UNIVERSITY OF TEXAS ARLINGTON

Export Control Technology Control Plan (TCP) for DD 2345: Unclassified Military Critical Technical Data (MCTD)

OVERVIEW

Militarily Critical Technical Data Agreement DD Form 2345 is used for:

- U.S./Canadian defense contractors or other entities to obtain DOD/DND **unclassified export controlled technical data**; and
- to attend gatherings such as symposiums; program briefings; meetings designed to publicize advance requirements of contracting agencies; pre-solicitation, pre-bid, pre-proposal, pre-award conferences; workshops; and tours.

Unclassified Militarily Critical Technical Data (MCTD) received during these activities is data that can be used to produce military or space equipment and related technology. It also includes such items as blueprints, drawings, computer software and operating instructions and technical information. Technical information, data, materials, or software received must be secured from use and observation by unlicensed non-U.S. citizens.

Procedures

The Office of Research Administration – Regulatory Services holds and administers a centralized DD 2345 Militarily Critical Technical Data Agreement on behalf of the University. If you are requested to provide a Militarily Critical Technical Data Agreement (Form DD 2345) or have one on file, that means that you may be receiving or will be granted access to **export controlled** technical data. You must have a Technology Control Plan (TCP) in place prior to bringing any of the technical data to UTA campus. The TCP is intended to provide the necessary guidance and safeguards you are responsible for, in order to comply with the Militarily Critical Technical Data Agreement and prevent the unlawful disclosure of export controlled information.

Instructions for Completion of this Form

The DD2345 TCP is pre-loaded with information about applicable UTA policies for handling unclassified export controlled technical data. Review the information, then provide additional information as instructed on page 1 (contact information, usage and sponsorship) and items 1a, 1b, 2a, 2b, 3, and 8.

Each person listed in section 9 who will have access to the militarily critical technical data (MTCD) from your project/event/conference/meeting must complete UTA's Export Control training module which is located at the following link: https://www.uta.edu/ra/real/researchspace.php?view=7.

For all sections of the TCP, carefully review the details and all information associated with any links provided, to ensure that your lab can and will meet the requirements. If there are any requirements that you are unable to meet, notify Regulatory Services to identify exceptions or accommodations. This TCP is a standardized template but can be altered to fit your particular lab/project.

To summarize your action items: 1) Supply additional information in the text boxes where applicable; 2) Review TCP details to ensure you can/will comply; 3) Obtain signatures from all personnel; 4) Ensure that all personnel complete training; 5) Submit to Regulatory Services at regulatoryservices@uta.edu for processing and approval.

Export Control Technology Control Plan (TCP) for DD 2345: Unclassified Military Critical Technical Data (MCTD)

This TCP contains CONFIDENTIAL information classified as Category I (Confidential) Data. The TCP must be maintained in a secure manner with access restricted to only University Administration and authorized personnel listed in this TCP.

Date:

Responsible Individual & Contact Information:

Background & Usage:

Export Controlled, Militarily Critical Technical Data will be received under UTA's DD 2345 (Militarily Critical Technical Data Agreement). The data are needed to bid or perform on a contract with any agency of the U.S. Government or the Canadian Government or for other legitimate business activities in which the contractor is engaged, or plans to engage.

Additional Case-Specific Information (name and description of conference, event, or meeting; host agency; description of the type of materials that will be received):

Support/Sponsorship:
Reference appropriate Agreement(s) related to the controlled information (Sponsored Project/NDA/MTA etc.) if applicable.

1. **Physical Security Plan** (In accordance with the Militarily Critical Technical Data Agreement, UTA agrees to secure the Militarily Critical Technical Data (MCTD) received/accessed. The sections below detail case-specific security provisions):

   a. **Location** (describe the physical location where the MCTD will be secured, including building and room numbers):

   b. **Physical Security**:

   MCTD will be secured whereby only individuals listed and authorized on this TCP have access. Physical/hard copy items will be secured in a locked drawer, cabinet, lab or office (listed in 1.a. above) where only authorized TCP individuals have access by key or key card.

