Technology Control Plans (TCPs): Security Measures, Considerations, and Best Practices

Implementing a TCP is a best practice whenever a research activity is subject to export controls. Many institutions perform research that involves highly controlled technical data, information, materials, equipment, and software. Although non-U.S. persons may not be involved in such projects, the export-controlled information and items must still be secured.

The purpose of a TCP is to ensure compliance with U.S. export control laws and regulations and to prevent access (visual, physical, electronic) by unauthorized non-U.S. persons to certain export-controlled information, technical data, materials, software, and equipment. If an export license has been obtained for a particular non-U.S. person to have access to project materials and information, or a license exemption is applicable, the non-U.S. person would be authorized for that project only. A TCP ensures the research team is informed, aware, and understands their compliance obligations and responsibilities by formalizing university procedures to safeguard export-controlled data, information, equipment, and software. For research projects, a TCP is most commonly implemented on a per-project basis to create a security "bubble" around a specific research activity. The TCP should be implemented before the project starts, and all project personnel should understand their responsibilities and the required security procedures.

While the ITAR is largely silent on the exact security measures necessary in a TCP, the EAR states that a TCP should contain, at a minimum, the following essential elements (EAR 2015):

- Institutional commitment to export compliance
- Physical security plan
- Information security plan
- Personnel screening procedures
- Training and awareness program
- Self-evaluation program and audits

Although each project is unique, there are elements common to every project. A best practice is to use a TCP template that incorporates the above elements, which can then be modified to fit the particular research project or situation. The TCP should have a statement regarding institution's commitment to complying with the export control regulations, and list the offices and personnel (for example, the Vice President for Research's office, export control officer, and lead principal investigator [PI]) responsible for the implementation and monitoring of TCPs. The TCP template should include measures for securing physical items such as hard-copy documents and ITAR-controlled equipment, and security measures for data and information that is transmitted electronically and/or stored on a computer. The template should also incorporate a statement that project personnel will be screened against U.S. government denied/restricted/prohibited party lists and mention the institution's export control training program and any training requirements for project personnel. It is important to have a compliance assessment in the template that includes a self-evaluation process and a yearly audit conducted by the export control officer or another individual in the institution who can conduct an internal audit. Finally, the template should include procedures for the disposition of export-controlled technical data, information, materials, equipment, etc. when the project has terminated.

Factors and Questions to Consider when Implementing a TCP

When implementing a TCP, take into consideration the complex environment unique to university research facilities, laboratories, and offices. A TCP may be required for a single researcher, office, or laboratory, or for laboratories shared by multiple investigators and research teams.

Shared Facilities and Laboratories

A TCP may be more difficult to implement when multiple PIs and research teams share facilities or laboratories. Evaluate the feasibility of:

1. Establishing a portion of the lab solely for the performance of export-controlled research activities and securing that portion of the lab from view or access by unauthorized non-U.S. persons;
2. Arranging "time-blocks" so that export-controlled activity would only occur during time periods when unauthorized persons are not present and no other research would be conducted in the same lab area; or
3. Not performing the export-controlled research.

Should the decision be made to conduct the export-controlled activity, the TCP should include the specific procedures necessary to either secure a specific section of the lab or arrange certain blocks of time for the export-controlled work to be completed.

Facility-wide TCP

A TCP can be applicable to an entire facility, series of rooms, or to a single lab or office. It is possible to implement a TCP that covers multiple export-controlled projects in a facility or series of rooms as long as unauthorized non-U.S. persons are not given access. Multiple export-controlled projects, PIs, and project personnel can be covered under a single facility-wide TCP. When an entire facility or wing of a building will accommodate export-controlled projects, in addition to the standard TCP procedures, it is important to include security procedures such as key-card access, and/or visitor logs, and a process for screening visitors' citizenship status.

Large Export-Controlled Projects

Assuming that a research team conducts export-controlled research in a single lab, implementing one TCP per research group makes TCP management easier. However, for a large export-controlled project, it may be preferable to implement multiple TCPs if more than one building is involved or if personnel from multiple colleges and departments will participate. To illustrate, if the U.S. Navy awards a program subject to the ITAR that will require expertise in the disciplines of fiber optics, structural mechanics, and electrical engineering, and the research groups are scattered among several buildings (ten PIs/project personnel are located in College A/Building A, seven in College B/Building B, and four in College A/Building C), then it would be easier to manage the large program by implementing three separate TCPs; one for each lab area. Project personnel, especially graduate students, come-and-go on projects, and the TCP will be easier to update if it is limited to a particular department or building.

