

Master Technology Control Plan

University of Hawai'i

Purpose

The purpose of this University of Hawai'i ("UH") Master Technology Control Plan ("Master TCP") is to control the dissemination of unclassified export-controlled technology or technical data (collectively referred to herein as "export-controlled technology") being utilized during the performance of UH projects, including those supported by the Research Corporation of the University of Hawai'i ("RCUH") (collectively referred to herein as "UH Projects"). This Master TCP shall be used exclusively for projects with UH and RCUH personnel, **when there is NO expectation** of exporting data, technology, equipment, information or materials to a non-United States ("US") person, company or government.

When there IS an expectation of exporting data, technology, equipment, information or materials to a non-US person, company or government, this Master TCP shall not be used. In this instance, a Project Specific Technology Control Plan ("PSTCP") or Site Specific Technology Control Plan ("SSTCP") may be required if any of the following conditions exist on UH Projects ineligible for the Fundamental Research Exclusion ("FRE") (see UH Executive Policy 12.218 - Compliance with United States Export Control Laws and Regulations at www.hawaii.edu/policy/, for definition and explanation of FRE):

- a) UH Projects that require the use of non-US Persons;
- b) UH Projects that require the use of students (including US citizens) for thesis or dissertation; and/or
- c) UH Projects that involve collaborative efforts with non-UH sites or participants.

UH Projects that will export or share any export-controlled information, technology, data, equipment or materials or services outside the US (even to a US military installation abroad) require a license or exemption. **The UH Office of Export Controls ("OEC") must be contacted for licensing and/or exemption evaluations prior to export.** It is imperative that all UH Projects plan well ahead as some shipments, licenses or exemptions may require a significant lead time.

This Master TCP describes how UH will control these data, information or materials to ensure that export-controlled technology is not provided to non-US persons (employees, students, colleagues or visitors) without the required export license from the US Departments of State or Commerce, and approval from the OEC. Additionally, this Master TCP ensures that all individuals working on a project containing export-controlled technology understand their obligations under US Export Control Laws and Regulations ("US Export Control Laws"). Disclosures of export-controlled technology (whether inside or outside of the US) to non-US persons (whether or not they're an employee, consultant, sponsor, student or visitor) is considered an export under US Export Control Laws and requires a license or other approval from the US Department of State. Disclosures without proper license or approval can result in fines and jail time *for the individual* making the disclosure.

Non-US persons may not work on projects ineligible for the FRE without written approval from OEC and, when required, a license from the appropriate federal agency. Additionally, students (including US persons) may not work on any project ineligible for the FRE for their theses or dissertations. **If a non-US person, or a student working on their thesis or dissertation, is required for a project ineligible for the FRE, OEC must be contacted for assistance with obtaining appropriate approvals and preparing an individual PSTCP.**

Applicable Regulations

- International Traffic in Arms Regulations (“ITAR”) 22 CFR § 120-130
- Export Administration Regulations (“EAR”) 15 CFR § 730-774
- Office of Foreign Assets Control Regulations (“OFAC”) 31 CFR § 500-598
- Industrial Security Regulation (“ISR”) DoD publication 5220.22-R
- National Industrial Security Program Operating Manual (“NISPOM”) DoD publication 5220.22-M

Policy

Per **UH Executive Policy 12.218 - Compliance with United States Export Control Laws and Regulations** (see www.hawaii.edu/policy/), UH must fully comply with all applicable federal statutes, executive orders, regulations, and contractual requirements for the safeguarding of export-controlled technology in its possession. This includes full and total compliance with US Export Control Laws. Under no circumstances shall employees or other persons acting on behalf of UH engage in activities in contravention of US Export Control Laws.

The intent of this Master TCP is to demonstrate the appropriate level of security for export-controlled technologies as it pertains to US Export Control Laws.

It is unlawful under US Export Control Laws to send or take export-controlled technology out of the US; or to disclose such technology, orally or visually, or to transfer export-controlled technology to a non-US person inside or outside the US without proper authorization. A license may be required for non-US persons to access export-controlled technology.