   MCTD items, documents, materials, or storage devices (if applicable) will be clearly identified and marked with the following warning:

> ***WARNING: AUTHORIZED PERSONNEL ONLY - This item is restricted by the federal International Traffic in Arms Regulations (ITAR) and/or the Export Administration Regulations (EAR). Disclosure to foreign persons without prior U.S. Government approval is prohibited. Violations of these export laws and regulations are subject to severe civil and criminal penalties.***

During work with the MCTD, materials will be physically shielded from observation by unauthorized individuals by operating in secured laboratory/work spaces, or during secure time blocks when observation by unauthorized persons is prevented.

If MCTD is removed from the approved location (1.a.), the Authorized TCP Individual will keep it within their "effective control" at all times by keeping the items under his/her physical possession or in a secured place such as a hotel safe, a bonded warehouse, or a locked or guarded exhibition facility;

MCTD will not be shipped, transmitted, or hand-carried outside of the U.S. without first consulting with UT Arlington's Export Control Officer.

Additional Case-Specific Physical Security Details, if applicable:

2. Information Security Plan:

a. Structure of IT security:

Computers storing MCTD will be password-protected. In the case of shared computers, the MCTD will be stored in a password-protected drive or file with access restricted to authorized TCP individuals.

If MCTD will be in electronic format, it will be maintained on the following devices (described for each location):

b. IT Security Plan – all Authorized TCP Individuals will comply with the standards, procedures, or policies outlined below for IT security:

All MCTD is considered Category I (Confidential) Data and will be maintained in accordance with UTA's Minimum Standards pertaining to backups, change management, virus protection, physical access, and system hardening: https://www.uta.edu/security/security_standards/servers_workstations/index.php

MCTD will be stored in a UTA-sanctioned data storage location: https://www.uta.edu/security/approved_storage/index.php.

MCTD in electronic format will be protected by password and will comply with UTA's password security standards:

https://www.uta.edu/security/password/index.php.

Use of portable/external storage devices such as flash drives or laptops will comply with UTA's standards for Security: https://www.uta.edu/security/usb_security/index.php. In addition, if a portable media or storage device is removed from the approved location (1.a.), it will remain within the Authorized TCP Individual's "effective control" at all times via the following procedures:

1. **An Authorized Individual will keep the items under his/her physical possession *or* keep it secured in a place such as a hotel safe, a bonded warehouse, or a locked or guarded exhibition facility;**
2. **An Authorized Individual will take security precautions to protect against unauthorized release of the MCTD:**
   a. **use of secure connections when accessing e-mail and other business activities that involve the transmission and use of the technology,**
   b. **use of password systems on electronic devices that store technology, and**
   c. **use of personal firewalls on electronic devices that store the technology;**
3. **Authorized Individuals will not ship, transmit, or hand-carry the MCTD outside of the U.S. without first consulting with UT Arlington's Export Control Officer.**

Use of mobile devices will comply with UTA's best practices and requirements: https://www.uta.edu/security/security_standards/mobile_devices/index.php.

If MCTD will be transmitted electronically (with Authorized Individuals or the Supplying Agency), describe how the transmission will take place and how it will be secured (procedures must be approved by Information Security):

****UTA's Information Security Office will review and approve procedures that are deviations, exceptions, or additions to any of the Security Plan referenced above.**

3. Personnel Changes and Maintaining Security:

In the case of personnel changes (termination or individual leaving the lab), MCTD will be protected by removing access (key, key card, etc.) of the individual and by changing any passwords on protected electronic devices and/or files.

Additional Case-Specific Physical Security Details, if applicable:

4. Conversation Security:

Discussions about the MCTD will be limited to Authorized TCP Individuals and will be held only in areas where unauthorized personnel are not present. Discussions with third party subcontractors will only be conducted under signed agreements that address the terms of the Militarily Critical Technical Data Agreement and export control regulations.

