

EXPORT CONTROL COMPLIANCE IN AN ACADEMIC SETTING: RISK AND RESPONSE

07B. EXPORT AND TRADE CONTROLS:
ITAR, EAR AND OFAC COMPLIANCE

November 9-12, 2011

Steven B. Eisner
Stanford University
Stanford, California

I. Introduction

This paper¹ addresses specific export control compliance risks presented within the context of higher education in the U.S. Suggested elements of a university export control compliance program, applicable to both fundamental research institutions and those that accept restricted research, are provided. The paper also provides recommendations and resources on how to identify export control risks, such as those created by industry/university collaborations and outside faculty activity, and compliance mechanisms to mitigate those risks. Finally, the paper considers institutional best practices in response to compliance risk when university activity becomes subject to U.S. export control regulations.

II. Export Control Compliance in an Academic Setting

A university export control compliance program can vary in scope and content from one institution to another depending on 1) the institution's volume of sponsored research activity; 2) whether it operates exclusively under the fundamental research regulatory safe harbor; and 3) its organization and culture. Simply put, "one size does not fit all" when it comes to an export control management system in U.S. higher education. An export control compliance program at a state university that takes restricted research and may operate under a hierarchical, centralized compliance system will look quite different than that at a highly decentralized, departmentally-driven private university that by policy will only perform openly conducted and unrestricted fundamental research. One program may be run out of the sponsored research office, another out of legal, and another from within the Office of the Vice Provost for Research. Each approach is satisfactory, as long as the institution can demonstrate that it has a system in place to identify and mitigate export control compliance risk.

¹ This paper is adapted from materials developed and presented by the author and Gretta Rowold, Executive Director of Export Compliance at the University of Oklahoma, at a concurrent session of the National Council of University Research Administrators (NCURA) Annual Meeting in Washington, DC in October 2009.

A starting point and framework for an effective university compliance program is presented by the 2007 U.S. Sentencing Commission Guidelines at Section 8B2.1. These elements are as follows:

- Standards and Procedures
- Governance, Organization and Reporting
- Assignment of Substantial Authority
- Training and Education
- Monitoring and Auditing, Program Assessment, & Helpline
- Consistent Enforcement and Discipline
- Responses to Noncompliance and Program Modifications

The U.S Sentencing Commission Guideline elements above are intended to apply to both U.S. industry and academia. Of course, by necessity a university export compliance management program will differ in many respects from an industry export compliance management program: unlike industry where protection of generated information is paramount, university culture is predicated on openness and a “publish or perish” environment. And whereas U.S. corporations are generally rule and enforcement driven, U.S. universities generally entail decentralized and entrepreneurial academic structures in which Principal Investigators, who are trained to question authority and the status quo as a foundation for professional advancement, are often delegated compliance oversight. It can be argued that a university’s export control compliance program is only as good as its ability to obtain faculty understanding, goodwill and support.

What becomes clear, then, is what will not work when it comes to a university export control compliance program:

- Taking a commercial/industrial export control compliance program and applying it directly to one’s own;
- Taking another academic institution’s export control compliance program and applying it directly to one’s own;
- Developing a university export control compliance program without understanding what is regulated; and
- Employing an existing, but outdated and hence inadequate export management system.

III. Suggested Elements for an Academic Export Control Compliance Program

This paper suggests nine elements to be incorporated into a university export control compliance program. These elements apply regardless of whether the institution conducts only fundamental research or performs restricted work. These nine elements are:

- Identifying Responsible Export Compliance Personnel
- Management Commitment and Statement of Policy
- Identifying High Risk Activities
- Developing a Written Plan and Documentation
- Training
- Recordkeeping
- Monitoring and Auditing
- Handling Problems and Violations
- Corrective Actions

This paper is directed to a discussion of the first six elements listed above, and addresses each in sequence. The last three elements – Monitoring and Auditing, Handling Problems and Violations, and Corrective Actions – are deferred to my NACUA workshop colleague, Mr. John Barker, Esq. of Arnold & Porter, who will comment upon these elements relative to recent Federal agency enforcement actions and university considerations in identifying and responding to potential of export control compliance violations.

A. Identifying Responsible Export Compliance Personnel

One of the simplest, yet perhaps most effective, steps a university can take to manage export control compliance risk is to identify a single individual with overall responsibility for export control compliance on campus. This person should, at the minimum, have taken the Bureau of Industry and Security's (BIS) introductory seminar "Complying with US Export Controls" that is offered in multiple cities and dates over the course of the year. BIS also offers an on-line training room with videos and PowerPoint presentations at http://www.bis.doc.gov/seminarsand_training/seminar-training.htm.

