CDAs, licensing, software licenses, and any other agreements that may result in sharing USC-owned items, technology, or information with foreign recipients;
ix. The sponsor requires pre-approval rights over publications or the participation of Foreign Persons;
x. International shipments, including equipment, chemicals, or biologicals to a foreign country;
xi. Interactions with Foreign Government officials; and
xii. The agreement contains a Controlled Unclassified Information (CUI) clause (e.g., DFARS 252.204-7012) or CMMC clause (e.g., DFARS 252.204-7021)

Faculty, researchers, employees, and students at USC are encouraged to contact OEC in these instances to obtain appropriate guidance.

V. International Collaborations Disclosure Requirements

USC is engaged in far-reaching, global research and learning programs and recognizes the importance of these international collaborations. As research and learning programs are becoming ever more global, federal sponsors are placing increased emphasis on the disclosure of foreign affiliations and sources of support. OEC provides resources that aim to assist faculty in ensuring relationships with foreign entities comply with federal disclosure requirements. Required disclosures include foreign components and other support.

Foreign Components

A "foreign component" is defined as "any significant scientific element or segment of a project outside of the United States… whether or not grant funds are expended" and must be disclosed on proposals and progress reports. Although there is not always a bright line on what amounts to a foreign component and what doesn't, indicators of a foreign component include foreign collaborations that:

- May result in co-authorship
- Involve use of facilities or instrumentation at a foreign site
- Result in receipt of financial support or resources from a foreign entity.

Foreign components must be disclosed:

- In grant applications or RPPRs
- By listing a "non-US performance site"
- Checking "yes" to the question on the Cover Page supplement Form asking: "Does this project involve activities outside of the United States or partnerships with international collaborators?"

Other Support

USC researchers must disclose all support they receive from other sources when they apply for federal grants. Other support includes resources and/or financial support from domestic or foreign sources. Examples of other support include:

- Grants and contracts (without regard for whether they are administered by USC)
- Faculty or other positions or appointments, regardless of remuneration
- Postdocs, students, or visiting scholars supported by a foreign government or institution
- Income, salary, consulting fees, and honoraria in support of an individual's research endeavors
- Participation in "foreign talent programs" such as China's Thousand Talents Program.
- In-kind support (e.g., office/laboratory space, equipment, supplies, employees).

Other support must be disclosed even if it is provided outside of a researcher's appointment period (e.g., summer for 9-month faculty). Such support should be disclosed on an "Other Support" or "Current

& Pending" form. Consult with OEC if you are unclear about whether an outside activity must be disclosed as "other support".

International Collaborations and Iran

Research and other collaborations with entities and/or individuals who reside in Iran are generally prohibited under the OFAC regulations. For additional information, see OEC's Guidance on Iran and OFAC.

VI. Research Security

USC Research security refers to the protection of the research enterprise from misappropriation, undue foreign influence, and risks to U.S. national or economic security, while maintaining openness, academic freedom, and responsible global collaboration. In an increasingly international research environment, certain activities may create elevated risk, particularly when they involve foreign entities or individuals, emerging or dual-use technologies, sensitive data, or access to specialized research infrastructure. Research security is not intended to limit collaboration, but to ensure that collaborations and research activities are conducted transparently, ethically, and in compliance with applicable requirements. Researchers and research administrators should be aware that activities such as international collaborations, co-authorship with foreign institutions, participation in talent recruitment programs, external academic appointments, hosting visiting scholars, international travel, and the transfer or sharing of research materials, data, or software can raise research security considerations. These risks may be heightened when activities involve countries or entities of concern, advanced or emerging technologies, or restrictions on publication or access. For example, collaboration with or funding from any DoD 1286 List entity will preclude a researcher from obtaining DoD support. Early disclosure of foreign support, affiliations, and collaborations, as well as careful consideration of how and where research data and technologies are accessed or shared, is essential to managing these risks effectively.

In order to promote sound research security practices, researchers must:

- Disclose all current and pending support
- Disclose all professional appointments and affiliations
- Disclose participation in foreign talent or recruitment programs
- Regularly ensure all disclosures are consistent and up to date
- Protect all proprietary, confidential, or export-controlled information
- Comply with all export control requirements
- Seek guidance from OEC prior to engaging in international collaborations, particularly in foreign countries of concern
- Confirm any sponsor-specific participation restrictions (e.g., DoD 1286, nationality restrictions on specific grants)
- Complete research security training in TrojanLearn
- Engage with OEC if you have any questions or need guidance

Research security obligations change frequently. For a complete description of USC's Research Security Program, please also review the Office of Ethics and Compliance website.