Other Uses of a TCP

Most TCPs are implemented specifically to control activities on certain research projects; however, a TCP can also be used to manage broad ranges of research activities, such as the use of export-controlled research equipment or the use of export-controlled substances. TCPs can be implemented to manage the generation of large amounts of sensitive data, such as export-controlled data being streamed from a satellite. A TCP can be used to ensure the custody, access, or use of export-controlled research equipment or substances are properly managed and compliant with export control regulations. This may be necessary even when a research activity and the resulting data are not export-controlled. For example, non-U.S. person use of a high performance computing center, or an ITAR-controlled camera such as a mil-rugged high sensitivity InGaAs Short Wave Infrared (SWIR) camera, or the use of a small amount of an explosive substance such as 2,4-dinitroanisole (DNAN) would require a TCP to prevent an inadvertent export because in each of these cases non-U.S. person access would require prior U.S. government approval in the form of a license.

Additional Factors and Questions to Consider When Writing the TCP

- Where will export-controlled research information, articles, materials, or substances be stored or locked and who will have access?
- Will any physical barriers, such as curtains or screens be necessary to shield research equipment or activities from view?
- Does the research activity require travel outside the U.S.? Will any researcher need to hand-carry export-controlled data, software, or equipment out of the U.S.? An export license may be required depending on the country and the nature of the technology, software, or equipment. A license could be denied for exports to certain countries.
- Will anything need to be shipped internationally? A license could be required prior to shipment.
- Are site visits anticipated by non-U.S. persons? Provisions will need to be made for escorts (certain export-controlled technical data, equipment, and materials cannot be visible), badging, and a visitor log.
- Are research project personnel required to take export control training prior to the start of the project and has the training been completed?

- Are there export licensing conditions or provisos that need to be incorporated into the TCP? For example, the transfer of export-controlled technology and software to the non-U.S. person is limited to that individual's role as described in the license application. There may be other limitations (provisos) the approving U.S. government agency has placed in the license that will need to be followed.
- Where will electronic export-controlled data and information be stored (laptop, desktop computer, or server)? Is the desktop computer part of a network? Are the department/college Information Technology (IT) personnel U.S. persons? Best practices include encrypting data files or folders and storing on a secure server. Only U.S. persons should have access to the encrypted files, folders, and servers.

Examples of Information Contained in a Technology Control Plan (TCP)

General information

- Program information (investigator[s], project director, project title, sponsor, start/end dates, award number, account number, etc.)
- Institutional policy / statement of commitment
- Project description

Program restrictions

- USML/CCL Categories of export-controlled technology, materials, and/or equipment
- Contractual restrictions, etc.

Research team information

- Research locations (room numbers and buildings)
- Research groups (if multiple)
- Team members (project personnel)

  Note: List project personnel, rooms, and buildings as an attachment to TCP for ease in updating changes to personnel and locations.

Security protocols

- Physical security
- Electronic and computer security
- Personnel responsibilities
- Site visits - non-U.S. person escort procedures

Regulatory Guidelines

- U.S. government approval / licensing guidelines, such as any required conditions or proviso requirements

- Foreign travel requirements
- International shipping
- Procurement of ITAR controlled tooling and equipment
- Export control training requirements
- Recordkeeping requirements
- Provisions for a self-audit
- Self-reporting mechanism for procedural violations (not necessarily an export violation) of the TCP
- Accountability and violation penalties

TCP Security Best Practices

Accumulated best practices implemented within the complex environment of university research facilities and laboratories that have evolved over the past decade serve as the basis for the following security measures. Most universities have a boilerplate TCP template that is customized for each use. The TCP template should include standard procedures related to physical security, electronic security, site visitors, transportation of export-controlled technology items on-campus or throughout U.S. territories, and international travel and shipping. Some procedures, such as physical and electronic security, will be applicable to most TCPs, while other measures may be deleted if not applicable to the research project (for example, international travel and shipping).