The university should take steps to make it known to faculty and students that the responsible export control official should be the point of contact for all export control questions or issues, and the official's contact information should be disseminated widely. This individual should be granted "substantial authority" to make independent decisions void of organizational conflicts of interest. Ideally, the official should have direct reporting lines to the university's executive level. In cases where the university is registered with the U.S. Department of State and conducts research subject to the International Traffic in Arms Regulations,² the individual responsible for export control compliance should serve as the institution's "Empowered Official" with authority "to inquire into any aspect of a proposed export and to verify the legality and accuracy of the information submitted for a transaction."

² 22 CFR 120-130

B. Management Commitment and Statement of Policy

A university export compliance program should include a policy statement from the highest levels of the institution. This statement, generally in the form of a memorandum from university leadership, should be distributed via email to faculty and posted on a university website. The statement should include an attestation that the university takes export control compliance seriously, is committed to upholding the laws of the United States, and that serious consequences may result from non-compliance.

Examples of 1) a general statement of a commitment to export compliance and 2) a statement of potential penalties resulting from non-compliance follow, respectively:

- 1) “The University recognizes that certain types of equipment, software and technology can be regulated by the U.S. government, and in some instances this affects the university’s, and its employees, ability to conduct research in a completely open environment. The University remains dedicated to its long-standing traditions of academic freedom and openness in research, but recognizes and is committed to complying with the various laws and regulations known as export controls. Compliance with export controls is not only important to the continued success of the University, but also to the national security and foreign policy interests of the United States of America.”
- 2) “It is the responsibility of all University staff and faculty members, students and researchers to maintain a working knowledge of export control regulations that apply to his or her situation. Under no circumstances should a violation of export controls occur. Non-compliance with these regulations may subject the University and the individuals involved to civil and criminal penalties including fines, prison time and permanent denial of export privileges. In addition, individuals found to have willfully violated university export control policies and procedures may be sanctioned, suspended or dismissed.”

C. Identifying High Risk Activities

The fact is that a university will never capture and control export control risk in its entirety. There are just too many variables and circumstances in a campus environment for all regulated items, activities and technology to be identified. What can be identified, however, are the specific export control risks with which the university is presented. A university export control compliance program must then prioritize those risks on the basis of their greatest liability and the

likelihood of their occurrence. Once the university has an understanding of those export control risks with which it is presented (each institution will have varying risks based on its research portfolio and organizational structure), it can then decide which risks it wishes to avoid, transfer, mitigate or accept. Central to that effort is ensuring that export control personnel understand what is regulated for export control purposes and what is not.

Understanding the particular export control risks that are presented to a university means understanding the ways in which the university is “exporting”. Exports can occur through international shipments and handcarries (physical exports), through “deemed” exports (domestic transfers of technology to foreign nationals), through international exports of technology (tangible or intangible), and exports of services (for example, technical and/or financial assistance and training).

There are common areas of heightened export control compliance risk within U.S. higher education that can be identified upfront. These risks are present regardless of whether your institution is a fundamental research university or a university that accepts export controlled projects. Examples of such common areas and activities within academia that present increased export control exposure are:

- A. Schools of Engineering and Applied Sciences
 - Departments of Astronautics and Aeronautics (ITAR risk)
 - Electrical and Mechanical Engineering
 - Computer Science
 - Is Functional Strong Encryption Code Being Developed?
- B. Life Science Research that Incorporates the Use of Pathogens and Toxins
 - Schools of Medicine (Immunology and Microbiology)
- C. Non-Disclosure Agreements/Material Transfer Agreements
 - Implies Presence of Disclosure-Restricted Technical Information, Software Code or Materials on Campus
 - Fundamental Research Safe Harbor Does Not Apply
 - Tip: Use an H1-B Deemed Export Questionnaire³ to Identify Presence of Disclosure-Restricted Technical Information and Software Code on Campus
 - Tip: Develop a Dedicated Webpage that Addresses the Handling of Non-Disclosure Agreements⁴ Consistent With University Policies and Procedures

³ See Exhibit 1

⁴ See Exhibit 2

D. Distance Learning Programs

- Acceptance of Tuition Fees from Persons in Embargoed Countries?
- Fundamental Research Exclusion Does Not Apply to Live Streaming Classes

E. Procurement/Purchasing/Property

- Is ITAR-Controlled Capital Equipment or Are ITAR-Controlled Components Being Purchased for Fundamental Research or Export Controlled Projects?
- Is University Property or Software Being Loaned Internationally?
 - Tip: Work with Vendors to Obtain ECCNs and ITAR Categories
 - Tip: Use an International Property Disposal/Loan Form⁵ to Document Due Diligence
 - Tip: Create a Property Export Control Checklist to Assess Eligibility of Temporary Exports Under License Exception TMP⁶

F. International Visitors Programs

- Sponsored/Exchange Visitors: Are U.S. Government Restricted Parties Meeting with Faculty and/or Visiting University Research Laboratories?
 - Tip: Use Restricted Party Screening Software for International Visitors as a Best Practice to Document Due Diligence

G. Technology Transfer/Industrial Contracts Offices

- Software, IP Licensing and Industry-Sponsored Agreements
 - Such Agreements Usually Include Clauses that Assume Export Controlled or Disclosure-Restricted Activity

H. Physical Exports

- Does the Item being Shipped or Handcarried Require an Export License?⁷
- Is the Recipient on a U.S Government Restricted Party List?