VII. USC Export Control Program

USC is committed to complying with all export control regulations applicable to university activity. The following is a description of USC's export control program, which is intended to effectuate this obligation.

A. Policies and Procedures

USC's Export Controls and International Collaborations Policy articulates the university's policy as it relates to research, instruction, healthcare, student outreach, and other strategic partnerships that may create obligations under the export control regulations, the Foreign Corrupt Practices Act (FCPA), and economic and trade sanction regulations. Some of the key areas of activity addressed by the policy include, but are not limited to:

- Research
- Exceptions
- Exception Request Process
- Actual Exports
- Doing Business with International Collaborators
- International Travel Considerations
- Immigration

i. Research

USC generally does not accept research projects that restrict the dissemination of research results or attempt to restrict participation in the research on the basis of nationality. University-based research projects without these restrictions are considered to be Fundamental Research. USC is able to accept pre-publication delays of a limited duration (e.g., 30-90 days) imposed by the sponsor for the purpose of protecting intellectual property rights and/or ensuring against inadvertent disclosure of proprietary or confidential information, if applicable.

ii. Exceptions

Projects with restrictions on dissemination of research results and/or participation in research projects based on nationality are not considered Fundamental Research and are therefore subject to the export control regulations. In limited circumstances, USC may accept these types of restrictions if the investigator submits an exception-to-policy request for the proposal. Therefore, the principal investigator must obtain exceptional approval to proceed, and in the event that approval is granted, adhere to all measures required to meet contractual limitations and Export Control requirements. See Section iii "Exception request process" and the International Collaborations and Export Control policy for additional information about proposal exception requests.

iii. Exception Request Process

When a research sponsor demands the right to approve publication of research outcomes (beyond limited reviews for inadvertent inclusion of proprietary data) and/or restricts access to research on the basis of nationality, the principal investigator ("PI") must submit a request for exception to the Senior Vice President of Research and Innovation. When publication and/or personnel limitations are set forth in a proposal solicitation, exceptions must be requested in advance of proposal submission, providing sufficient time for the review process in advance of the proposal deadline. When limitations are not known until the time of award negotiation, exceptions must be requested and reviewed prior to award execution, allowing sufficient time for the review process. The request must address the following elements:

- Rationale for why the research should take place at USC;
- Steps that will be taken to ensure that USC will comply with applicable personnel and/or publication restrictions;
- Steps to ensure that students participating in the project, if any, will retain their rights to openly publish their own work; and
- Assurance that all project personnel (including faculty, staff, and students) have or will agree in writing to the conditions of the award.

A decision on the proposed exception is made by the Senior Vice President of Research and Innovation upon recommendation of a standing committee of faculty from a broad range of disciplines, except as specified for expedited reviews. If research does not qualify as Fundamental Research, complying with Export Control regulations may involve:

- Limiting foreign national access to all or part of the research; and/or
- Obtaining a license from the Departments of Commerce and/or State, as applicable, before disclosing export-controlled technology, technical data, or software source code to a foreign national in the United States (a Deemed Export), or before sending controlled items or information to a foreign country.

Under university policy, additional measures designed to encourage compliance with Export Control regulations may include:

- Limitations on where the research can take place at USC;
- Implementation of a TCP to protect potentially export-controlled items or information; and
- Adhering to publication and personnel restrictions and the requirements of any university-imposed TCP (if applicable).

The Senior Vice President of Research and Innovation, or their designee, is authorized to grant an expedited approval without committee review when both of the following conditions apply:

- Work will be conducted in its entirety at either the Institute for Creative Technologies ("ICT") or the Information Sciences Institute ("ISI") and be subject to a TCP to ensure compliance with applicable restrictions; and
- The PI has notified the Senior Vice President of Research and Innovation about the intent to include students in the project. Upon award of funding, the Office of Research and OEC will engage with the Graduate School to ensure that each student is made fully aware of, and agrees to, possible restrictions on publications resulting from the work on the project, and at the time the student consents to taking on restricted research (under stated publication restrictions), a plan for academic oversight is formulated that protects and outlines the student's pathway to degree completion and publications. The consent needs to be in place prior to the time the student starts work on the project.