Physical Security

Implement the following security measures to shield export-controlled items and documents that are clearly visible in the workspace so that unauthorized persons will not have visual or physical access:

- Do not prop or leave open doors to individual offices, research facilities, or other areas during the conduct of export-controlled work. Post signs at the entrances during times when export-controlled items and information are visible; for example, "Unauthorized Non-U.S. Persons Not Permitted."
- If there has been implementation of a time-block schedule, a time schedule of days/times when non-U.S. persons cannot be present in the research area should visually posted.
- Doors should be locked and a clean desk policy in effect whenever labs, rooms, or facilities are left unattended and export-controlled items and information are visible on the desk or in the research area.
- Label export-controlled equipment by suitable means and shield it from unauthorized visual access at all times. Non-U.S. persons will not be allowed entry to offices or research facilities when export-controlled items are visible and/or in use, unless prior licensing approval has been obtained or an EAR exception or ITAR exemption is applicable.

- Store all back-up hard-drives, flash-drives, and hard copies of documents that contain export-controlled information in a secure location (for example, a locked drawer or cabinet) when not in use. Give access only to individuals authorized by the TCP. The names of the individuals who have keys to drawers, file cabinets, rooms, or labs that contain or store export-controlled information and equipment should be identified within the TCP.
- Mark research deliverables containing ITAR-controlled technical data: "ITAR-controlled - do not distribute to non-U.S. Persons."
- Only print export-controlled technical data on a designated printer located in the secured research area. Retrieve printed information immediately.
- Dispose of printed matter containing export-controlled data by depositing in a "burn barrel" or by crosscut shredding prior to disposal or recycling.
- Displays of information containing export-controlled technology or technical data should be positioned so that it is not viewable from outside the research area. This includes sight lines that are visible at a distance where binoculars or similar devices could make the information viewable.
- Block or cover windows, doors, or other sightlines into research areas where export-controlled technology or technical data are present.
- Do not take research materials that contain export-controlled technical data outside of the research area except for when it is necessary to conduct approved project work in other official work locations (such as transit to an external location for testing). It is important to follow transportation protocols when the research materials are taken outside the research area.

Electronic Information Security

Unfortunately, cyber security threats and breaches are all too commonplace, and institutions of higher education are often targets. It is important to protect export-controlled research results, data, and information not only from outside threats, but also from inadvertent release to unauthorized non-U.S. persons, whether on or off-campus. The TCP should contain measures to secure and manage electronic export-controlled technical data and information. The following are best practices and security measures:

- Do not post export-controlled data generated from any project on Internet websites or social media venues.
- Prohibit using, processing or storing export-controlled data on "cloud" based systems (such as Amazon EC2, Dropbox, OneDrive, or iCloud) or using email services such as Yahoo! and Gmail. These systems may not be hosted from the U.S. and an export may occur when transferring export-controlled data and information.
- Encrypt all technical data saved on any computer (including flash drives and back-up hard drives) and encrypt all folders, files, or other devices that contain any export-controlled technical data.
- Password-protect and lock all computers that contain or process export-controlled technical data when unattended.

- Label all devices that contain EAR- and ITAR-controlled data/information (for example, flash drives, laptops, computers, and back-up hard drives). When not in use, store these devices in a secure location (secured drawer or cabinet) to prevent unauthorized access.
- Do not email, receive, or distribute ITAR-controlled technical data without encryption (for example, to/from sponsor or between project personnel). ITAR-controlled technical data and information cannot be emailed or transferred to individuals or entities outside the U.S. without prior U.S. government approval.

  Note: Export-controlled data should not be stored on a computer or server that is part of a network system unless the IT personnel who have access to the system are U.S. citizens/Permanent Residents or access by non-U.S. persons has been authorized by the appropriate U.S. government agency. It is always a good idea to consult with your local IT department for assistance and the appropriate resources. It may be possible to utilize secured cloud resources such as Daptiv (eProject) or other cloud service providers that are approved for storing ITAR and other export-controlled information.

Transporting Export-Controlled Data, Information, or Equipment

At times, it may be necessary for researchers to share export-controlled data or documents with project team members located in another area on campus or possibly run tests, for example, on the data at an off-campus facility. Only approved project personnel identified in the TCP should transport or carry export-controlled data, documents, or equipment across or off university premises. The TCP should incorporate measures to ensure the security of the items. Examples of security precautions include:

- Export-controlled data, documents, information, or equipment must be in the possession of the authorized project personnel at all times when removed from the research facility.
- All electronic data when being transported must be stored in encrypted files or folders on a flash-drive or laptop. Store devices containing electronic export-controlled data in a secure storage device such as a briefcase, vehicle, and/or a hotel safe.
- Export-controlled data or information temporarily stored at a private residence should be kept in a secure location to prevent access by unauthorized non-U.S. persons.