⁵ See Exhibit 3

⁶ See Exhibit 4

⁷ Stanford's copyrighted [Export Controls Decision Tree](#) is available for use by the University community via submission of a written request to the author at steve.eisner@stanford.edu.

- Tip: Use Restricted Party Screening Software for International Shipments (Screen Recipient and Recipient’s Organization) to Document Due Diligence
- Is there a Prohibited End-Use Involved⁸?

D. Developing a Written Plan and Documentation

It is important for any university export control compliance program to document its policies and procedures in a written fashion. A variety of formats can be used for this purpose, from a memorandum to a dedicated export control website, or from a declaration of export control requirements in a faculty or research policy handbook to a formal and detailed Internal Export Compliance Plan. Again, the scope and content of the written plan will be dependent on the degree of export control risk that the university’s policies, its culture, and its research activity present.

Stanford University has found that written procedures, decision matrices and checklists are paramount during the proposal review process. University export control compliance is best served at the “point of attack” – if export control personnel are able to identify and mitigate risk before research activity ever takes place, the salutary effects are two-fold: export control infractions will be contained and proposing faculty will in most instances not be unduly surprised by unpalatable (or worse, unacceptable) grant or contract export control terms at the time of award.

Stanford, as an institution that by policy only conducts basic and applied “fundamental research” as defined by the Export Administration Regulations⁹ and the ITAR, provides an Openness in Research checklist¹⁰ as an export control compliance tool for local research administration staff during the proposal development process. In addition, the University’s standardized Proposal Development and Routing Form (PDRF), a primary component of the web-based Stanford Electronic Research Administration (SeRA) module used by local and centralized sponsored administration staff, asks a series of export control questions that address the use of disclosure-restricted technical information, software code or ITAR defense articles in the conduct of the proposed research project. Because ITAR compliance risk represents the greatest threat to Stanford’s policies on openness¹¹ and non-discrimination¹² in research,

⁸ See the General Prohibitions at Part 736 of the EAR and general end-use restrictions at EAR Part 744.

⁹ 15 CFR 730-774

¹⁰ See Exhibit 5

¹¹ RPH 2.6 (<http://rph.stanford.edu/2-6.html>)

Stanford's export control officer reviews all research proposals, including SBIRs and STTRs, for which the Department of Defense and NASA are either Prime or direct sponsors. For that purpose, Stanford's export control officer developed an export control proposal review and submission approval matrix¹³ for Stanford's Office of Sponsored Research so that he would be routed proposals that met pre-specified conditions. During his review, the export control officer pays particular attention to each proposal's Scope of Work, to ensure that the activity meets DoD's and NASA's definitions of "fundamental research"¹⁴.

E. Training

Similar to the manner whereby university export control personnel should conduct a high risk assessment to identify export control activities that present heightened export compliance risk, export control personnel should revisit their high risk assessment to identify those departments and research groups most in need of export control training. The objective here is to help educate faculty and staff who can help minimize export control risk.

Because of the large number of foreign students in U.S higher education, and because of the increasingly globalized nature of research collaboration, university export control training should focus initially on 1) deemed exports and 2) physical exports. Sponsored research training should cover those Federal solicitation and contract terms that negate a university's ability to invoke the fundamental research safe harbor (e.g. troublesome clauses such as DFARS 252.204-7000). Faculty training at fundamental research institutions should address export control "flags" that can arise in the conduct of fundamental research, such as the need for an industry sponsor to share proprietary background IP or ITAR controlled hardware/software with a university research group. Faculty training at institutions that accept export controlled research should include content that explains the appropriate use of common EAR license exceptions¹⁵ (TSR, ENC) and ITAR exemptions (University Bona Fide Full Time Regular Employee Exemption) and their limitations. Faculty departmental staff meetings tend to be an excellent forum for outreach.

¹² RPH 10.4 (<http://rph.stanford.edu/10-4.html>)

¹³ See Exhibit 6

¹⁴ The ITAR generally defines university "fundamental research" as activity described under Budget Category 1 ("Basic Research") or Budget Category 2 ("Applied Research"). Activity described under Budget Category 3 ("Advanced Technology Development") is not considered university fundamental research. Likewise, NASA generally considers fundamental research to be activity described in Technology Readiness Levels (TRLs) 1 through 4 on a scale of 1-9. NASA's Export Control Guidelines generally do not consider the development of flight operational hardware or software as fundamental research.