The Senior Vice President of Research and Innovation and/or standing committee may require that additional conditions be met, including but not limited to obtaining required licenses from the Departments of Commerce and/or State, as applicable, and implementation of a TCP to protect export-controlled items or information.

In the event that an expedited exception is denied by the Senior Vice President of Research and Innovation or their designee, the Principal Investigator will be given the opportunity for full committee review, at their request. Please see the International Collaborations and Export Controls policy for additional information about the proposal exception request process.

iv. Actual Exports

All overseas shipments constitute exports that are subject to the EAR or ITAR, and may require specific government authorization before hardware, software, or related technical data may be exported. A "shipment" in this context includes both sending an item abroad using a freight forwarder such as FedEx or DHL, as well as personally taking an item abroad on an overseas trip. These rules apply in the research context even if the research is considered "fundamental", because the fundamental research exclusion only protects the ability to freely share the results of research in publications and presentations. The exclusion does not include international shipments of materials, items, technology, or software generated in the course of fundamental research.

Keep in mind that if commercial items are not specifically identified in the EAR, they fall into a "basket" category known as "EAR99." This basket category includes a wide range of common items, such as pencils, Band-Aids, automobiles, and household appliances. EAR99 items generally can be exported without a prior license from the Commerce Department, except to OFAC-sanctioned countries, entities, and individuals. (Click on the OFAC link or contact OEC to determine whether a particular country, entity, or individual is sanctioned.)

If you intend to ship an item overseas, consult with OEC before doing so.

v. Doing Business with International Collaborators

The Office of the Vice President for Strategic and Global Initiatives must approve all initiatives that involve establishment of an overseas presence or international collaboration with any overseas university, institution, or governmental entity, excluding sponsored research agreements and technology licenses.

USC employees and third-party subcontractors are prohibited from directly or indirectly giving or receiving improper payments or other benefits to or from a Foreign Official to gain a commercial or other advantage in violation of the FCPA. The types of payments covered by the FCPA are broad and cover anything that may confer a benefit on someone in a position to provide a commercial or other advantage to USC. See Section II.D of this document for additional information.

vi. International Travel

Travel outside the United States can present a range of legal and safety issues for faculty, staff, and students under United States law and university policy. Please review the material available at OEC's website, https://oec.usc.edu/international-activity/international-travel-guidance/, and click on the links provided for additional guidance. The U.S. State Department also publishes a "Traveler's Checklist" that provides helpful tips regarding international travel: https://travel.state.gov/content/travel/en/international-travel/before-you-go/travelers-checklist.html.

Export-controlled information and international travel

Traveling with information that falls within the categories of Fundamental Research or published/publicly available information, as described in Section III of this document, does not raise export control concerns in most cases. However, if the university has accepted restrictions on the free dissemination of the information received or generated in the course of a research project or has agreed to research personnel access restrictions (usually on the basis of nationality), then export control regulations apply, and an export license may be required prior to taking the information outside the United States. Prior to bringing abroad information where the university has accepted restrictions on dissemination or access, please contact OEC.

OFAC countries

Travel to OFAC-sanctioned countries (e.g., Iran, Cuba, North Korea) may be prohibited or severely restricted. If you plan to travel to one of these destinations, contact the Office of Ethics and Compliance for guidance well in advance of the anticipated travel.

Additionally, research and other collaborations with entities and/or individuals who reside in Iran are generally prohibited under the OFAC regulations. OFAC usually requires a license prior to travel to Iran to attend or present at an open conference. Similarly, a presentation via webinar to a live audience that includes individuals inside Iran would also require a license from OFAC. Because it can be a lengthy process to obtain a license, contact the Office of Culture, Ethics, and Compliance at least six months prior to the intended travel. For additional information, see OEC's Guidance on Iran and OFAC.