A non-US person is a person who is not a US citizen, alien/lawful permanent resident/green card holder, or other “Protected Individuals” under the Immigration and Naturalization Act (8 USC § 1324b (a) (3)) designated an asylee, refugee, or temporary resident under amnesty provisions. The law makes no exceptions for non-US graduate students. Non-US persons include 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 US, as well as international organizations, foreign governments and any agency or subdivision of foreign governments (e.g., diplomatic missions, state universities).

In general, export-controlled technology means activities, items, information or materials related to the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, operation, modification, demilitarization, destruction, processing, and use of items with a capacity for military application or utility, or any information relating to a contract with dissemination restrictions.

Export-controlled technology does not include basic marketing information on function or purpose; general system descriptions; information concerning general scientific, mathematical, or engineering principals commonly taught in schools, colleges and universities; or information in the public domain. In these later cases, it does not matter if the actual intended end use of the information is military or civil in nature.

Scope and Approach

The Principal Investigator (“PI”) for each UH Project is responsible for compliance with this Master TCP. This Master TCP is applicable to all UH and RCUH personnel performing work on any export-controlled UH contract or UH Project and will include all operating locations, offices, temporary operating locations, and facilities whether located on campus or during visits to military facilities or to other government facilities. Employees shall ensure compliance with the spirit and intent of the protection criteria contained herein and will be especially cautious when dealing with non-US persons or entities, whether within the US or abroad. This Master TCP has been put in place to ensure that transfers of export-controlled items, materials, equipment, software, data, information or technology to non-US persons does not occur without appropriate licenses. Each project will require adherence to the ITAR under the jurisdiction of the US Department of State, the EAR under the jurisdiction of the US Department of Commerce, and OFAC regulations under the jurisdiction of the US Department of Treasury.

This plan is required because one or more of the following conditions exist:

- Export-controlled technology under a classified UH Project:
This type of UH Project may involve classified information/equipment which, in itself, is export-controlled. Handling of classified information is delineated in the ISR/NISPOM and this Master TCP does not modify or supersede the handling requirements for said classified information. Per the ISR/NISPOM, and in sum, no release of classified information (i.e. confidential, secret, top secret) is permitted to any person (US person and/or foreign national) without the proper security level clearance and a documented “need to know” for that specific information. However, the purpose of this Master TCP is to delineate the controls necessary for handling the unclassified export-controlled technology (as defined in this Master TCP), if any, that are used on a classified project.
- Export-controlled technology under an unclassified UH Project:
This type of UH Project may involve access to export-controlled items, materials, equipment, software, data, or technology. The DFAR 252.204-7008 clause is to be used when the contract involves export controlled items or technology. The clause states “... the parties anticipate that, in the performance of this contract, the Contractor will generate or need access to export-controlled items.”
- Publication or foreign national restriction on a UH Project:
This type of UH Project may not involve export-controlled items, materials, equipment, software, data, or technology but this Master TCP is required due to a publication restriction or foreign

national restriction. The PI and UH Project participants may not release any information or publish results of the research without the prior approval of the sponsor unless the information or research results are already in the public domain.

Non-US persons may not work on any of these types of projects without the appropriate export license from the US Departments of State, Commerce, or Treasury, and approval from the OEC. It is essential to understand that if the UH Project is export-controlled, the appropriate agency must issue a license for non-US persons to work on the project, prior to commencement of work. The PI and all employees who have supervisory responsibility of non-US persons must be fully aware of their responsibilities regarding possible technology transfer and access to export-controlled technologies. **In the event the project involves non-US persons participating under an export license, the OEC will require the preparation and execution of a PSTCP.**

Non-US Person Visits or Co-Location of Non-US Persons

As previously noted, UH Projects involving non-US persons shall require a PSTCP and will not be included under this Master TCP. To ensure compliance with federal regulations and protect UH research participants from unintentional disclosures, controls must be in place to prevent an unintentional export to non-US persons. Non-US persons, including collaborators, visitors or tours, may not have access to UH facilities where export-controlled research is conducted, including but not limited to research project data, information, materials, etc., without prior written approval from the OEC and an export license, if required.