¹⁵ See [Part 740](#) of the EAR

If university resources are available, the development and deployment of an on-line export control training module to be integrated into a university's on-line training catalog can provide a useful entrée to a broad trainee base.

In this export control officer's view, the most effective export control training takes place not on an intermittent basis but on one that happens day in and day out through email exchanges, extended telephone conversations, and the use of sponsored research proposal review templates.¹⁶ Export control outreach, in its most successful form, is a proactive activity communicated with the intent to inform and protect, rather than control.

F. Recordkeeping

A university export control compliance program must include an organized recordkeeping system in which export documentation, including use of export licensing exemptions, exceptions and exclusions, can be easily retrieved and reproduced if necessary.¹⁷ Export control forms and certifications document a university's due diligence with applicable export control regulations, and represent a significant mitigating factor in any enforcement action by demonstrating that there is a demonstrated effort to run a compliant export control program.

A basic university recordkeeping program should include guidance on:

- What records to keep
- Where to keep records
- Keeping originals vs. electronic or digital images
- The period of retention (at least 5 years from the date of export)
- The importance of being able to reproduce upon request
- Requirements for the destruction of ITAR defense articles/technical data (DoD Demilitarization Manual¹⁸) and disposal of records

Any university export control recordkeeping system should be established in a manner consistent with the university's risk profile, policies and procedures. If an institution is a fundamental research university, the foundation of the recordkeeping program may simply entail the collection of export control certifications prior to or upon export. At Stanford, for example, an electronic

¹⁶ See Exhibit 7

¹⁷ Recordkeeping provisions are found at 15 CFR 762 (EAR), 22 CFR 122.5 (ITAR) and 31 CFR 501.601 (OFAC)

¹⁸ See DoD 4160.28-M-V3

export compliance certification program¹⁹ for physical and deemed exports has been created whereby a Principal Investigator or researcher is responsible for submitting an online export control form applicable to the export in question (i.e. NLR, TMP, Bona Fide Employee Exemption). The metadata from those forms are routed into a central data repository on a university server, and is accessible to the university export control officer on demand in case of an audit or other data call.

IV. Conclusion

A university export control compliance program can vary in scope and content from one institution to another; “one size does not fit all”. It must prioritize its risks on the basis of greatest liability and likelihood of occurrence. Once the university has an understanding of those export control risks with which it is presented, it can then decide which risks it wishes to avoid, transfer, mitigate or accept.

One of the simplest, yet perhaps most effective, steps a university can take to manage export control compliance risk is to identify a single individual with overall responsibility for export control compliance on campus. The university should take steps to make it known to faculty and students that the responsible export control official should be the point of contact for all export control questions or issues.

Importantly, a university export compliance program should include a policy statement from the highest levels of the institution. This statement should be distributed via email to faculty and posted on a university website. The scope and content of an institution’s written compliance plan, which should reference the institution’s policy statement, will be dependent on the degree of export control risk that the university’s policies, its culture and its research activity present. The university written export compliance plan must describe and implement a recordkeeping system in which export documentation, including use of export licensing exemptions, exceptions and exclusions, can be easily retrieved and reproduced.

Finally, key university personnel must be identified and trained; the most effective export control training takes place on a consistent basis through email exchanges, extended telephone conversations, and the use of sponsored research proposal review templates. Export control outreach, in its most successful form, is a proactive activity communicated with the intent to inform and protect, rather than control.

¹⁹ See <http://export.stanford.edu/forms.html>



Questionnaire Pertaining to the Potential Release of Regulated Export Control-Listed Technology or Technical Data to Stanford Foreign National Employees

NOTE: This Questionnaire must be submitted by the applicant's Principal Investigator or Faculty supervisor. In cases where the applicant does not have a Principal Investigator or Faculty Supervisor, a department's Human Resource Manager must submit this Questionnaire on the applicant's behalf. In either instance, by submitting this Questionnaire, you are certifying that you are either the applicant's Principal Investigator/Faculty supervisor or Human Resource Manager.

In addition, all Principal Investigators/Faculty supervisors and Human Resource Managers submitting this Questionnaire must have completed the STARS course [ORA-1130 "Export Controls: An Overview for Research Administrators"](#). Course fulfillment is a one-time requirement only.