Devices and Information Security

USC personnel can bring their devices containing data storage as long as they do not contain any export-controlled technology or non-commercial, special purpose encryption software. If a device has something other than standard commercial or "mass market" encryption software, an export license may be required before taking that device overseas. International travel also poses unique information security risks compared to domestic travel. All university faculty, staff, and students should adhere to the information security practices outlined in OEC's International Travel Guidance in order to protect the security and confidentiality of the information they will bring with them when they travel overseas. USC Office of Cybersecurity (USCCyber) offers international travel information security guidance resources, available at https://sites.usc.edu/trojansecure/usc-information-security-international-travel-guidance/ (USC login required).

vii. Immigration

OEC works with USC's Visa services offices to ensure compliance with federal export control regulations around sharing proprietary, confidential, or otherwise controlled information, source code, or technology with foreign nationals located in the U.S. or abroad.

Under federal export control regulations, exports are considered to be an export to the foreign person's country of origin and are subject to the same rules that an actual export would be. Deemed exports can be conveyed through visual inspection, oral exchange, electronic/digital exchange, or made available by practice/application (e.g., training).

B. Training and Education

The primary goal of export controls education and training at USC is to increase awareness and maintain compliance with U.S. export control and trade sanctions laws. Export control training is designed to educate the USC community on its responsibilities under these laws and the procedures in place for ensuring compliance. It is especially critical that faculty and administrative staff who direct or participate in research projects involving export-controlled goods, technology, or software participate in training provided through OEC.

Live Training

OEC frequently conducts individual and group training sessions on Export Controls and International Collaborations, including for department and school/unit meetings, faculty or staff meetings, and specialized group trainings. OEC also initiates training in schools/units where the research is most impacted by export controls. To schedule a presentation, contact OEC at compliance@usc.edu.

Online Training

USC's TrojanLearn course "Export Controls at USC: An Introduction" is designed to enable researchers and other employees to understand the kinds of activities that may raise export control considerations so that they can proactively engage with OEC for guidance on whether the regulations apply in specific situations. The target audience for this course is USC faculty and staff who conduct restricted research, and research units and other departments affected by export controls.

To access the TrojanLearn course, click the link below (login required). After completing the course, the results will be recorded on the user's TrojanLearn transcript.

Export Controls at USC: An Introduction

Educational Resources

The OEC Export Controls webpage includes an overview of relevant information and FAQs, as well as downloadable one-sheet guidance on export control-related topics such as technology transfer, technology control plans, international travel, controlled equipment use, and projects with restrictions. OEC also has a one-sheet guidance library – Research Lifecycle: Compliance Guidance – that provides targeted and issue-specific guidance regarding key compliance obligations in order to assist researchers and administrators in the shared endeavor to promote the ethical and compliant conduct of research at USC. Each one-sheet provides an overview of the most important requirements to keep in mind, links to relevant university resources where additional information can be found, and key contacts to reach out to with additional questions.

C. Monitoring and Auditing

i. Research

OEC periodically monitors restricted research projects for compliance with management plans implemented by the International Collaborations and Export Controls Committee. Such monitoring includes confirming that the measures implemented in any Technology Control Plan (TCP) have been put in place, such as physical security controls and information security controls. OEC also monitors on whether there have been any changes to the Statement of Work (SOW) or project personnel.

OEC works with university partners to monitor on research activity with export control considerations. Such monitoring areas include, but are not limited to:

- International partnerships/MOUs, in partnership with USC Global
- Technology transfers, including the receipt of proprietary technical data, in partnership with USC Stevens Center for Innovation
- Research data security obligations, in partnership with the Office of the Chief Information Security Officer (OCISO)
- Restricted research projects, in partnership with the Information Sciences Institute (ISI) and the Institute for Creative Technologies (ICT)

ii. International Travel

OEC performs periodic monitoring on international travel to identify instances of travel that may have export control implications and provides guidance as needed. International travel monitoring supports export controls/sanctions compliance by identifying cases such as the following:

- Travel abroad as part of a sponsored project with restrictions
- Travel abroad and hand-carrying or shipping items/technology beyond the "Tools of the Trade" (laptops and other computing and data storage devices that are all standard, off-the-shelf products generally available to the public through retail outlets, containing an operating system and software applications that are generally available to the public)
- Travel abroad with export-controlled or restricted data sets
- Travel to an OFAC-sanctioned country (e.g., Iran)

iii. Immigration

OEC partners with the Office of International Studies (J-1 "visiting scholar" visas) and Faculty and Staff Visa Services (H-1B visas) to identify export control issues related to immigration, such as visiting scholars and workers who might have access to controlled information or visiting scholars or workers who are receiving support from a foreign entity.

