UC San Diego

RESEARCH COMPLIANCE AND INTEGRITY
Export Control

Technology Control Plan (TCP)

PURPOSE

This Technology Control Plan (TCP) describes the procedures put in place to protect certain export-controlled equipment, software, materials, technology, and technical data from transfer and access (oral, visual, electronic, physical, etc.) by unauthorized personnel, including non-U.S. Persons. These procedures include physical and information security, procurement, shipping/transporting, personnel screening, training and awareness, and compliance assessment. This TCP includes protocols to control the disposition of research project equipment, software, materials, and technical data.

Additionally, this document informs campus personnel of the security responsibilities and requirements for export restricted items.

SCOPE AND APPROACH

The Principal Investigator or Director is responsible for compliance with this TCP. This TCP is applicable to all UCSD personnel performing export-controlled work or with access to export restricted items and information. This plan is required due to the following conditions:

- ✓ **Access to Export-Controlled Items or Information:** This activity involves access to export-controlled items, materials, equipment, software, data, information, or technology purchased or provided by a third party.

AUTHORIZED PERSONS

Only the persons approved by UC San Diego Export Control listed on the TCP Authorized Persons List (Attachment A) may access export restricted items and information. All UC San Diego Authorized Persons are responsible for appropriately protecting export-controlled equipment, materials, software, technology, and technical data as outlined in this TCP. PIs and supervisors of Authorized Persons shall take steps to confirm that all individuals attend training, review the TCP, and agree to uphold the requirements of this TCP before allowing access to export restricted project items, materials, equipment, software, data, information, or technology.

UC San Diego Export Control must review and authorize all non-U.S. Persons prior to participation. A federal license or exemption may be required.

Personnel Screening: Screen all Authorized Persons to identify Restricted Parties and confirm U.S. Person status before adding any individuals to the Authorized Persons List.

Personnel Training: All Authorized Persons shall attend annual TCP training to attain understanding of the regulations and expectations of safeguarding the items listed in the TCP. Contact Export Control at export@ucsd.edu to schedule a session or take electronic TCP training in UC learning.

Personnel Changes: Inform Export Control as soon as possible to add new Authorized Personnel or upon the termination or departure of Authorized Personnel.

VISITORS

Maintain logs to record *physical* access by non-Authorized Personnel of ITAR-controlled, EAR500/600 series items, or when controlled-information is visible in workspace, computer screen, etc.

- Authorized Persons will escort visitors.
- Confirm visitors are U.S. Persons. If not, consult with Export Control.
- Conduct Restricted Party Screenings on non-UC San Diego visitors.

POTENTIAL LONG-TERM ACCESS

Consult with Export Control prior to placement of any non-US Person (paid or unpaid, employee, student or visiting scholar or guest) within facilities where export restricted research is conducted or ITAR or EAR 500 or 600 items are stored. An NDA for the non-US Person or license may be required.

PHYSICAL SECURITY PLAN

Protect unclassified export-controlled information and items in accordance with the guidelines of this TCP.

Store sonobuoys in locked containers, inside locked facilities at the following locations:

- Camp Elliott, 10201 Pomerado Road, San Diego, CA 92131
- Nimitz Marine Facility (MarFac) ,297 Rosecrans St #3505, San Diego, CA 92106 MARFAC

While on ships for deployment, sonobuoys are in a large box stored and strapped on deck (moved with a crane). There are cameras monitoring the sonobuouys while in transit.

Control visual access by closing the door, protecting/shielding the screen, or confirming only Authorized Persons are in the room. Post a sign notifying of export-controlled activities when only Authorized Persons are permitted.

Secure documentation with export-controlled technical information (including manuals for ITAR items), data, or materials, software, or hardware, in a locked desk drawer, locked filing cabinet, or locked office.

Segregate authorized non-US Persons without approvals for access to controlled information or items. Notify unauthorized non-U.S. Persons and their supervisor of controlled activities and implement time-blocks for the location to prevent access.

Do not hold conversations and discussions in areas where Unauthorized Personnel are present.

Transfer or Disposal of Export-Controlled Items

Work with Export Control prior to any transfer or sale to other UCSD, Surplus, or external parties.

Consult with Export Control on the destruction of equipment, items, and software.

INFORMATION SECURITY PLAN

Protect unclassified export-controlled information residing on unclassified computer systems in accordance with the guidelines of this TCP in conjunction with lab, department, or division IT or central campus ITS.

The following measures provide control access to devices, systems, and controlled information identified in this document:

Labs and personnel working with export-controlled data must become CCR certified.

ONLY UC San Diego Information Technology approved equipment (*e.g.,* computers, instruments, peripheral devices) to download, process, analyze, and store CUI or export-controlled information. Incorporate user identification, password protection, and firewalls to protect from unauthorized access. **Lock and password protect devices**.