The Export Administration Regulations (EAR) and the International Traffic in Arms Regulations (ITAR) require US citizens to seek and receive US Government approval before releasing regulated technology or technical data identified on [US export control lists](#) to foreign nationals in the US. Under both the EAR and ITAR, the release of regulated export control-listed technology or technical data to foreign nationals in the US is deemed to be an export to that person's country or countries of nationality. Significant [civil and criminal penalties](#) apply to the unauthorized release of regulated export control-listed technology or technical data to foreign nationals in the US.

Regulated export controlled technology (regulated technology) is generally defined as specific unpublished technical information necessary for the "development", "production", or "use" of items or software on US export control lists. Regulated technology includes information released through giving technical assistance to a person or providing technical data. Regulated technology and technical data can take the form of unpublished software source code, instructions, blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, and technical manuals. It also includes technical information about regulated technology that may be communicated in meetings, emails, and telephone conversations or through visual observation.

Regulated export controlled technology and technical data does NOT include technical information or software that results from Stanford research. The products of Stanford's [fundamental research](#) are treated as published as they are intended to be shared broadly – thus they lie outside the scope of US technology export controls and are not regulated. In almost all instances, Stanford's exposure to regulated export control-listed technologies occurs when a Stanford sponsor or a third party – a company or a government agency, for example – asks Stanford personnel to accept proprietary, [disclosure-restricted](#) or export control-marked technical information, materials, or software code. A foreign nationals' use of regulated export control-listed items or software does not require US Government approval unless the third party-supplied item or software is [ITAR listed](#) (defense articles) or if the third party discloses regulated [development, production or use technology](#).

The questions that follow are designed to assist Stanford in accurately certifying to USCIS whether unpublished, regulated technology or technical data will be released to a Stanford foreign national employee, and if so, whether an export license will be required. These questions will also help mitigate institutional and individual export control compliance risk.

Please note that Stanford University's [export control website](#) contains background information, tools and resources including an [export control tutorial](#) available as a desktop reference in PDF format that you may find helpful. In addition, Stanford's Export Control Officer (steve.eisner@stanford.edu, 4-7072) is available should you have questions or wish to request guidance. Export control regulation is complex and you should not hesitate to seek this guidance.

- Do you know, or anticipate, that the proposed Stanford foreign national employee will require access to or use of an [ITAR listed item](#) or [ITAR listed software](#) that is NOT the product of university fundamental research?

Yes No

- Do you know, or anticipate, that the proposed Stanford foreign national employee will require access to commercial or third-party unpublished [development, production or use technology](#) that would be subject to export control regulations?

Yes No

- Do you know, or anticipate, that the proposed Stanford foreign national employee will require access to technical information or software source code that is subject to disclosure restrictions?

Yes No

- Do you know, or anticipate, that the proposed Stanford foreign national employee will be exposed to regulated export control-listed technology or technical data in any other manner?

Yes No

Submission of this Questionnaire confirms your understanding that you will be held accountable under US export control law for the information so provided. Again, Stanford's Export Control Officer is available should you still have concerns or wish to request further guidance before completing this questionnaire.

OFFICE OF THE VICE PROVOST AND DEAN OF RESEARCH

Export Controls Home

Background

Resources

Export Controls Roadmap

Decision Tree

Tools and Checklists

Restricted Party Screening

Stanford Correspondence

In the News

Forms

Regulations

Dean of Research Home

Export Controls

Handling of Non-Disclosure or Confidentiality Agreements

In the course of their Stanford work, Principal Investigators and other researchers may be asked to accept confidential, proprietary or restricted information, materials, software code or technology from a sponsor or third party. The sponsor or third party - a company or a government agency, for example - will require that the researcher sign a Non-Disclosure Agreement (NDA), sometimes also called a Confidential Disclosure Agreement (CDA) or Confidentiality Agreement.

In some cases, non-disclosure requests are embedded in the content of several kinds of institutional agreements between the University and the sponsor or third-party. Examples of such institutional agreements include equipment or software purchases or loans, technology licensing, data sharing agreements, and material transfer agreements. In these kinds of institutional agreements, a Stanford office, usually the Office of Sponsored Research or the Industrial Contracts Office, will be involved and will negotiate terms consistent with University policies. These offices will also have the exclusive authority to bind Stanford to the negotiated terms of institutional agreements, and also have the exclusive authority to sign on behalf of the University.

In other cases, a sponsor or third party may ask an individual at Stanford to sign such an agreement as part of an ongoing or proposed activity in which there is mutual interest, such as a clinical trial or potential collaborative research project. In these cases, the NDA is between the sponsor or third party and the individual. **The researcher cannot sign on behalf of Stanford University and must sign as an individual.** Because sponsor or third-party NDAs frequently contain terms that violate Stanford research policy, individual researchers intending to sign on their own behalf should contact the Office of the Dean of Research, the Office of Sponsored Research or the Industrial Contracts Office as applicable for guidance.