When the responses indicate possible export control implications, OIS and FSVS contact OEC for further review and assistance. These offices support OEC's monitoring efforts by sharing relevant reports.

iv. Restricted Party Screening

The U.S. Department of Commerce, the U.S. Department of State, and the U.S. Department of the Treasury maintain certain sanctions and other trade restrictions against lists of individuals, entities, and organizations that have violated U.S. export control laws, have participated in proliferation activities, or have been determined to be terrorists, terrorist organizations affiliated with certain sanctioned

governments, and for other reasons. These lists are collectively known as "Restricted Parties Lists." The most significant of these are OFAC's lists of sanctioned entities and individuals, including the Specially Designated Nationals and Blocked Persons (SDN) List, Foreign Sanctions Evaders (FSE) List, and the Sectoral Sanctions Identification (SSI) List. The OEC website has a Restricted Parties page with guidance, resources, FAQs, and links to the highest-risk restricted entity lists such as the DoD 1286 List and DoD 1260H List.

OEC maintains a screening tool allowing for prompt identification of any sanctions or export controls that may apply to a given entity or individual. Please reach out to OEC with any questions about whether a transaction with a particular entity or individual may be subject to restrictions.

v. Controlled Equipment

USC Equipment Management tracks equipment purchases made across all USC campuses and locations. It also conducts a biennial equipment inventory. OEC reviews the equipment inventory to assess potentially export-controlled or higher-risk equipment on campus and monitors the use of such equipment, including follow-up with the user as necessary. OEC periodically surveys users of higher-risk or potentially controlled equipment to help identify how people are using the item and who has access to the item.

D. Enforcing Standards Through Publicized Disciplinary Guidelines

Under federal law, failure to comply with Export Controls regulations can result in severe fines and even imprisonment. For example, violations of federal law can result in civil penalties of up to $500,000 per violation and criminal penalties of up to $1 million per violation and up to twenty years in prison.

Under USC policy, failure to comply with Export Controls and/or USC-imposed requirements may also be cause for disciplinary action up through and including termination. Possible violations include, but are not limited to, engaging in an export without obtaining a license, failing to obtain appropriate authorization from OFAC prior to undertaking travel to sanctioned countries, giving or receiving improper payments or other benefits to a Foreign Official to gain a commercial or other advantage in violation of the FCPA, and failing to adhere to university-imposed measures intended to mitigate potential export risk.

Sanctions for violations by a faculty member will observe all provisions of the Faculty Handbook under Section 6-AA (2). Sanctions for violations of this policy for staff or other non-faculty employees will observe all provisions of the staff employment policies. Sanctions for violations by students will observe all provisions contained in the USC Student Handbook (formerly SCampus).

E. Preventing And Detecting Instances of Non-Compliance

OEC's monitoring efforts as described above are designed to prevent and detect instances of non-compliance. Each USC employee also has the responsibility to report possible violations of United States export control laws or regulations. Suspected violations should be reported to OEC, together with the details of the suspected violation. Suspected violations may be reported to compliance@usc.edu. Possible violations of United States export control laws or regulations will be assessed by OEC.

F. Record-keeping

The University of Southern California is subject to several regulatory recordkeeping requirements related to its export activities. The ITAR [22 CFR 122.5], the EAR [15 CFR 762.2], and OFAC [31 CFR 501.601] require that records be kept reflecting the export, reexport, and temporary import of defense articles, defense services, dual use commodities and related technologies. Types of records to be maintained are based on the individual controlled items or activities.

The storage of appropriate records related to exports, either originals or backups, may be maintained by both the individual unit and OEC. This is generally (and preferably) done by keeping originals locally and providing an electronic summary to OEC. Records must be kept in a manner that facilitates the ability to retrieve them for any purpose, especially during an internal or U.S. Government audit.

Unless specified otherwise, all records shall be retained for no less than five (5) years after the date of export, reexport, the project's technology control plan (TCP) or license termination date, or any other aspect of the transaction, whichever is later.