From time to time it is appropriate to co-locate a non-US person within UH space or facilities due to research or programmatic needs. Prior to placement of any non-US person (paid or unpaid, employee or visiting scholar or guest) within UH facilities where export-controlled research is conducted, an export evaluation must be conducted to determine if any additional precautions or licenses are required. **It is the responsibility of the PI to contact the OEC for prior written approval and, when appropriate, an executed PSTCP or SSTCP for the non-US person and/or an export license, if required.**

UH personnel finding themselves working with or co-located with a non-US person are personally responsible for verifying that an export evaluation has been conducted and the non-US person has been approved for the project and work location. UH personnel may contact their PI or OEC to verify that an export evaluation has taken place and approval for the non-US person. Any export-controlled technology, materials, software etc. that is shared or provided to a non-US person without a license or license exception/exemption could result in an unlawful export, requiring a Voluntary Self-Disclosure to the appropriate federal licensing agency.

Controls

- A laboratory space (as minimal as possible to accomplish the aspect of research that is export-controlled) should be designated as an area in which special procedures must be followed. To that end, the entire UH Project should be evaluated to isolate those individual tasks within the project that needs to be subject to control. Research operations may be limited to secured areas and

physically shielded from access or observation by unauthorized individuals. These areas must remain locked at all times.

- Logs should be maintained for managing access into and movement out of any restricted laboratory space that is designated as an “export-controlled area”. Research operations must be restricted to secure blocks of time when unauthorized individuals cannot observe, nor have access to, export-controlled technologies. Individuals participating in the UH Project may be required to wear a badge, special card, or other similar device indicating their authorized access to designated project areas.
- Export-controlled technology must be clearly identified and marked as export-controlled. All technical documents that are determined to contain export-controlled shall be marked with:

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

- Locks on any entry into designated laboratory space containing export-controlled technologies should be installed or changed so that only personnel permitted on a project can gain access. A plan must be included to control access by janitors, maintenance workers, locksmiths, and delivery/courier individuals, to the extent that such plans are necessary and appropriate. Tangible items such as equipment, associated operating manuals, and schematic diagrams should be stored in rooms with key-controlled access. Soft and hardcopy data, lab notebooks, reports, and other research materials should be stored in locked cabinets. **OEC must be contacted for assistance to ensure compliance with US Export Control Laws.**
- Computers and information systems must be secured and/or monitored so that export-controlled information is not inadvertently made available to individuals not permitted to receive it. At a minimum, computers should be secured as described in “Securing Your Computer and Protecting Your Information” at <http://www.hawaii.edu/askus/718>; laptop users must secure their systems as described in “Best Practices for Laptop users” at <http://www.hawaii.edu/askus/927>. Note that electronic information is still export-controlled wherever it resides, even behind passwords, encryption, and firewalls. Owners of information systems shall use these practices to secure export-controlled data:
 - Password protection with the abilities to log user access and access attempts with timestamps, to lock out users who unsuccessfully attempt to log on after a limited number of attempts, and to audit user activity for suspicious activity.
 - Passwords that are unique to individual users (not shared with groups), and equipped with multi-factor authentication.