NOTE 1: Work done as part of a consulting arrangement falls outside of the individual's Stanford responsibilities. The guidance on this page does not apply to consulting arrangements. Because of the significant risk involved, in no way should an individual who has accepted the receipt of export controlled information under a consulting agreement either bring such export controlled information onto campus or use it in any "incidental" way with Stanford property.

NOTE 2 : NDAs are generally NOT permitted for class projects at Stanford. Students should not be asked to sign an NDA in order to participate in a class project, and companies should not provide any information to project-based classes if they are not willing to permit the information to be made public.

For additional information, including specific actions that must be taken by Stanford faculty when entering into commercial consulting or non-disclosure agreements, please see the University Provost's [Statement on Outside Consulting Activities by Members of the Academic Council](#).

Important points to keep in mind when reviewing NDAs between yourself and a sponsor or third party

- Proprietary or disclosure-restricted information is **NOT** covered by the fundamental research safe harbor that excludes the information from export controls. The acceptance of disclosure-restricted information, equipment, software code or technology may expose the recipient to "deemed export" compliance risk. Deemed exports occur when one shares [export control-listed](#) proprietary or disclosure-restricted hardware, information or technology with foreign persons, including international students and researchers. Deemed export violations can occur even if items or data being shared are not labeled as export controlled and may result in [civil and criminal penalties](#). This occurred recently at the [University of Tennessee](#). See Section IV of Stanford's [Export Control policy](#) for additional information on the acceptance of third-party information.
- The principle of openness in research - that is, freedom of access by all

Key Resources

[EXPORT CONTROL POLICY](#)

Updated policy and procedures on tangible exports and acceptance of 3rd party proprietary or restricted information

[FACULTY CONSULTING POLICIES](#)

Attachment A to RPH 4.3 Addresses the terms and conditions under which Stanford faculty may enter into consulting and confidentiality agreements

Questions?

If you have questions about the applicability of export control regulations to a particular situation, or about any of the information presented on this page, contact:

Steve Eisner,
Export Control Officer
steve.eisner@stanford.edu
(650) 724-7072

[Search Export Controls](#)



interested persons to the underlying data, to the processes, and to the final results of research - is of overriding importance at Stanford. See Stanford's [Openness in Research policy](#) for discussion of acceptable and unacceptable agreements.

- It is the responsibility of the sponsor or third party to identify and define precisely the confidential, proprietary or restricted information being shared. This cannot be left to the judgment of the individual accepting the material.
- It is the responsibility of the individual accepting the information to protect it appropriately.
- Any assertion by the sponsor or third party of limits on publication of results, or restrictions on sharing based on nationality or citizenship, should be immediately questioned with the appropriate Stanford office. The offices listed at the bottom of this page can advise. Contact the [Assistant Dean of Research](#) for assistance.

Standard Templates (see <http://www.stanford.edu/group/ICO/researchAdmins/raConfidential.html>).

A standard template for a Non-Disclosure Agreement is available from Stanford's Industrial Contracts Office.

- If the sponsor or third party will agree to use this agreement, you may sign it with no further review. Be sure to keep a copy in your files.
- If the sponsor or third party presents their own agreement for your signature, review its terms against those in the Stanford template. If the terms are substantively the same, you can feel comfortable signing it.

Things to look for and People to Contact

- These agreements should not contain any clauses governing intellectual property ownership. Contact the [Industrial Contracts Office](#) to review any agreement including such terms.
- If an agreement refers to export controls ([references to ITAR or EAR](#)), contact Stanford's [Export Control Officer](#). Should you accept export-controlled information, you will need to complete this [Stanford certification](#).
- The researcher is responsible for the acceptance and protection of the information, materials or technology being shared, and is the appropriate signer of the agreement. If the sponsor or third party insists on an institutional signature, contact either the [Office of Sponsored Research](#), or the [Industrial Contracts Office](#).
- Other than the guidance provided here, Stanford University does not review or provide guidance related to these agreements. If you have further questions about an agreement between a sponsor or third party and yourself, you may want to contact your own legal advisor.

| [Dean of Research Office](#) | [Industrial Contracts Office](#) |
| [Office of Sponsored Research](#) | [Office of the General Counsel](#) |

Stanford Directories | Maps & Directions

© Stanford University. All Rights Reserved. Stanford, CA 94305. (650) 723-2300. [Terms of Use](#) | [Copyright Complaints](#)



**NOTIFICATION ON THE REEXPORT AND USE
OF ITEMS SUBJECT TO U.S. EXPORT CONTROL REGULATIONS**

TO: [*Name of Original Foreign Collaborator in Receipt of Items*]
FROM: [*Name of Stanford PI*]
DATE: [*Date*]
SUBJECT: **Reexport and Use of U.S. Export Controlled Item(s)**
cc: [*Department/Project Files; steve.eisner@stanford.edu*]