VIII. APPENDICES

A. TCP Template
B. NSDD 189 Memo
C. International Collaborations and Export Controls Policy

A. TCP Template

UNIVERSITY OF SOUTHERN CALIFORNIA

Technology Control Plan

I. Institutional Commitment

The University of Southern California is committed to complying with export control laws, which are federal regulations that control the conditions under which certain information, technologies, and commodities can be transmitted overseas to anyone, including U.S. citizens, or to a foreign national on U.S. soil. The university is also committed to complying with access and distribution restrictions imposed by federal sponsors (including DoD and DHS) to facilitate control, distribution, and release of information controlled for reasons of national security, including but not limited to Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

Implementation of required security measures to meet export control obligations and/or sponsor cybersecurity mandates is a shared responsibility that includes central administration, school/unit administration, and researchers and research personnel. This Technology Control Plan ("TCP") is written explicitly for all research and non-research activity where the university agrees to implement access or dissemination controls on data received, accessed, or generated by USC faculty, staff, Graduate Research Assistances, students, consultants, temporary hires, and/or visitors working in support of such projects ("USC Personnel"). This TCP is intended for projects or services that must comply with federal information security requirements (e.g., NIST SP 800-171, NIST SP 800-53, and FISMA, etc.). NIST SP 800-171 is a special publication issued by the National Institute of Standards and Technology (NIST) that outlines cybersecurity requirements for protecting Controlled Unclassified Information (CUI) in non-federal information systems and organizations.

II. Scope

This Technology Control Plan (TCP) applies to "Covered Projects", defined as research and non-research related contracts where the sponsor requires, either alone or in combination:

- Prior approval on any publications, presentations, or other public disclosures of project-related information.
- The right to approve project personnel prior to their participation.
- Compliance with federal information security standards (NIST SP 800-171, NIST SP 800-53, or FISMA), including but not limited to requirements that USC demonstrate

compliance with the Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC) framework and/or other information security requirements.

- That USC will access, receive, or generate information subject to access or dissemination controls for reasons of national security and/or export controls.
- Any other restricted handling and/or dissemination controls for reasons of national security or export controls.

III. Cybersecurity Requirements

In connection with Covered Projects (including both research- and non-research-related contracts), sponsors commonly require the implementation of heightened cybersecurity measures to protect against unauthorized disclosure or compromise of data. For Covered Projects sponsored by the Department of Defense ("DoD"), these heightened cybersecurity measures usually require adherence to NIST SP 800-171. NIST SP 800-171 is comprised of fourteen (14) control families that require the implementation of administrative, technical, and physical measures to ensure that CUI is appropriately secure and meets DoD cybersecurity requirements.[1] In order to meet these requirements, USC Personnel must adhere to the requirements of this TCP as well as any required measures mandated by the local school or unit where the Covered Project occurs.

Covered Projects that require adherence to NIST SP 800-171 must be performed in a research location that has either:

- Submitted a System Security Plan (SSP) to the DoD and attested that NIST SP 800-171 requirements have been sufficiently met and will continue to be met in the future; or
- Obtained certification under the CMMC framework and have attested that NIST SP 800-171 requirements have been sufficiently met and will continue to be met in the future.

The determination as to whether a specific project requires USC to submit an SSP to DoD or, alternatively, requires USC to obtain or demonstrate third-party certification under the CMMC framework, is project-specific and derives from the contractual obligations imposed by DoD on USC and applicable research projects. Additionally, it is important to note that other frameworks like NIST SP 800-53 or FISMA are less common but may have similar requirements that must be evaluated by Compliance._Please see Section V. (Project-specific requirements) below for the IT security standard(s) applicable to this Covered Project and for identification of the information security environment where this Covered Project must be performed.

[1] The NIST SP 800-171 control families are Access Control, Awareness and Training, Audit and Accountability, Configuration Management, Identification and Authentication, Incident Response, Maintenance, Media Protection, Personnel Security, Physical Protection, Risk Assessment, Security Assessment, System and Communications Protection, and System and Information Integrity.