Site Visit Controls

There may be occasions when individuals and groups will visit the research facilities where export-controlled work is conducted. Arrange in advance visits from non-project personnel so the export-controlled data, documents, materials, or equipment can be removed, covered, or shielded from view to prevent visual or physical access by non-U.S. persons. If there is an anticipation of site visits, the TCP should include the following:

- Visitors must sign a Visitor Log before entering the research facility. At a minimum, visitors should provide name, short purpose of visit, and citizenship.
- Visitors to research facilities with a facility-wide TCP should be provided with a visitor badge. If the individual is a non-U.S. person, the badge should be marked (such as color) to indicate non-U.S. citizenship status.
- Notify all authorized researchers participating in export-controlled research activities in advance of visits or tours so that export-controlled items and technical data can be stored or shielded from view.
- Escort non-U.S. person visitors at all times in areas where export-controlled research is being conducted. Export-controlled data and items will not be visually accessible during the visit.
- Researchers must not conduct export-controlled research or discuss technical details when non-U.S. persons are present.
- Escorts must not allow the visitors to wander, take videos or photographs, or include any unannounced non-U.S. person in the site visit. Escorts are to report any embarrassing incidents, unannounced changes, unannounced visitors, video crews, misinterpretation of academic background, or multiple visit requests to the proper university officials.

Export-Control Training

The TCP should identify mandatory training requirements that authorized project personnel (including students, visiting scholars, subcontractors, etc.) need to complete prior to participating in an export-controlled research activity. If audited, the institution will be asked for its export control training records.

Recordkeeping Requirements

The TCP should include a statement regarding export control record retention. If the research activity is associated with an export license or agreement, records pertaining to the export must be kept for five years *after* the expiration of the license or agreement (EAR 2015; ITAR 2014; Records 2011). For example, if a Technical Assistance Agreement (TAA) related to the research activity is in effect for ten years (the maximum allowed), documents must be kept for a total of 15 years. The researcher will need to take into account the regulatory agency's record retention requirements as well as the institution's policy.

Personnel Screening

Incorporate personnel screening procedures into the TCP template. Individuals who have access to export-controlled project materials, data, equipment, or software should be screened against the various U.S. government denied parties/entities lists. If an individual or an entity is found on a list, then the export control officer, Empowered Official, and/or Office of General Counsel will need to evaluate. An export license may be required for the person to participate, where in fact a license could be denied.

Compliance Assessment

The TCP should contain procedures for conducting a self-evaluation. As a critical component to an institution's ongoing compliance monitoring, self-evaluation is an internal assessment process whereby procedures are reviewed and any findings reported to the Project Director/PI and designated export control official (usually the export control officer). The Project Director/PI or designee should complete an internal audit.

The institution's designated export control official may also conduct periodic evaluations and/or training to assess compliance with the TCP procedures. It is common to conduct a formal TCP audit within one year of TCP implementation, and subsequent years throughout the life of the project. Modifications to approved security measures or personnel changes must be authorized in advance by the Project Director/PI and designated export control official, and documented in the TCP. Other important amendments may include changes to research location or the scope of the research activity.

Note: Should the Project Director/PI, or project team member discover a potential export control violation has occurred, it is important to contact the designated export control official, Empowered Official, and/or Office of General Counsel immediately. These individuals are responsible for determining if a potential export violation has occurred that requires disclosure to the appropriate government agency. If a violation is suspect, all non-U.S. person given access to the export-controlled items or activity must be immediately discontinued until U.S. government approval has been obtained or the activity has officially been determined not to constitute a violation.

Termination of Export-Controlled Activity or Project

Instructions regarding the disposition of export-controlled data and items upon completion of an export-controlled research activity should be documented in the TCP. It may be necessary to keep certain security measures in effect after a research activity has concluded to comply with export control laws and regulations, and protect residual export-controlled technical data, information, or equipment. If the controlled data or equipment has been returned to the sponsor, destroyed, or determined to be no longer export-controlled, the TCP can be closed. However, as stated above in Recordkeeping Requirements, all records and documents pertaining to export licenses and agreements related to controlled articles and technical data shall be retained in accordance with the institution's policy and applicable federal regulations.