Dear [*Name of Original Foreign Collaborator in Receipt of Items*]:

Stanford's Office of the Dean of Research wants me to inform you that any reexport or transfer of the U.S.-origin item[s] identified below [*is/are*] subject to U.S. export control regulations. These regulations include the International Traffic in Arms Regulations (ITAR), the Export Administration Regulations (EAR) and regulations administered by the Treasury Department's Office of Foreign Assets Control (OFAC). I'm told that it's unlawful under these U.S. export control regulations to reexport or transfer these items to any unauthorized destination, or to any U.S. sanctioned country, person or entity¹ or to divert or use these items for any proliferation activity, including but not limited to the design, development, production, stockpiling or use of any nuclear explosive device, chemical or biological weapons, or missiles without first obtaining an export license from the appropriate U.S. government agency.

I've also been asked to mention that individuals and organizations outside the U.S. found to have violated U.S. export control regulations may be prohibited from receiving U.S.-origin goods, technology or services, or contracting with the U.S. government or may have their property and other assets in the U.S. blocked or frozen. In addition, foreign persons found to have violated U.S. export control regulations that later come under U.S. jurisdiction may become subject to criminal and civil penalties.

Stanford University will acknowledge that you have read and have understood its contents upon receiving this Notification.

Stanford PI Signature and Date:

Name of U.S Origin Item(s):

¹ Countries, persons or entities subject to U.S. sanctions and embargoes may be found in part at <http://www.treas.gov/offices/enforcement/ofac>, <http://www.pmdtc.org/country.htm> and <http://bxa.doc.gov/DPL/thedeniallist.asp>



Property Export Control Checklist License Exception TMP (Temporary Exports)	Yes	No
Is the item or software to be shipped or hand-carried abroad?		
Is the item or software currently overseas and being retransferred to another country or to a new overseas custodian?		
Is the item or software to return to the US within 12 months or either consumed or destroyed abroad?		
Is the item or software for temporary shipment, retransfer or hand-carry to any country other than Iran, Syria, Cuba, North Korea or Sudan?		
Will the item or software to be shipped, retransferred or hand-carried be used ONLY either a) as a “tool of the trade” to conduct Stanford University business or b) for exhibition or demonstration or c) for inspection, testing, calibration or repair?		
If for inspection, testing, calibration or repair, will the item or software be shipped, retransferred or hand-carried to any country other than: Albania, Armenia, Azerbaijan, Belarus, Cambodia, China, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Libya, Macau, Moldova, Mongolia, Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan or Vietnam?		
Will the item or software remain under the “effective control” of Stanford personnel while the property is abroad? Note: “Effective Control” is defined as retaining physical possession of an item or maintaining it in a secure environment such as a hotel safe or a locked or guarded facility.		
Is the encryption code incorporated in the item or on the software media limited to that available through retail purchase (phone order, mail, internet, or over-the-counter transactions)?		

If the answers to **ALL** of these questions are **YES**, and your equipment, components or software are not designed for use in/with/by satellites or spacecraft or otherwise regulated as a defense article (see Stanford’s Export Control Decision Tree at exp.stanford.edu), then your shipment, retransfer or hand-carry is eligible for shipment under License Exception TMP. For questions, please contact Steve Eisner, University Export Control Officer, at 4-7072 or steve.eisner@stanford.edu

EXHIBIT 4



Stanford University Openness in Research CHECKLIST

The principle of openness in research is one of overriding importance to this University. Accordingly, no program of research that requires secrecy may be conducted at Stanford, other than the exceptions specifically allowed in the University's Openness in Research policy (Research Policy Handbook 2.6).

Use this checklist when reviewing:

- requests for proposals or project solicitations,
- program award notices,
- Non-Disclosure Agreements (NDAs),
- any other documents related to research proposals, contracts, cooperative agreements, and other arrangements for sponsored research projects

to assure that they do not require secrecy or impose unacceptable restrictions.

In any proposals for research funding, Stanford will include language indicating its commitment to openness in research, and its intention to adhere to policy in this regard.

Does this project or agreement:	YES	NO
Contain language referring to or mandating compliance with export laws or regulations?		
Restrict researcher participation (faculty, student, others) based on country of origin or citizenship?		
Require researcher participation in US-citizen-only meetings?		
Prohibit the hiring of non-US citizens to be involved in the proposed research?		
Grant the sponsor a right of prepublication review for matters other than the inclusion of patent and/or proprietary sponsor information?		
Provide that any part of the sponsoring, granting, or establishing documents may not be disclosed?		
Limit access to confidential data so centrally related to the research that a member of the research group who was not privy to the confidential data would be unable to participate fully in all of the intellectually significant portions of the project?		