IV. Principal Investigator and Research Team ("Authorized Personnel") Responsibilities

a. Adherence to information security administrative and technical controls

As noted above, all sponsored projects to which this TCP applies must be performed in a compliant IT environment that has implemented the relevant information security controls as stated in contractual requirements (e.g., has submitted a System Security Plan (SSP) or has obtained certification under the CMMC framework). Affirmation of compliance by the local IT team who oversees the research location is required prior to beginning work on an awarded project. In the case that an SSP is required, it is the responsibility of the responsible IT team to submit and maintain all documentation required in connection with the development and implementation of the SSP.

b. Education and Training

All Authorized Personnel involved in the conduct or administrative support of restricted research projects subject to NIST SP 800-171 or other applicable information security requirements must receive appropriate training to effectively carry out their assigned information security-related duties and responsibilities. The extent of training required depends on the role that Authorized Personnel perform. For example, information security professionals require additional and more detailed training than researchers and other administrators. It is essential to validate that training aligns with the relevant standards and frameworks, including NIST SP 800-171, NIST SP 800-53, and FISMA. Please see below for the education and training requirements applicable to the Authorized Personnel for this Covered Project.

c. Identification and Marking of Restricted Information

Proper tagging and marking of restricted information types, such as Controlled Unclassified Information (CUI), is essential for ensuring the appropriate protection and handling of sensitive information. All Authorized Personnel must adhere to the identification and marking standards set forth in USC's Document and Media Labeling Standard, a copy of which will be made available to Authorized Personnel in connection with this TCP.

d. Publication of Research Outputs

All sponsor requirements regarding review and approval of any intended output from the Covered Project named in this TCP must be followed, including any and all requirements on timing, implementing requested changes, and adhering to all limitations associated with the disclosure of research output related to or arising from this Covered Project. Research and non-research related outputs include all presentations, publications, or any other form of disclosure (written or oral) that the research team would like to undertake arising out of

activity performed in connection with the project identified below. This includes publications disseminated internally, such as within the School/Unit.

e. Access Control

For Covered Projects subject to information security requirements, the Access Control family in NIST SP 800-171 and NIST SP 800-53 specifies a set of security requirements designed to protect project data by restricting access to authorized users and processes. At minimum, these requirements include:

- Limiting access to authorized users
- Limiting use of external connections
- Requiring multi-factor authentication
- Controlling unsuccessful login attempts

Authorized Personnel must adhere to all access control measures implemented in the IT security environment applicable to this Covered Project, as specified in this TCP.

f. Physical Security

For Covered Projects that are subject to NIST SP 800-171, NIST SP 800-53, or FISMA requirements, physical security mandates safeguarding of facilities, equipment, and information from unauthorized physical access. At minimum, this includes:

- Limiting physical access to systems, equipment, and storage areas containing CUI or FCI to the Authorized Personnel identified in this TCP.
- Protecting and monitoring physical access points to prevent unauthorized access to systems and data
- Escorting visitors when accessing sensitive areas
- Maintaining audit logs of physical access to facilities, systems, and areas where CUI is stored or processed.

g. Incident Reporting

USC is required to adhere to the DoD requirement that data incidents, including data breaches, be disclosed to DoD within 72 hours. In reviewing a data incident, USC is required to conduct a thorough review for evidence of compromise of CUI, including but not limited to identifying compromised computers, servers, specific data, and user accounts. This review will also include analyzing USC's information system(s) that were part of the cyber incident, as well as other information systems on USC's network that may have been accessed, in order to

identify compromised information that may affect USC's ability to provide operationally critical support as a result of the incident.

The Principal Investigator (PI) and research team must adhere to all behaviors set forth in applicable training and as contained in USC's Incident Response protocol and promptly identify the IT security contact designated in this plan, along with the USC Office of Cybersecurity (USCCyber) and the Office of Culture, Ethics, and Compliance (OCEC) immediately upon discovery of a potential data security incident.

V. Project-specific Requirements

The requirements below apply to the identified project to which this TCP applies.

Project Information

- Project Title:
- Cayuse Project Number (if applicable):
- Sponsor/Customer:
- Restricted clause or reference to information security or other requirements contained within the contract and/or grant:

Authorized Personnel

- Principal Investigator:
  - Telephone Number:
  - E-mail address:
  - Building/room location(s) where project will be performed:
- Other research personnel by title, role, and USC status (faculty/staff/student):
- Administrative personnel (including research administrators and IT/IT security personnel):

Project-specific Requirements

- *Project overview*: [Brief overview of the project, including what sensitive data and materials will be provided/generated and how they will be delivered]

- *Applicable IT security environment*: [Reference applicable compliant IT environment]

- *Disclosure limitations*: [Reference applicable disclosure standards – e.g., no disclosure without sponsor approval; disclosure after pre-publication review for restricted outputs, etc.]