- Process to require users to change passwords annually.
 - Strong encryption protocols such as AES 256.
 - Software firewall protection which prohibits non-essential incoming traffic that does not have an associated outgoing connection.
 - Up-to-date anti-malware and anti-spyware software with a process to keep definitions up-to-date.
 - Annual process to review user access and determine whether changes are necessary, and an ongoing process to change user access whenever users' roles change.
 - Physical security of the information system behind a locked door and/or other means to prevent unauthorized access such as remote video or audio monitoring of the physical location.
- Where students are engaged in a UH Project, their identity, nationality, and level of access must be continually monitored during the course of the UH Project. This is necessary as the needs for these management measures may change when individuals they are intended to cover, for compliance with US Export Control Laws, either leave or join the UH Project.
 - Photographs for export-controlled items may be prohibited. If so, all cell phones should remain off and stored in a separate area, outside of rooms containing an export-controlled item(s).
 - After being approved to work on the UH Project and *before* they have the export-controlled software installed, all personnel (including investigators, staff, and students) must be informed of their obligations to take security precautions with export controlled information, equipment, and computers with export-controlled information and/or software.
 - Persons presenting research findings or other technical information at open conferences may not divulge information subject to US Export Control Laws without prior approval from the US Department of State, Directorate of Defense Trade Controls (DDTC), or US Department of Commerce, Bureau of Industry and Security (BIS). Sponsored UH Project agreements containing export-controlled items, materials, equipment, software, data, information or technology may require that project personnel formally request and obtain prior government approval before the release of a publication or presentation. These requests shall be made in compliance with, and within the timeframe stated in the sponsored UH Project agreement. If no timeframe is stated in the UH Project agreement, three to six months may need to be anticipated for approval to be received from the contracting officer. Public release of information shall not occur until any required permission or other government approval is received by DDTC or BIS.

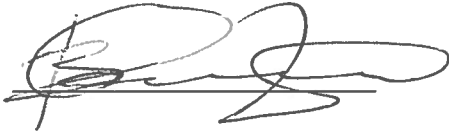
- In most cases, export-controlled research will contractually require that project personnel shall not release or disseminate any information pertaining to the UH Project without the prior written approval of the sponsor, excluding information already in the public domain. In the rare case that there is not a contractual publication restriction and the UH Project involves controlled items, research result and publications generated from the controlled items are still subject to the approval of the sponsor. Therefore, when publications of the UH Projects that involve controlled items are subject to the approval of the sponsor, the impact of such restrictions should be considered prior to employing graduate students and tenure track faculty. Publications (including but not limited to theses, dissertations or journal publications) may be delayed or denied based on the approval of the sponsor or US government.
- All physical items shall be shredded, torn, or dismantled, such that the export-controlled technology's information contained within is unintelligible. Files on hard drives shall be deleted using appropriate sponsor approved measures. UH ITS destruction resources, such as a degausser, shall be used for properly disposing of export-controlled information and/or equipment.
- Individuals shall not take or work on export-controlled projects/information while traveling abroad without prior approval and licenses when required. Electronic devices (e.g. laptops, tablets, smart phones, etc.) containing export-controlled information shall not be taken even if export-controlled information is encrypted or not accessed. In order to minimize the risk of an unlicensed data export, the following options are recommended:
 - Only take "clean" electronic devices. These devices must not contain any unlicensed export-controlled information, should be encrypted, and should only contain user data necessary for the trip. All devices should be reviewed prior to departure to ensure compliance with US Export Control Laws, including but not limited to encryption regulations.
 - The traveler must maintain physical control of all electronic devices while outside of the US.
- **Project personnel must be aware that failure to comply with US Export Control Laws may lead to significant civil and/or criminal penalties which include, but are not limited to, monetary penalties up to \$1,000,000.00 per violation; prison term up to 20 years; denial of export privileges; and debarment from US government contracts.**

Reporting and Responsibilities

Any person having knowledge of a potential violation or non-compliance with the provisions of this plan or any applicable export control directive shall immediately report the circumstances surrounding the

activity to the OEC. Contacts are available at: <http://www.hawaii.edu/offices/export/>. When appropriate, UH shall disclose involvement in violations to the proper authorities in accordance with applicable regulations. Any deviations or waiver from or exception to these procedures require prior approval from OEC.

Approved:



Dr. Vassilis Syrmos

Vice President for Research and Innovation, UH Empowered Official

Date:

MAR 12 2015