If the answer to any of these question is "Yes," or if you have other questions related to openness in research, please contact the Dean of Research office.

(Ann George, 723-9721, anngeo@stanford.edu).

CONTINUES ON REVERSE SIDE

<http://www.stanford.edu/dept/DoR/C-Res/ITARlist.html>

EXHIBIT 5

If accepting proprietary information as part of a project:	YES	NO
Is the information clearly defined?		
Can the information be appropriately protected?		
Can proprietary information be removed from research results, so that results may be freely published?		

If the answer to any of these question is "No," please contact
the Dean of Research office.
(Ann George, 723-9721, anngео@stanford.edu).

If accepting information identified as export-controlled:	YES	NO
Has a Non-Disclosure Agreement been reviewed with Stanford's Export Control Officer?		
Is there any need to share this information with others, including international students or other non-citizens?		

In either case, when dealing with export controls, please contact
the university's Export Control Officer.
Steve Eisner, 724-7072, steve.eisner@stanford.edu



PDRF Response Requiring Export Control Review	Export Control Officer Approval Required Before Submission?
1. Sponsor Identified as the Department of Defense (DoD)	
a) Agreement Type: Grant/Contract or Cooperative Agreement (School of Medicine [SoM] Grant Proposals Excluded from Approval Requirement)	Yes
b) Agreement Type: All Others	No
2. Sponsor Identified as the National Aeronautics and Space Administration (NASA)	
a) Agreement Type: Grant/Contract or Cooperative Agreement	Yes
b) Agreement Type: All Others	No
3. Subcontract w/DoD as Prime (also applies to SoM)	Yes
4. Subcontract w/NASA as Prime (also applies to SoM)	Yes
5. SBIR/STTR Subcontract	
a) DoD/NASA/Other National Security Prime (CIA/DHS/DoD Subagencies)	Yes
b) All Other Primes	No
6. Project Requires Access to Disclosure Restricted Technical Information or Defense Articles (Export Control Review Required for All Sponsors)	Yes
7. Project Involves International Shipment/Handcarry (Export Control Review Required for All Sponsors)	No



Template Language: International Travel/International Shipments

Hello Dr. Eisner,

As part of my duties as University Export Control Officer reporting to the Dean of Research, I'm forwarded proposals that involve international travel and/or international shipments. The purpose of this is to provide guidance to our faculty with the goal of mitigating export compliance risk for you and the University.

One step in this risk mitigation exercise is that we ask our research community to complete applicable export compliance certifications to document due diligence. The background and context to this requirement is outlined by Ann Arvin in her memo to Stanford faculty and research administrators at http://export.stanford.edu/doc_memo.html.

One applicable certification to your proposed work is the Annual "TMP" Export Certification form, which documents that researcher travel with laptops, other digital devices and certain proprietary information that may be stored on them does not require an export license, if the terms of the Certification can be met. I don't seem to have a Certification on file for you.

Could you please take a look at <https://www.stanford.edu/group/export/forms/TMP-annual.html> including the preamble to the form itself and complete/submit the Certification before your next international travel with Stanford-owned digital storage devices?

In addition, international shipments need to be evaluated for export control and possible licensing requirements. A Stanford Export Control Decision Tree is available at <http://export.stanford.edu/tree/index.html> for a self-assessment. It's unlikely that your shipments or handcarries, should you have them, will require an export license – the One-Time NLR form at <https://www.stanford.edu/group/export/forms/NLR.html> will likely be the applicable form. I can assist you directly with shipping determinations if you'd find that useful.

Finally, Stanford's Global Activities Operating Guide for faculty at http://fingate.stanford.edu/docs/global_activity_ops_guide.pdf might prove informative to you not just for this project, but for others that will come your way going forward.

I'll be glad to answer any questions or to otherwise be of help in any way I can.

With appreciation,

Steve



Template Language: University/Industry Collaborations

Hello Dr. Eisner,

I'm reviewing your proposal below that appears to involve collaborative activity with a business concern and thought I'd try to provide some guidance that will help mitigate export compliance risk for you and the University.

The US government considers university fundamental research to be a public domain activity since the resulting information is intended to be shared broadly with the interested scientific community. For this reason, the conduct and products of university fundamental research are not regulated for export control. However, because commercial research and development activity is by nature proprietary and in most instances are subject to disclosure, dissemination or access restrictions for competitive reasons, export control regulations generally do apply to the conduct and products of commercial research.

The Dean of Research has developed a website at <http://export.stanford.edu/nda1.html> to assist the Stanford research community should exposure to commercial research activity be anticipated. We hope this page might prove informative to you not just for this project, but for others that will come your way going forward.

I'll be glad to answer any questions you might have.

With appreciation,

Steve