- *Applicable EAR/ITAR export control classification(s), if applicable/known*: [Reference applicable USML category or CCL ECCN]

- *Education and training*: [Insert all training requirements by personnel name derived from role which identified personnel perform]

- *Attestation*: All personnel must confirm that they have received a copy of this TCP and agree to adhere to its requirements. A template copy of this attestation is appended as Attachment A to this TCP.

ATTACHMENT A

Project Title _____

Principal Investigator _____

This is to acknowledge that I have been briefed that this TCP applies to the project listed above. I understand that my participation on this project may involve the receipt or use of technology, items, software, hardware, technical data or other information that is considered to be export-controlled, non-public, and/or constitutes Controlled Unclassified Information (CUI) information or Federal Contract Information (FCI) that is subject to access, use, and disclosure limitations for reasons of national security and/or export control, as specified in this TCP. I agree to adhere to all project-specific requirements set forth in this TCP with respect to administrative, technical, and physical controls to ensure that project information is appropriately secured and meets sponsor-mandated cybersecurity requirements. Furthermore, I understand that I may not disclose, orally or visually or transfer by any means, export-controlled technology or technical data to a non-US Person located inside or outside the US without a license or applicable exemption. I understand that all non-US students, visitors, staff, postdocs, or any other person must receive preauthorization consistent with the requirements of this TCP before accessing export-controlled materials or data. I have discussed this TCP and its requirements with the Responsible Person for this project and I agree to follow all of the procedures contained in the TCP. If I have any questions about the applicability of the TCP to this project, I will contact the Responsible Person for guidance.

Signature _____

Printed Name _____

Date _____

B. National Security Decision Directive (NSDD) 189 Memo

[National Security Decision Directives (NSDDs)]

[stamped:] UNCLASSIFIED

September 21, 1985

NATIONAL POLICY ON THE TRANSFER OF SCIENTIFIC, TECHNICAL AND ENGINEERING INFORMATION

I. PURPOSE

This directive establishes national policy for controlling the flow of science, technology, and engineering information produced in federally-funded fundamental research at colleges, universities, and laboratories. Fundamental research is defined as follows:

> "'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 from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons."

II. BACKGROUND

The acquisition of advanced technology from the United States by Eastern Bloc nations for the purpose of enhancing their military capabilities poses a significant

threat to our national security. Intelligence studies indicate a small but significant target of the Eastern Bloc intelligence gathering effort is science and engineering research performed at universities and federal laboratories. At the same time, our leadership position in science and technology is an essential element in our economic and physical security. The strength of American science requires a research environment conducive to creativity, an environment in which the free exchange of ideas is a vital component.

In 1982, the Department of Defense and National Science Foundation sponsored a National Academy of Sciences study of the need for controls on scientific information. This study was chaired by Dr. Dale Corson, President Emeritus of Cornell University. It concluded that, while there has been a significant transfer of U.S. technology to the Soviet Union, the transfer has occurred through many routes with universities and open scientific communication of fundamental research being a minor contributor. Yet as the emerging government-university-industry partnership in research activities continues to grow, a more significant problem may well develop.

III. **POLICY**

It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted. It is also the policy of this Administration that, where the national security requires control, the mechanism for control of information generated during federally-funded fundamental research in science, technology and engineering at colleges, universities and laboratories is classification. Each federal government agency is responsible for: a) determining whether classification is

appropriate prior to the award of a research grant, contract, or cooperative agreement and, if so, controlling the research results through standard classification procedures; b) periodically reviewing all research grants, contracts, or cooperative agreements for potential classification. No restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification, except as provided in applicable U.S. Statutes.

[stamped:] UNCLASSIFIED

C. International Collaborations and Export Controls Policy

The most up-to-date version of the International Collaborations and Export Controls policy is available on USC's Policies and Policy Governance webpage (USC login required): https://policy.usc.edu/international-collaborations-and-export-controls/.