Other TCP Procedures

Project Director/PI Responsibilities

The Project Director/PI is responsible for ensuring that project personnel have completed any required export-control training, are briefed, and understand the requirements and protocols enumerated in the TCP. The Project Director/PI is also responsible for confirming that all project personnel both sign the TCP certification (discussed later) and have an accessible copy of the TCP (for example, a hard-copy manual in the work area and a softcopy on applicable research computers). The Project Director/PI will monitor compliance with TCP procedures and alert the designated export control official should changes to the TCP become necessary or if a potential violation has occurred.

Project Personnel Responsibilities

Before the export-controlled activity begins, project personnel are responsible for completing any required export-control training, attending a TCP briefing, and making sure they understand and agree to follow the TCP procedures. Questions and concerns regarding the TCP procedures should be addressed to the Project Director/PI and the designated export control official.

TCP Certification

All project personnel, including the PI/Project Director, must sign a TCP Certification (typically at the end of the TCP). The certification states that the individuals signing the TCP have received a briefing on the TCP procedures, they have received a copy of the TCP, and they understand and agree to follow the protocols outlined in the TCP. The project personnel also certify that they could be held personally liable if they knowingly, willfully, or unlawfully disclose export-controlled information to unauthorized non-U.S. persons.

Summary

U.S. export control laws and regulations can affect a broad range of university-based activities including fundamental research. It is important for the researcher to understand how the export control regulations apply to research projects. When the regulations do apply to a research activity, it is important that the researcher and institution stay compliant. Penalties for noncompliance can be severe, include imprisonment, debarment, loss of export privileges, and research funding, damage to the reputation of the institution and the researcher, and possibly civil fines and penalties.

University research and the technologies developed are a vital component to our nation's prosperity and economic development both at home and abroad. Researchers and institutions must both understand and embrace the myriad of compliance obligations to perform the type of cutting-edge research that moves our institutions and our nation forward on the world stage. Compliance ultimately rests with both the researcher and institution.

Acknowledgements

The authors would like to thank Dava Casoni for certain core concepts described in this module. We especially thank Dr. Jaime Arango for his guidance in authoring this module. We also appreciate the insightful comments provided by anonymous reviewers.

References

- Babcock, Wade, and Jerome Persh. 2002. "Safeguarding America's Critical Technologies (and Avoiding Personal Risk) An Introduction to Export Control and Critical Technology Restrictions." *The AMPTIAC Quarterly* 6(2):11-5.
- Boyd, Dallas. 2011. "Protecting Sensitive Information: The Virtue of Self-Restraint." *Homeland Security Affairs* 7:10.
- Export Administration Regulations (EAR), 15 CFR § 730-774 (2015).
- International Traffic in Arms Regulations (ITAR), 22 CFR § 120-130 (2014).
- Liebman, John R., Roszel C. Thomsen II, James E. Bartlett III, and John C. Pisa-Relli. 2014. *United States Export Controls (7th Edition)*. Law Journal Press.
- Records and Recordkeeping Requirements, 31 CFR § 501.601 (2011).
- U.S. Department of Commerce, Office of Inspector General (OIG). 2004. "Bureau of Industry and Security: Deemed Export Controls May Not Stop the Transfer of Sensitive Technology to Foreign Nationals in the U.S." Accessed April 2, 2015.
- U.S. Government Accountability Office (GAO). 2006. "Export Controls: Agencies Should Assess Vulnerabilities and Improve Guidance for Protecting Export-Controlled Information at Universities." Accessed April 2, 2015.

Additional Resources

- Evans, Samuel A. W., and Walter D. Valdivia. 2012. "Export Controls and the Tensions Between Academic Freedom and National Security." *Minerva* 50:169-90.
- Georgi, Kay C., and Paul M. Lalonde, eds. 2014. *Handbook of Export Controls and Economic Sanctions.* American Bar Association.
- Kramer Levin. 2014. "FAA Memorandum May Jeopardize Certain State University Research Projects Involving Unmanned Aircraft." In *Unmanned Aircraft Systems*, June 20.
- U.S. Department of State and the Broadcasting Board of Governors Office of Inspector General. 2004. "Review of Export Controls for Foreign Persons Employed at Companies and Universities." Accessed April 2, 2015.
- U.S. Government Accountability Office (GAO). 2011. "Export Controls: Improvements Needed to Prevent Unauthorized Technology Releases to Foreign National in the United States." Accessed April 2, 2015.
- U.S. Government Accountability Office (GAO). 2012. "Export Controls: Proposed Reforms Create Opportunities to Address Enforcement Challenges." Accessed April 2, 2015.

Original Release: April 2015