Use strong passwords that are compliant with current UCSD password policies.

MAINTAIN CURRENT EQUIPMENT/APPLICATION UPDATES all project equipment and applications that access the data with patches and anti-virus updates.
Purge data from connected equipment, including printers.

Only use **mobile devices** (cell phones, smartphones, tablets, etc.) for export-controlled information if files can remain encrypted while stored.

EMAILS: Avoid placing export-controlled information in the body of the email.
(1) attach controlled information in a password protected (and labeled) document;
(2) indicate in the subject line "Export-Controlled Information Attached"
(3) encrypt the email.
Encryption directions available here.
Do not email passwords. Use token request or SFTP when available from Sponsor.

ENCRYPT all external devices with export-controlled information (e.g., flash drive, hard drive, etc.) at the drive or file/folder level. Encryption must meet the current Federal Information Processing Standards Publication 200 (FIPS-200) standards. Always encrypt data while storing, transmitting, and sharing.
Drives with network access or backup servers must encrypt and password protect, controlled information.
Only store or share controlled data on UC San Diego approved servers for export-controlled information.

Use University or sponsor provided conference call or video platforms and do not record. And **always enable security features**.

Do not use public Wi-Fi hotspots to access controlled data.

PRESENTATIONS AND PUBLICATIONS

Persons presenting research findings or other technical information at open conferences may not divulge information subject to export control regulations without prior approval.

Follow requirements in sponsored project agreements to request and obtain prior approval before the release of a publication or presentation, within the time frame stated. If no time frame is stated provide, three to six months for approvals. Public release of information shall not occur until any required permission or other government approval is received by U.S. Department of State, Directorate of Defense Trade Controls, (DDTC), or U.S. Department of Commerce, Bureau of Industry and Security (BIS) or other relevant U.S. government agency.

When publications of projects that involve controlled items are subject to the approval of the sponsor or involve technical data of defense articles, 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 U.S. government.

INTERNATIONAL TRAVEL

Consult with Export Control prior to traveling with or accessing export-controlled information or items when traveling abroad.

REGULAR ASSESSMENTS AND UPDATES

Export Control will conduct an annual review of this TCP with Authorized Personnel to determine whether changes, updating, or upgrading of the TCP protective measures are warranted. Authorized Personnel should periodically review this TCP and identify potential changes. These reviews will include a check of the project personnel listing, verification of physical security protective measures, and a review of the information security protective measures. Export Control will work with Authorized Personnel to make necessary updates to the TCP.

REPORTING AND RESPONSIBILITIES

Any person having knowledge of a potential violation or noncompliance with the provisions of this plan or any applicable export control directive shall immediately report the circumstances surrounding the activity to the Export Control (export@ucsd.edu) or call (858) 246-3300.

All Authorized Personnel must report any suspicious or unsolicited request for export-controlled information by unauthorized persons. Unsolicited contacts can be in the form of email, personal or telephonic questioning, and requests for assistance via social media. Unsolicited emails will be forwarded to abuse@ucsd.edu. Personal or telephonic queries can be reported through email descriptions of the query and unauthorized person involved. Regardless of whether the contacts seem suspicious they should be reported immediately.

When appropriate, UCSD shall disclose involvement in violations to the proper authorities. Any deviation or waiver from or exception to these procedures requires prior approval of Export Control. Any violation of the terms of this plan may be grounds for disciplinary action.

Business managers and departmental administrators must read the TCP and agree not to add non-US person personnel or to otherwise provide access to export controlled projects without Export Control approval.

Penalties for export control violations range from $250,000 to $1 million per violation and include prison time for criminal penalties. Penalties are specific to each regulatory regime and based on the specific violations. Penalties may be assessed against the institution and against individuals involved in violations. Disclosing violations is likely to significantly reduce penalties.

SHIPPING & TRANSPORTING

When transporting documents, notes, or encrypted export-controlled data, keep items secured and avoid stops at locations not listed on this TCP.

Track shipments of ITAR/EAR-documents or items. Confirm documents and items are labeled. Place items in an inner envelope/box/crate, etc. marked "**ITAR/EAR-CONTROLLED**: **NO NON-US PERSON ACCESS**." Place inside an envelope, box, crate, or container for shipping or transporting with **no export-controlled markings.**

Obtain documentation from the receiver on protocols confirming receipt of item by a U.S. Person or authorized non-U.S. Person.

Coordinate with Export Control controlled shipments internationally or to non-U.S. Persons.

ITAR items ***will*** require a license. Do not ship until the license is approved and received by Export Control.

EAR-controlled items ***may*** require a license. Coordinate with Export Control in advance for next steps.