5. **Personnel Screening Procedures:**

In accordance with The University of Texas System's policy on Criminal Background Checks (*UTS124*, *amended August 31, 2010*), a criminal background check (CBC) will be performed on each employee.

In accordance with the Militarily Critical Technical Data Agreement, no person who will have access to MCTD is disbarred, suspended, or otherwise ineligible to perform on U.S. or Canadian Government contracts or has violated U.S. or contravened Canadian export control laws or has had a certification revoked under the provisions of U.S. DoDD 5230.25 or Canada's TDCR. Regulatory Services will perform Restricted Person/Party Screening prior to authorization of an individual on this TCP or engagement of a third party subcontractor.

6. **Training / Awareness Program:**

The Responsible Individual listed on this TCP is responsible for training other authorized TCP personnel regarding the procedures detailed within this document.

Each person listed as authorized personnel on this TCP will be familiar with the federal export control regulations and UT Arlington's Policy for Export Controls: http://www.uta.edu/research/administration/departments/rs/export-control/index.php

Each person listed as authorized personnel on this TCP will complete the online training module "Export Control": https://www.uta.edu/ra/real/researchspace.php?view=7.

No additional personnel will have access to the controlled material/information without approval by UT Arlington's Responsible Official for Export Control (through amendment of the TCP).

7. **Self-Evaluation Program:**

The Responsible Individual will review and evaluate the effectiveness of this TCP on a routine basis. The review will address each of the items described in the sections above (1. – 6.)

Any violations will be reported to the Export Control Officer via an Incident Report. Corrective action will be taken immediately following the identification of any violations of the TCP. If deficiencies are identified, the TCP will be modified to provide appropriate protection. Modifications will be coordinated and approved by the University Export Control Officer before implementation.

8. **Completion of Project and Disposition of Controlled Items:** Describe the anticipated or estimated length of this project, and explain the disposition of the controlled information/materials/technology

at the conclusion of the project (ex. materials will be returned or transmitted back to the sponsor; hard copies will be shredded; electronic data will be destroyed, etc.).

Export Control Technology Control Plan (TCP) for DD 2345:
Unclassified Military Critical Technical Data (MCTD)

9. Project Personnel & Certifications (In the table below, list every person who will be authorized to access the MCTD).

****Each person signing below certifies that their citizenship status provided in this document is correct and that they have read, understand, and will adhere to the terms of this Technology Control Plan and any referenced policies, procedures, or standards. Signature certifies that individual agrees not to disseminate militarily critical technical data in a manner that would violate applicable U.S. or Canadian export control laws and regulations.****

Training & Awareness: You must (1) read and adhere to the procedures of this TCP (including the Overview at the beginning of this document), (2) complete site-specific training with the Responsible Individual, (3) complete the online Export Control training module, and (4) be familiar with and adhere to any applicable EAR and/or ITAR regulations. **Reasonable Care**: You may be held personally liable for violations of the ITAR or EAR export control regulations. As a result, you must exercise care in using Export-Controlled Information, Technology, or Materials. Controlled Items must be handled in accordance to the security plans and/or controls specified in this TCP and only be shared with authorized Project Personnel. Unsecured Export-Controlled Information or Materials should not be left unattended. You must not travel internationally with any controlled information, technology, or materials without first consulting the Export Control Officer. Both civil and criminal penalties may be imposed for unlawful export and disclosure of Export-Controlled Information up to and including incarceration. If you have any questions or concerns, contact the Export Control Officer at regulatoryservices@uta.edu or 817-272-3723.

Name	Completion Date of Online Training Module	Citizenship Status (U.S., non-U.S., Permanent Resident)	Role/Status (faculty, staff, student, non-UTA collaborator)	Signature & Date

Review & Approval of TCP by University Authorized/Empowered Official for Export Control:

____
Empowered Official

____
Date