Export Control will apply for all export licenses. Retain copies of the license. Provide copies of all shipping paperwork to Export Control. Consult a shipping Broker prior to shipping equipment/items internationally.

Attachment A:
Acknowledgement of Responsibilities for Technology Control Plan

By signing below, I certify that the personal information provided below is accurate and complete and acknowledge the following:

1. I have been provided a copy of the Technology Control Plan (TCP), have read and understand its provisions, and intend to abide by its terms and conditions including, but not limited to, only permitting project personnel who have been authorized by the Export Control Officer (ECO) to access *Covered Items and Information*.

2. I have completed the required Technology Control Plan Training Program specified by the ECO and agree to complete required refresher training for as long as I have access to *Covered Items and Information*.

3. I understand that I can be held personally responsible for any unlawful disclosures or exports, including transfers to foreign nationals in the United States, of *Covered Items or Information*. I further understand that individual per violation fines and penalties of up to $1,000,000 and 20 years of imprisonment are possible for violations of US export control laws.

4. I understand that my obligation to protect *Covered Items and Information* continues beyond the end of my participation on this project and my affiliation with the University of California.

5. I understand that if I have questions or concerns regarding the content and implementation of this TCP or about US export control requirements that I should contact the ECO right away for assistance.

CERTIFICATION

I accept responsibility for the oversight of this TCP. I will coordinate all changes in locations, scope of work, personnel with Export Control. I will share concerns with Export Control. I understand that I could be held personally liable if I unlawfully disclose export-controlled information or items to unauthorized non-U.S. Persons.

John Hildebrand	jahildebrand@ucsd.edu
TCP Lead / PI Name (Print)	**UCSD Email**
JohnHildebrand	jahildebrand@ucsd.edu
Employee ID #	**Telephone #**
John Hildebrand	10/27/2023
TCP Lead / PI Signature	**Date**

TCP Authorized Persons List

I understand that I could be held personally liable if I unlawfully disclose export-controlled information or items to unauthorized non-U.S. Persons.

Frasier, Kaitlin	kfrasier@UCSD.EDU
Name (Print)	**UCSD Email**
21822055603650	kfrasier@ucsd.edu
Employee ID #	**Telephone #**
Frasier, Kaitlin	11/8/2023
Signature	**Date**

Jones, Joshua	j8jones@ucsd.edu
Name (Print)	**UCSD Email**
Joshua M. Jones	j8jones@ucsd.edu
Employee ID #	**Telephone #**
Jones, Joshua	12/22/2023
Signature	**Date**

Kieran Lenssen	klenssen@UCSD.EDU
Name (Print)	**UCSD Email**
10438670	klenssen@ucsd.edu
Employee ID #	**Telephone #**
Kieran Lenssen	11/13/2023
Signature	**Date**

Sean Wiggins	swiggins@ucsd.edu
Name (Print)	**UCSD Email**
Sean Wiggins	swiggins@ucsd.edu
Employee ID #	**Telephone #**
Sean Wiggins	11/21/2023
Signature	**Date**

Thayre, Bruce	bthayre@ucsd.edu
Name (Print)	**UCSD Email**
Employee ID #	**Telephone #**
Signature	**Date**

Whitaker, Katherine	kwhitaker@UCSD.EDU
Name (Print)	**UCSD Email**
Employee ID #	**Telephone #**
Signature	**Date**

Name (Print)	**UCSD Email**
Employee ID #	**Telephone #**
Signature	**Date**

Name (Print)	**UCSD Email**
Employee ID #	**Telephone #**
Signature	**Date**

Name (Print)	**UCSD Email**
Employee ID #	**Telephone #**
Signature	**Date**

Attachment B: Data or Equipment

DATA/EQUIPMENT	**Sonobuoy**
Classifications: **ITAR – USML / EAR CCL / CUI**	ITAR
Description	
Sonobuoy models and quantities: **53D (6) 53 (97) 53G (144)** **77B (34) 77C (11) 57B (9)**	
Dates	**Location**
9/18/2023	Camp Elliot Container 5338373 Locked container, inside locked facility.

DATA/EQUIPMENT	**Sonobuoy**
Classifications: **ITAR – USML / EAR CCL / CUI**	ITAR
Description	
Model & quantity: **53D (48) 53F (240) 53G (144)** **62E (105) 77B (106) 57B (96)**	
Dates	**Location**
9/18/2023	Camp Elliot Container 5473985 Locked container, inside locked facility.

DATA/EQUIPMENT	**Sonobuoy**
Classifications: **ITAR – USML / EAR CCL / CUI**	ITAR
Description	
Model & quantity: **53G (40) 53F 0 53D 3 62C 3**	
Dates	**Location**
9/18/2023	MARFAC Quonset Hut Locked container, inside locked facility.